Troubleshooting Guide For Cisco Unified Expert Advisor

Release 7.6(1)

May 2009

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: 408 527-0833

Table of Contents

List of Figures

Chapter 1

Overview

This manual describes how to troubleshoot common issues for Unified Expert Advisor. The document also explains the tools and techniques that can assist in the troubleshooting process.

When troubleshooting a telephony or IP network environment, it is important to define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem from most likely to least likely until the symptoms disappear.

This chapter contains the following topics:

Problem Solving Process

Guidelines to Assist in Isolating Problems

The following steps provide some guidelines to assist in isolating a particular issue.

Step 1 Analyze the problem and create a clear problem statement. Define symptoms and potential causes.

Step 2 Gather the facts that you need to help isolate possible causes.

Step 3 Consider possible causes based on the facts that you gathered.

- *Was anything recently added, removed, or modified?*
- *Is it a reproducible event?*

- *Does it occur at a particular time of day, or day of week?*
- *Have there been any changes made to the domain, network, or security policies?*

Step 4 Create an action plan. Begin with the most likely problem and devise a plan in which you manipulate only one variable at a time.

Step 5 Implement the action plan, performing each step while testing to see whether the symptom disappears.

Step 6 Analyze the results to determine whether the problem has been resolved. If it has, the process is complete.

Step 7 If the problem has not been resolved, create an action plan based on the next most probable cause on your list, or contact the Cisco Technical Assistance Center (TAC), or your Cisco Partner.

Note: Only change one variable at a time. If that does not resolve the issue, undo that change and move on to the next step of your plan.

Troubleshooting Checklist

Complete this checklist to assist in isolating the issue, or to provide information to your support partner or Cisco Technical Support.

1. What is the version of Unified Expert Advisor that is currently running? Include any patch or upgrade information.
2. Is this a new installation or an upgrade?
3. If this is an upgrade, what version was previously installed?
4. When did the problem occur?
5. What are the observed symptoms, and the conditions under which these symptoms occur?
6. Was anything changed or updated in hardware, software, or network components prior to the first occurrence of the observed symptoms?
7. Describe the related call flow. Some examples include: Public Switched Telephone Network (PSTN) originated or IP Phone originated.
8. Is the problem reproducible?
9. What is the call transfer method used?
10. Are you able to capture a screen shot of the error or failure? If Yes, save it to a file and attach to a case.

Network Topology

Complete this checklist to assist in isolating the issue, or to provide information to Cisco Technical Support.

1. Has auto-negotiate been disabled on all PCs, routers, and switch ports?

   Note: Duplex/speed mismatch between a device and its corresponding port on the switch is the single most common problem for network latency.

2. Is a network topology diagram available?

3. Which type of IP Gateway is being used in this Unified Expert Advisor solution?

4. On which server are the recorded media files located, and what is the path to those files?

5. Collect and provide versions of IOS, applications, and Engineering Special (ES)/patch levels in the environment.

Chapter 2

Obtaining Log Files

Log files are obtained through the Real Time Monitoring Tool (RTMT) Plugin. You obtain the plugin from the operations console.

This chapter contains the following topics:

Downloading and Installing the RTMT Plugin

The RTMT plugin can be downloaded from the operations console. Versions of the plugin are available for both Windows and Linux platforms.

To download and install the RTMT plugin:

Step 1 Log in to the operations console for Unified Expert Advisor.

Step 2 Select **Tools > RTMT Plugin Downloads**.

Step 3 Select the platform (Windows or Linux) then click **Download**. The plugin is downloaded to your local computer. The file size of the executable is around 35 MB.

Step 4 Double-click the plugin executable on your local computer to install it. Details on the installation can be found in Chapter 2 of the "*Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*.

Obtaining Log Files Using the Real Time Monitoring Tool

Use the Real Time Monitoring Tool to browse, view, and download log files. This task explains how to obtain the logs for the runtime server(s).

Step 1 Start the Real Time Monitoring tool. From Windows, select **Start** > **Programs** > **Cisco** > **CallManager Serviceability** > **Real-time Monitoring Tool**.

Step 2 Log in with the username and password you created for Unified Expert Advisor while installing Unified Expert Advisor.

Step 3 Select the Default Profile.

Step 4 In the left pane, labeled **System**, Click **Trace & Log Central**.

Step 5 In **Trace & Log Central**, double-click **Remote Browse**. A dialog appears.

More details about Remote Browse can be found in the *Real Time Monitoring Tool Administration Guide for Cisco Unified Expert Advisor*.

Step 6 In the dialog, select the radio button for **Trace Files**. Click **Next**.

Step 7 Select the checkbox next to **Expert Advisor Runtime Service**. You can check either the box for *All Servers* to view the logs for all runtime servers in this cluster, or you can check the box for individual servers. Click **Next**.

Step 8 You can optionally select System Services/Applications to obtain logs for additional system services, or just click **Finish** to obtain just the runtime server logs.

Step 9 A new pane appears in **Trace and Log Central** with a folder called **Nodes** in it. Double click the **Nodes** folder and drill down to the runtime servers. Double-click the **runtime** folder to display the list of log files in the right pane.

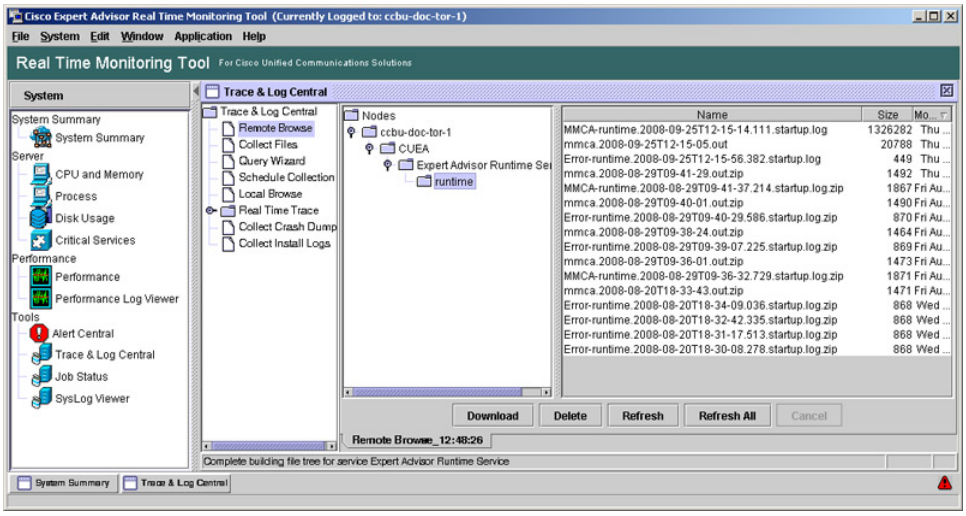
There are several log files that appear in the right page, including:

- MMCA-runtime.[TIMESTAMP].log
- MMCA-runtime.[TIMESTAMP].startup.log
- MMCA.[TIMESTAMP].out
- Error-runtime.[TIMESTAMP].startup.log
- Various zipped version of the above files

Step 10 Double-click the latest version of MMCA-runtime.[TIMESTAMP].log to open it in the default viewer. This file contains a majority of the call-logging for the runtime server. You can optionally select the file and click **Download** at the bottom of the page.

Note: Zip files must be downloaded and unzipped locally with a zip program to be viewed, they cannot be viewed from within the RTMT tool.

Figure 1: Viewing Logs in RTMT



Chapter 3

General System-level Troubleshooting Tips

General Tips

Unified CVP and Gateway logs both indicate that Unified CVP is playing Music On Hold (MOH) to the caller, but the caller hears dead air

Symptom(s): Attempting to Queue to a Unified ICM Skill Group (Assignment Queue) via Unified CVP. Unified CVP logs indicate it is playing media to caller. Call is established, but caller hears dead air.

Resolution: On the gateway, make sure you do NOT have a line that says: "no ip route". If you do, type "ip route" to double-negate it.

Agents are logged in and available in Unified Expert Advisor, but they don't show up as logged in or ready in Unified ICM real time monitor

Symptom(s): Agents are logged in and available in Unified Expert Advisor, but they don't show up as logged in or ready in Unified ICM real time monitor. These expert advisors (agents) also don't appear in the ICM Agent Explorer.

Resolution:

- Verify all expert advisors have first name and last name in Cisco Unified Presence server, and in the Unified Expert Advisor operations console.
- Verify that the runtime server is in service (Operations Console > Serviceability > Control Center).
- Verify that the skill group peripheral number in the ICM Skill Group Explorer matches the skill group peripheral number" in Unified Expert Advisor's Assignment Queue configuration

page (Operations Console > Daily Management > Assignment Queues). If they do not match, then you can change it in Unified ICM to match Unified Expert Advisor (it cannot be changed in the Unified Expert Advisor Operations Console).

Agents are logged in and available in Unified Expert Advisor, but they don't show up as logged in or ready in Unified ICM real time monitor

Symptom(s): On the Expert Advisor PG system, in the PG directory, a file called AutoConfigError.txt contains errors such as the following:

```
2008/06/17 16:41:39: Config update error on ADD of AGENT PID=5001
PerNum='MMCA_1
' Ent Name='MMCA_1.Boston.ExpertAdvisor'
PerName='MMCA_1'
The enterprise name that was entered is already in use
```

Resolution:

- Duplicate agent configuration can happen if you delete and recreate the same agent or assignment queue on the runtime servers. Restarting the PG and the runtime server generally resolves the issue.
- This can also happen if you actually have agents with duplicate first and last names. In this example, 'MMCA_1.Boston.ExpertAdvisor' means you have an expert advisor who's name is 'ExpertAdvisor Boston'. Look in the Expert Advisor OAMP screen for each expert, in the Unified ICM section at the bottom of the screen, and make sure you have only one expert who's name is 'ExpertAdvisor Boston'.

Expert logs into Cisco Unified Presence, but never receives a welcome message.

Symptom(s): Expert logs into Cisco Unified Presence, but never receives a welcome message. The agent state monitoring tool **`show agent all`** also shows expert as Available but NOT_READY.

Resolution: The Runtime server may not be in service. Verify the runtime server is running.

Experts Phone Never Rings

Symptom(s): Call is ready to be received by an expert advisor, but the phone never rings. Caller hears Busy.

Resolution: Verify the SIP port in the SIP Trunk configuration matches the SIP port in the SIP Security Profile which is configured for that SIP Trunk.

Unified Presence SIP Proxy is using a high amount of CPU

Symptom(s): IM messages cannot be sent or call routing fails at an extremely high rate for Unified Expert Advisor and/or Unified CVP that go through the Cisco Unified Presence server proxy.

Resolution: Use the following configuration under the proxy service parameters in Unified Presence (if not set to this by default):

- Set initial processes to 20
- Set max no. of spare processes to 20.
- Set max no. of processes to 20.

Unified Expert Advisor Runtime stays in partial service on startup

Symptom(s): Unified Expert Advisor Runtime stays in partial service on startup. The logs show that RDA is unable to go into partial service as MPI receives a '404' response (not found) from Cisco Unified Presence.

Resolution: Verify that the Cisco Unified Presence users configured as the Unified Expert Advisor Runtime users are different for each runtime server. Also verify that those users have Cisco Unified Personal Communicator (CUPC) privileges granted in the end user configuration on the Cisco Unified Communications Manager (Unified CM). One way to verify this is to shut down the Unified Expert Advisor runtime servers, start Cisco Unified Personal Communicator and login as the users configured for the Unified Expert Advisor runtime server. Verify that users can login and send messages to each other.

NullPointerException appears in the top level install.log file

Symptom(s): A NullPointerException may appear in the top level install.log file. This error appears in all Unified Expert Advisor systems during an initial install or upgrade.

Resolution: This message is a benign log statement has no effect on any functionality. It is the result of the existing code in the underlying VOS platform.

Unified Expert Advisor web page timeout does not default back to login page

Symptom(s): An unused screen may time out and automatically log out the administrator without any evidence of the log out on the screen. When the administrator tries to click something on that page, the login page appears and the requested action is not performed.

Resolution: You will experience this problem on any Operations Console page. Be sure to edit and save changes before the default timeout (30 minutes) occurs.

Operations Console screens don't return to previous screen when cancelled

Symptom(s): When you select an existing Runtime Server and then click Cancel, the page changes to the Runtime Server summary page. It does not return to the previous page. The same problem exists if you select the Reporting Server, and click Cancel. It returns to the Reporting Server summary page.

Resolution: This is a benign problem and has no effect on any functionality.

Chapter 4

Tracing a Call Through the System

This section details tracing a call through the components of the Unified Expert Advisor system.

The components of the system include:

- Ingress Gateway - as a Caller source
- Unified CM - as a Caller source
- Cisco Unified CVP Call Server / VXML Server
- Cisco Unified ICM
- Cisco Unified Presence Proxy Server
- Unified CM - as an expert advisor destination

Tracing the Call

What components did the call reach?

You can track the call through the system by searching for a Cisco-GUID. The Cisco-GUID is the common denominator that is used in logging for every call across each component. Find the relationships in the Unified CVP logs.

The Cisco-GUCID has the format: **`DEAD91DD1000011A74D013BE0A5687DD`**.

There are two exceptions to the common Cisco-GUCID:

- When Unified CM is the caller source, use the LegID. The format of LegID is: **`120111222148396083`** .

- If the call never makes it to Unified Expert Advisor from Unified CVP 4.x, then search for the GUID. The GUID has a format of: **`05A2AEC3-10000115-550959F1-0A568782`** .

To determine which components the call reached, sear for the Cisco-GUID/GUCID in the following logs:

- Unified Expert Advisor MMCA logs
- Unified ICM VRU PIM "VRU Capture" logs
- Unified Expert Advisor PG PIM and OPC logs
- All Unified CM and Unified Presence logs
- Unified CVP logs
- Ingress gateway logs (if your calls are arriving via TDM)
- VXML gateway logs
- **Note:** For IOS logs, turn on "debug ccsip all"

Using calltrace.sh to Parse the Logs

If Call GUID is known and only one call needs to be traced then you can use the following shell script to quickly parse the logs.

Obtain the logs and use the following bash shell script below to grab the important lines from the runtime logs.

To run the script

1. Copy the log files to a computer that can run the script. The computer must be able to run a bash script.
2. Change your working directory to the location of the logs.
3. Run <location of script>/calltrach.sh <guid>

Three files are created:

- <guid>.txt displays the lines with the guid in them
- <guid>.fgrep.txt displays the strings used to search with, guid, contactid, mpi interaction ids
- <guid>.fulltrace.txt contains the complete call trace with any of the above strings in them

Note: This script can take a long time to run based on the size of the logs. It will search over zipped logs and has to traverse the entire set of logs twice, the first to get the right parameters, the second to get the full call trace. For example, with 5GB of zipped logs (close to 50GB unzipped), on a powerful server, this took approximately 10-15 minutes to complete.

calltrace.sh

```
#!/bin/bash

#Do full grep over all logs for this GUID provided
zgrep $1 MMCA-runtime* > $1.txt

#Find all interaction ids over previously grepped logs by getting 10th param on
SEND_NEW_INTERACTION_REQ lines
GET_INTERACTION_IDS=$(grep SEND_NEW_INTERACTION_REQ $1.txt | cut -f10 -d'[' | cut -f1
-d']' | cut -f2 -d '=')

#get Contact id from guid log on CONTACT_CREATED line
CONTACT_ID=$(grep CM-6-CONTACT_CREATED $1.txt | cut -f2 -d'[' | cut -f1 -d']' | cut -f2
 -d '=')

#Use array to iterate over any interactions created for this guid, usually there are 2,
 but there may be 1 or more than 2
declare -a MPI_INTERACTION_ID
MPI_INTERACTION_ID=($GET_INTERACTION_IDS)

echo "Contact ID = $CONTACT_ID"

#Echo search strings to new file
echo $CONTACT_ID > $1.fgrepsearch.txt
echo $1 >> $1.fgrepsearch.txt

for interaction in "${MPI_INTERACTION_ID[@]}" ; do
    echo "found interaction $interaction"
    echo $interaction >> $1.fgrepsearch.txt
done

#use search strings in file to get all details of call trace and output to fulltrace
file
zfgrep -h -f $1.fgrepsearch.txt MMCA-runtime* > $1.fulltrace.txt
```

Tracking the Call in Unified CM

If the call was delivered to a Unified CM phone, then the Cisco-Guid should appear in the CM logs.

If the call was originated by a CM phone, then you will not find the Cisco-Guid there. To find the call:

- Search the Unified CVP log for all lines containing both the Cisco-Guid AND the text "[INBOUND]: Display Name"
- In the resulting lines, look for "**`LEGID = 120111222148396083`**" (for example, the number is different for each call)
- Search the CM logs for the LegId you find above.

- **Note:** in order to get the necessary information in the Unified CVP logs, use Unified CVP's diagnostic page or other method to turn on DEBUG level logging, and the DEBUG41 trace masks (on by default in CVP 7.0+).

Tracking the Call in Unified ICM

Cisco-Guid is in the ECC variable `user.media.id`, once CVP has received the call.

Search these log files:

- Unified ICM VRU PIM Trace logs - these contain all the CVP - ICM GED-125 messaging and is always enabled.
- Unified Expert Advisor PG OPC log

Search the Historical Database:

- Termination_Call_Variable – written as each ICM call leg ends, for each PG
- Call_Route_Variable – written as each routing script ends

ECC Variable records are written one per variable, per TCD record. To find the user.media.id ECC variable, you need to know its internal ID (a number in the 5xxx range), and do a join from the corresponding TCD record where Termination_Call_Detail.RecoveryKey = Termination_Call_Variable.TCDRecoveryKey.

Note: By default, Unified ICM does not store ECC variables in the database. In order for this to work, you must set the variable to "persistent" in the ECC Variable config tool.

Tracking a Call that does not reach Unified Expert Advisor

ICM Script Editor – Script Monitor	
If call doesn't reach script	Check your Unified ICM and CVP configuration See the CVP troubleshooting guide: **http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_troubleshooting_guides_list.html**.
If call tries to queue but fails SendToVRU or RunExtScript nodes	Check the CVP > CallServer > SIP > DNIS length. See the Unified CVP troubleshooting guide: **http://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_troubleshooting_guides_list.html**.
If call fails the queue node before queuing	Check the Unified Expert Advisor assignment queue and the Unified ICM Skill Group configuration. Check the Skill Group real-time data.

ICM Script Editor – Script Monitor	
	See the Unified Expert Advisor administration guide: **http://www.cisco.com/en/US/products/ps9675/prod_maintenance_guides_list.html**.
If call fails the queue node after queuing	Check the Translation Route configuration in Unified ICM and Expert Advisor. Check CUP static routes: TransRoute DN's should be mapped to runtime servers. Check CVP SIP tab: Proxy Server should point to CUP server. Check script variable call.RequeryStatus for reason code. See the Unified ICM configuration guide: **www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html**[4], or the Unified CVP and Expert Advisor documents listed above.

Skill Group real-time data	
In ICM Script Editor select **Script > Display Real Time Data ? Skill Group (from dropdown list)**	
Log = 0(No logged in agents)	is Expert Advisor in service? is EA PIM in service?
Log = 0(No logged in agents)	check what AQ agents are logged in to do they meet all membership criteria? ensure AQ maps to correct skill group Skill Group Peripheral Number matches skill group name suffix
Log > 0; Ready = 0(All agents not ready)	check for agent configuration errors check for autoconfiguration errors(See section on Unified ICM troubleshooting)

4) http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Chapter 5

Unified ICM and ICM Gateway Troubleshooting

Interactions between the Unified ICM PG and Unified Expert Advisor

The Unified ICM Gateway (running on the runtime servers) and the Peripheral Gateway (PG) connects the Expert Advisor system to the Unified ICM system. When the Unified ICM PG starts, the PG issues monitor requests and queries for all known agent devices and it requests configuration information from the active runtime server. This is how initial agent state is acquired for an Expert Advisors, and how Assignment Queues (skill groups in ICM) and Expert Advisors (agents on ICM) are autoconfigured from the Expert Advisor system to Unified ICM.

The PG also issues ROUTE_REGISTER_EVENT messages to request routing control over the Translation Route DNs specified in the Expert Advisor system (in **System Management > Translation Route Targets**).

Once the PG is up, the running (active) PG receives Agent state events that indicate the current state of Unified Expert Advisor system resources as they change.

Note: Unlike other types of PGs, no call events are received from the Unified Expert Advisor system. The only exception is the routing dialog to route calls and a single CALL_TERMINATION_EVENT to indicate when a call has ended on Expert Advisor.

EMSMON - Monitoring the PIM

Tracing to the screen in the PG is disabled by default. However, you can use EMSMon to view logged messages as they appear in real time.

To run EMSMon on the instance *icm* for *PG1A* and *pim1* you would issue the command **`emsmon icm PG1A pim1`** from a DOS prompt on the server running the PG.

Note: The command can be run remotely on any Unified ICM machine by adding a forth parameter with the PG machine name, for example **`emsmon icm PG1A pim1 MYSERVER`**. Note that this only works if the machines have a trusted relationship within the domain.

Close the DOS window or type CTRL-C to exit EMSMon.

PROCMON

The procmon tool allows you to look into the PIM and see what it is doing or has done. The syntax for starting procmon is the same as EMSMON, the difference is procmon is an interactive shell.

Start procmon with the command **`procmon icm PG1A pim1`** where **`icm`** is your instance name, **`PG1A`** is the correct PG, and **`pim1`** is the correct PIM for your system.

Note: The procmon tool should be run on the active side PIM. If the listed commands are not run on the active side, they do not return any information.

debug - Set Tracing

`debug /on`, or **`debug /on /level 3`** will turn on the suggested default level of tracing. Levels are from 1 to 5, with 1 being the least tracing (0 actually none) and 5 being the greatest amount of tracing.

Example output:

```
C:\Documents and Settings\torero>procmon icm PG1A pim1
>>>>debug /on /level 3
>>>>quit
```

as - Autoconfiguration Status

The **as** (Autoconfiguration Status) command provides a brief summary of the status of autoconfiguration. **`Authentication Send completed`** means the command has completed.

Be sure to note the error count. If any errors are present you can look in the log files in **`C:\icm\<INSTANCE>\<PG>\logfiles`**, for example **`C:\icm\icm\pg1A\logfiles`** or look at the *autoconfigerror.txt* file which is available in **`C:\icm\<INSTANCE>\<PG>`** for example **`C:\icm\icm\pg1A`**.

Example output:

```
C:\Documents and Settings\torero>procmon icm PG1A pim1
>>>>as
Autoconfiguration Status Information
Total AutoConfiguration Errors = 0
Autoconfiguration Send completed
>>>>quit
```

dagent - Dump Agent

The dagent (dump_agent) command will show you the PIM's view of what the agents state is. The format is **`da {icmid}`**.

Note: The overall state show is inapplicable for Expert Advisor, the skill ActiveGroupAssignment states are the ones to investigate, for example if the agent is ready and assigned to a skill group, the **`ActiveGroupAssignment`** state should display as **`State=AS_AVAILABLE`**. If any don't match what the agent's assignment queue state is in Expert Advisor, then the logs need to be investigated to see what the PIM received from the Expert Advisor system.

Example output:

```
C:\Documents and Settings\torero>procmon icm PG1A pim1
>>>>dagent 1
HashIndex=49 SkillTargetID=5025 PeripheralNumber=1 ExtensionNumber=1(1)
ConfigExtension=-1(-1) InstrumentNumber=-1(-1)
     AgentDeskSettingsID=-1 ConfigSkillGroupIDSize=0
AgentPassword={enc:1}1B2M2Y8AsgTpgAmY7PhCfg==
   EnterpriseName=Runtime_PG_1.Cable.Clark Description= UserDeletable=N
   FirstName=Clark LastName=Cable LoginName=1
     ActiveGroupAssignmentSize=51 StateSize=51 DurationCurrentStateSize=51
     ActiveGroupAssignment[0] -        3 (0x3) Priority=0 State=AS_AVAILABLE
DurationState=0
     ActiveGroupAssignment[1] -        2 (0x2) Priority=0 State=AS_AVAILABLE
DurationState=0
     ActiveGroupAssignment[2] -        5 (0x5) Priority=0 State=AS_AVAILABLE
DurationState=0
     ActiveGroupAssignment[3] -       -1 (0xffffffff) Priority=255 State=AS_LOG_OUT
DurationState=0
     ...
    ActiveGroupAssignment[47] -       -1 (0xffffffff) Priority=255 State=AS_LOG_OUT
DurationState=0
    ActiveGroupAssignment[48] -       -1 (0xffffffff) Priority=255 State=AS_LOG_OUT
DurationState=0
    ActiveGroupAssignment[49] -       -1 (0xffffffff) Priority=255 State=AS_LOG_OUT
DurationState=0
    ActiveGroupAssignment[50] -       -1 (0xffffffff) Priority=255 State=AS_LOG_OUT
DurationState=0
               ConfigParam= SupervisorAgent=N
               ConfigParam= AgentLoginDisabled=N

       State                  =AS_AVAILABLE
       PrevalentState         =AS_AVAILABLE
       AcdLineState           =LS_IDLE
       InsideLineState        =LS_IDLE
       OutLineState           =LS_IDLE
       ConfXferLineState      =LS_IDLE
       ACDOutLineState        =LS_IDLE
       ACDConfXferLineState   =LS_IDLE
       ACDCallID              =-1
       InsideCallID           =-1
       OutBoundCallID         =-1
       ConfXferCallID         =-1
       ACDOutBoundCallID      =-1
       ACDConfXferCallID      =-1
       Line Information
           Extn:1/0 LT=LT_INBOUND_ACD  LS=LS_IDLE    SkGrp:0xFFFFFFFF CID=-1

>>>>quit
```

lc - List Calls

The **lc** (list_calls) command displays calls that are active. For the Expert Advisor system this means all calls that had a routing dialog for, but have not yet received a CALL_TERMINATION_EVENT message.

If there are no calls active on Expert Advisor and a lc reveals calls on the PIM generally that means that no CALL_TERMINATION_EVENT was received for that call.

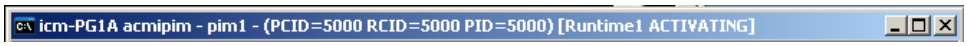
PG Troubleshooting Tips

PIM Not Activating

The Gateway PG is a part of Unified ICM so it is prone to ICM configuration errors that are unrelated to Expert Advisor. If the PG never goes into the ACTIVATING state (ACTIVATING is a transient state), then focus on finding out Unified ICM configuration errors.

- The title bar of the PIM process displays the current state. For example, the image below shows *Runtime1 ACTIVATING*. ACTIVATING is a transient state and should switch to ACTIVE once the runtime has been started.

  Figure 2: PIM Activating

- Check that the Peripheral and logical controller number correctly match between ICMSETUP (**`icm\bin\setup.exe`**) and those in the PG explorer.
- Are you looking at the right side (if the PG is duplexed)? The non active side will always be IDLE or CONFIGURED.
- Is the Expert Advisor runtime of the side in question up and ready to accept connections? If not, then investigate the problem on the runtime by analyzing the log file(s), starting the service, and so forth.

PIM not connecting – Stuck ACTIVATING

If the PIM is stuck in the ACTIVATING state:

- Verify Expert Advisor is up and running. (A timeout socket error will usually be observed in the log for this and the next two problems)
- Are the IP addresses in the A and B PIM correct for their respective primary and standby Expert Advisor runtimes. Also the A and B side Expert Advisors should match on each side (I.E. A side should point to A/A, B side should point to B/B.
- Is the Port correct in icm setup? The port should always be 42067.

- Has the ProtocolVersion registry setting for the PIM been changed to 13 if you are using a version of ICM prior to Unified ICM 7.5(1)? You will see an OPEN_REQ get sent but it will be rejected in the log for this failure.

PIM Connects but Autoconfiguration Incomplete or Other Errors

If the PIM is connected and Skill Groups are created on the Unified ICM, but no Services are configured, check if the '/ExtendedAgent' is specified in the configuration parameter field of the Peripheral tab in the PG explorer. Verify that the configuration parameter field of the Logical Controller is blank.

Autoconfig errors

If either the as procmon command (page 24) indicates there are auto-configuration errors (the process window also indicates errors) or the *autoconfigerror.txt* file exists, then there are autoconfiguration errors. The *autoconfigerror.txt* file is in the base PGn{a|b} directory, for example **`C:\icm\icm\pg1A`**), where icm is the instance name.

Examine the autoconfigerror.txt file. Generally it indicates what the problem is, for example a duplicate enterprise name. If it is a duplicate enterprise name it usually results from either a duplicate name on Expert Advisor (change it), or old unused records on ICM that have not been purged.

Periodically all *delete-able* records should be deleted from the Agent, Skill Group, and Service explorer. After deleting them they should be permanently deleted by using the Deleted Objects tool, select the items and then select 'Delete Permanently'. This tool can be found under Configure ICM/Administration.

Note that after deleting deleted-objects that the PG will need to be restarted to correct any errors.

Not purging deleted objects is acceptable, but realize that those items that had errors are not configured and may have an impact on routing (generally limited to configuration errors on skill groups/Assignment Queues).

Agents are not getting configured

If Expert Advisors on the system are not getting configured as agents on Unified ICM, look under the *Config* registry hive for the PIM (for example, **`HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\icm\PG1A\PG\CurrentVersion\PIMS\pim1\ACMIData\Config`**'). Verify that the EventMaskConfig key is 11 decimal.

Agents configured but no Historical agent data in Unified ICM

In the PG explorer, in the **Agent Distribution** tab, ensure that *enable agent reporting* is checked. Ensure also that there is at least one distributor site in the **Agent Distribution Entries** and one is enabled.

Ensure the name in the **Distributor Site Name** matches the name of the distributor. This can be checked by running \icm\bin\setup.exe on the distributor. Note that the name is not necessarily the host name of the machine. On the distributor the name can also be found as the key 'SiteName' in the ..\RealTimeDistributor\CurrentVersion' registry hive, for example **`HKEY_LOCAL_MACHINE\SOFTWARE\Cico Systems, Inc.\ICM\icm\Distributor\RealTimeDistributor\CurrentVersion\SiteName`**.

TCD Disposition 27's With Long Durations

If you see many TCD's on the Termination_Call_Detail table with disposition 27 and large durations (3600, 7200, etc.) it generally indicates missing TERMINATION_CALL_DETAIL records.

If needed search the PIM log for the call ID to ensure no TCD was received and then troubleshoot Expert Advisor.

Agent State Mismatch

If you encounter a situation where agent states on ICM seem to not match those on Expert Advisor use procmon dagent (page 24) for a single agent or the real time tables to confirm.

If they do not match look in the PIM log for the last AGENT_STATE_EVENT received for the agent in question.

If it matches the ICM values in procmon, pursue troubleshooting in Expert Advisor through the Gateway (ICM Gateway Process) to the Resource Manager (RM) to see if there is a configuration issue or a possible defect in Expert Advisor.

If it does NOT match what procmon displays, then pursue ICM problem diagnosis as this may indicate a defect in ICM.

ICM Gateway Process Troubleshooting Tips

ICM Gateway Process stuck on Starting

Verify the server ready by looking for SERVER_READINESS_UPDATE in the Runtime log. The Gateway does not come up until it is informed by the system infrastructure that the server is ready. (the readiness update is true), for example **`%MMCA_____ICMGW-6-SERVER_READINESS_UPDATE: %[ready=true]: Received server readiness update`**

View the available log files from the CLI: **`file list activelog mmca/logs/runtime`**

View the appropriate log file from the CLI: **`file view activelog mmca/logs/runtime/LOGILENAME`** .

Is the ICM Gateway on the runtime listening on the configured port? (Default: 42067).

Is the PIM started? Is the PIM in activating state? Is the other side of the PIM active (only one side can be active at any time)?

Is the PIM trying to connect to the right port (Default: 42067)? Check the port setting on the PIM, and it should match the ICM Gateway process on the runtime's listening port.

Can the runtime server and the PIM ping each other?

ICM Gateway Process goes OOS

Is the server readiness state changed to false? Search for SERVER_READINESS_UPDATE in the Runtime log.

View the available log files from the CLI: **`file list activelog mmca/logs/runtime`**

View the appropriate log file from the CLI: **`file view activelog mmca/logs/runtime/LOGILENAME`** .

If you see a false update (**`%MMCA__________ICMGW-6-SERVER_READINESS_UPDATE: %[ready=false]`**, then the Gateway is instructed by the Infrastructure to shut down.

Is the PG OK?

Did the other side of the PG take over?

Did the network go down?

Agent not shown in Agent Explorer

Search for INVALID_OAMP_AGENT_RECORD in Expert Advisor runtime log. If found, that agent record is not sent to ICM because of lack of ICMFirstName or ICMLastName.

Is there another agent with the same ICMFirstName and ICMLastName? The ICM uses an agent's name to uniquely identify the agent.

Is there an agent being deleted before having the same first/last name (as of a restriction in ICM auto-config library)?

Troubleshoot on the ICM side if none of the above is true.

Call failure

Does the ICM Gateway Process on the runtime server receive the routing request from the Contact Manager (CM)? Search for ROUTE_REQUEST in the Runtime log.

View the available log files from the CLI: **`file list activelog mmca/logs/runtime`**

View the appropriate log file from the CLI: **`file view activelog mmca/logs/runtime/LOGILENAME`** .

If not found, the call fails before it reaches the ICM Gateway Process on the runtime server.

Does the ICM Gateway process on the runtime receive the routing response from the PIM? Search for ROUTE_SELECT in the log. If not found, the call fails in the ICM.

Does the RouteSelected value in the ROUTE_SELECT log message match the Incoming label for the AQ to which the call is routed? If not, the call is routed to the wrong AQ.

ECC or peripheral variables not displayed to CUPC

Make sure the mapping (from ECC/peripheral variable to Expert Advisor attribute) is configured. It is configured in operations console in **Daily Management** > **Contact Attribute Sources**.

For ECC variables, make sure the name matches the name configured in ICM (this is case sensitive).

View the available log files from the CLI: **`file list activelog mmca/logs/runtime`**

View the appropriate log file from the CLI: **`file view activelog mmca/logs/runtime/LOGILENAME`** .

Look for NO_ATTRIBUTE_DEF_ID in Expert Advisor runtime log.

If found, either the mapping is not defined or the ECC variable name doesn't match what is defined in ICM.

Appendix A

Trace Definitions

Infrastructure Trace Definitions

Infrastructure Trace Definitions for Subsystems

Trace	Description
TRACE_HANDLED_EXCEPTION	Description of the exception and how it was handled
TRACE_JMX	JMX and management interface related traces.
TRACE_JMS	JMS and message bus related traces.
TRACE_HEARTBEAT	Related to heartbeats, heartbeat thread, or heartbeat send/received
TRACE_PARAM	For any parameters (not just method arguments)
TRACE_CALL	For traces related to a call / call processing
TRACE_MESSAGE	For general debug details of incoming/outgoing messages
TRACE_NOTIFICATION	Trace for notification api
TRACE_GENERAL_CFG	General traces for config api
TRACE_OOOQUEUE	Set this bit to enable OoOQueue tracing
TRACE_METHOD	When entering/exiting a method
TRACE_LOW_LEVEL	Bits and Bytes, etc

Runtime Server Subsystem Trace Definitions

Agent State Monitoring (ASM)

TRACE_ASM - Details on Agent State Monitoring

Reporting Adaptor (RA)

Trace	Description
CONFIG	Trace configuration
MSG_PUBLISHING	Trace message publishing
RAI_MESSAGE	Trace MPI messages
CEI_MESSAGE	Trace CEI Messages
SYSTEM	Trace global activity
REI_MESSAGE	Trace REI messages
REPORTING_ADAPTER	Trace reporting adapter

Intelligent Call Manager Gateway (ICMGW)

Trace	Description
CONNECTION	ACMI connection management tracing, including OPEN_REQ/OPEN_CONF, and CLOSE_REQ/CLOSE_CONF
AGENT_STATE_UPDATE	Agent State Update Trace Mask
AUTO_CONFIG	Auto-config Trace Mask
ROUTING	Routing Trace Mask
ILLEGAL	Illegal Message Trace Mask
REPORTING	Reporting Trace Mask
OAMP	OAMP Trace Mask
HEARTBEAT	Reporting Trace Mask

Work Assigner (WA)

Trace	Description
TRACE_CONTACT	Trace everything associated with a contact.
TRACE_MATCHING	Trace all match processing.
TRACE_RESOURCE	Trace everything associated with a resource.
TRACE_SENDMSGS	Trace all messages sent.
TRACE_RECVMSGS	Trace all messages received.
TRACE_DEBUG	Trace all debug events.
TRACE_STATE	Trace all state processing.
TRACE_QUEUING	Trace all queuing activity
TRACE_TRACKINGOBJECT	Trace everything associated with a tracking object.
TRACE_CONFIG	Trace all configuration related activity.
TRACE_TIMER	Trace all timer related events.
TRACE_ADMIN	Trace all admin events and responses.

Resource Manager (RM)

Trace	Description
ENDPOINT	For the Endpoint API tracing.
MPI_METHOD_ENTRY/EXIT	When entering/exiting a method in the MPI channel
MPI_MESSAGE	For general debug details of incoming/outgoing messages for MPI channel.
RDI_METHOD_ENTRY/EXIT	When entering/exiting a method in the RDI channel
ASSIGNMENT_QUEUE_ENTRY/EXIT	For the Assignment Queue API method entry/exit tracing.
CMI_MESSAGE	For general debug details of incoming/outgoing messages for CMI channel.
RESOURCE_METHOD_ENTRY/EXIT	For the Resource/Agent API method entry/exit tracing.
REI_MESSAGE	For general debug details of incoming/outgoing messages for REI channel.
TASK_METHOD_ENTRY/EXIT	For the Task API method entry/exit tracing.
CMI_METHOD_ENTRY/EXIT	When entering/exiting a method in the CMI channel
TASK	Traces for the Tasks in the core API.
CONFIG_METHOD_ENTRY/EXIT	When entering/exiting a method in the RDI channel
RESOURCE	Traces for Resources in the core API.
RDI_MESSAGE	For general debug details of incoming/outgoing messages for RDI channel.
INTERACTION_METHOD_ENTRY/EXIT	For the Interaction API method entry/exit tracing.
INTERACTION	For the Interaction API tracing.
MPI_CALL	For traces related to a call / call processing inside the MPI channel.
MPI_EVENTS	For internal events processed inside the MPI channel.
REI_METHOD_ENTRY/EXIT	When entering/exiting a method in the REI channel
WRI_EVENTS	For internal events processed inside the WRI channel.
WRI_MESSAGE	For general debug details of incoming/outgoing messages for WRI channel.
RESOURCE_EVENTS	For internal events posted or dispatched by the Resource API.
MESSAGE	For general debug details of incoming/outgoing messages
REI_EVENTS	For internal events processed inside the REI channel.
CONFIG_MESSAGE	For general debug details of incoming/outgoing messages for RDI channel.
RDI_EVENTS	For internal events processed inside the RDI channel.
ASSIGNMENT_QUEUE	Traces for Assignment Queues in the core API.
ENDPOINT_METHOD_ENTRY/EXIT	For the Endpoint API method entry/exit tracing.
WRI_METHOD_ENTRY/EXIT	When entering/exiting a method in the WRI channel

Contact Manager (CM)

Trace	Description
CONFIG	Trace config activity
BRE_MESSAGE	Trace BRE messages
CONTACT_MANAGER	Trace contact activity
MPI_MESSAGE	Trace MPI messages
SYSTEM	Trace global activity
CONTACT	Trace contact activity
KB_MESSAGE	Trace KB messages
PARTICIPANT	Trace participant activity
WA_MESSAGE	Trace Work Assigner messages
ICM_MESSAGE	Trace ICM Gateway messages
CONTACT_DETAIL	Trace CONTACT_DETAIL activity

Media Platform Interface (MPI)

Trace	Description
SIP_STACK_DSUTIL_THREAD	Only set this trace with the assistance of Cisco.
SIP_STACK_AUTHENTICATION	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_RESOLVER	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPMLAPI_CALLSTATE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT_ACK	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT_PRACK	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPMLAPI_CALLMANAGEMENT	Only set this trace with the assistance of Cisco.
SIP_STACK_CONFIG	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_CONNECTION	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LlSM	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPOBJECT_HEADER	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPMLAPI_REGISTRATION	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPREFER_REFER	Only set this trace with the assistance of Cisco.
SIP_STACK_DUMP	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LlSM_CLIENT	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPDIALOG_OFFERANSWER	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPMIME_MIME	Only set this trace with the assistance of Cisco.
MPI_CALL_TRACE	Only set this trace with the assistance of Cisco.
MPI_METHOD_TRACE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LlSM_SERVER_SWITCHSTATE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSUTIL_DSMESSAGESTATISTICS	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPHLAPI_HLCALL	Only set this trace with the assistance of Cisco.

Trace	Description
SIP_STACK_DSSIPLLAPI_CONNECTIONMANAGEMENT	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_CLIENT_SWITCHSTATE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_CLIENT_TIMERS	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_PERF	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPEVENTS_EVENTS	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_CLIENT_USERCB	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_WIRE	Only set this trace with the assistance of Cisco.
MPI_HANDLED_EXCEPTION_TRACE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPHLAPI_HLCALLMANAGEMENT	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT_CANCEL	Only set this trace with the assistance of Cisco.
MPI_PARAM_TRACE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT_REQUEST	Only set this trace with the assistance of Cisco.
MPI_LOW_LEVEL_TRACE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSUTIL_SOCKET	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONKEY	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_TRANSACTIONMANAGEMENT_RESPONSE	Only set this trace with the assistance of Cisco.
SIP_STACK_EXCEPTION	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_SERVER_USERCB	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_SERVER_TIMERS	Only set this trace with the assistance of Cisco.
SIP_STACK	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPOBJECT_MESSAGE	Only set this trace with the assistance of Cisco.
SIP_STACK_DSSIPLLAPI_LISM_SERVER	Only set this trace with the assistance of Cisco.

Resource Desktop Adaptor (RDA)

Trace	Description
CONFIG	Config trace bit is used to trace the RDA configuration issue with the database including loading, updating, deleting the message set, initial setup configuration properties, expert advisor configuration properties.
IM_ACTIVITY	IM activity is a place holder for future IM activity. Currently, no trace is used by this trace bit.
MPI_MESSAGE	MPI message trace bit is used to trace the RDA JMS message exchange between the MPI layer. MPI message trace bit is used to trace the RDA JMS message exchange between the MPI layer. MPI layer including the agent presence subscription and notification, system user publication, registration to the presence service. It also indicates the condition of the IM message exchange between the expert advisor and the system.

Trace	Description
SYSTEM	System trace bit is used to trace the RDA subsystem status such as whether the system is in partial service, out of service or in service It also trace the error condition like topic issue.
REI_MESSAGE	RDI message trace bit is used to trace the RDA JMS message exchange between the REI protocol.
PRESENCE_ACTIVITY	PRESENCE_ACTIVITY trace bit is a place holder for future PRESENCE activity. Currently, no trace is used by this trace bit.
PARSER	PARSER trace bit is place holder for any PARSER activity. Currently, no trace is used by this trace bit.
RDI_MESSAGE	RDI message trace bit is used to trace the RDA JMS message exchange between the RDI protocol. RDI message trace bit is used to trace the RDA JMS message exchange between the RDI protocol. It mainly indicates the condition of the IM message exchange between the expert advisor with the RM subsystem including offerTaskRequest, re-prompting, taskAssignCmd and resource state change request.

Reporting Server Subsystem Trace Definitions

Reporting Subsystem (RS)

Trace	Definition
EXTRA_DEBUG	Only set this trace with the assistance of Cisco.
DETAILED_DEBUG	Only set this trace with the assistance of Cisco.
DEBUG	Only set this trace with the assistance of Cisco.

ORM Server Subsystem Trace Definitions

ORM (OAMP Resource Manager)

Only set these traces with the assistance of Cisco.

OAMP Server Subsystem Trace Definitions

OAMP (OAMP)

Trace	Definition
TRACE_BULK	To control logging for looping/bulk operations
TRACE_GENERAL_UI	For tracing the general OAMP UI
TRACE_EXCEPTION	For tracing Exceptions
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods

Common Subsystem Trace Definitions

Infrastructure

Trace	Description
TRACE_STATS	Operations of the Stats Manager
TRACE_SERVICEABILITY	Traces to do serviceability, the act of logging and tracing
TRACE_THREAD	All Infrastructure thread operations
TRACE_SNMP	TRACE_SNMP SNMP Forwarder/logging/stats
TRACE_SHUTDOWN	Log detailed shutdown info
TRACE_LICENSING	Log any/all licensing operations
TRACE_STARTUP	Log detailed startup info
LOAD_SUBSYSTEM	When loading subsystems
TRACE_TIMER	Logs when a Timer expires

OAMP_BO

Trace	Description
TRACE_BULK	To control logging for looping/bulk operations
TRACE_EXCEPTION	For tracing Exceptions
TRACE_GENERAL_BO	General Traces for OAMP back-end
TRACE_PARAM	For tracing Parameters
TRACE_DBACCESS	Trace DB Access for db fetch and modify such as Save, Update, Delete
TRACE_METHOD	For tracing of Entry/Exit of Methods