Contact Center Trace Levels

- Trace Levels, on page 1
- EMS Log Compression, on page 8
- Set Router Tracing, on page 9
- Set INCRP NIC and NetworkCIC Tracing, on page 10
- How to Set OPC Tracing, on page 11
- How to Set Unified CCM PIM Tracing, on page 12
- How to Set JTAPI Gateway Tracing, on page 13
- How to Set CTI Server Tracing, on page 13
- Setting VRU PIM Tracing, on page 14
- Setting Outbound Option Tracing, on page 15
- Trace File Retention Settings, on page 16
- Router Full Dump Enabled by Default, on page 17

Trace Levels

Support personnel who debug the Unified Communication solution need not know the details of trace levels across Unified Communication solution applications. If debugging a problem requires more detailed debug information, three levels of trace setting exist that can map internally to a particular application or application component. The intent is not to revamp existing trace setting values but to map the levels to the relevant and existing trace settings for a particular component. Use the following defined trace levels with the Diagnostic Framework Portico and the Unified System CLI tools.

The following trace levels are defined for the Unified Communication solution:

Trace Level	Trace Value	Description
Default	0	Default install, should have no or minimal performance impact
Warning	1	Log more detailed (plus default level) trace messages, small performance impact
Error	2	Log more detailed (plus warning and default level) trace messages, medium performance impact
Debug	3	Log most detailed (plus error and warning and default level) trace messages, high performance impact.

Note If you have enabled the debug trace levels, disable them after collecting the logs to avoid an unnecessary performance impact to your solution.

If the trace level does not match any of the defined levels, it displays custom (99).

Most EMSTraceMasks are based on this registry key: `HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<Instance>\<Component>\EMS\CurrentVersion\Library\Processes\<process>\EMSTraceMask`

Get and Set trace level and collect trace files are supported only for the following processes.

Note If the trace mask is the same for multiple levels, the GetTraceLevel returns the highest level. For example, GetTraceLevel returns Level 3 for Logger/baimport.

Trace–All Nodes

You can set trace levels on these processes:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
NM	0x00	0x0F	0x0F	0xFF
NMM	0x00	0x0F	0x0F	0xFF

The Diagnostic Framework does not support the Administrator Workstation.

Trace–Administration and Data Server

You can set trace levels on these processes for the Administration and Data Server:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
CONFIGLOGGER	0x00	0x0F	0xFF	0xFFF
CMSNODE	0x00	0x00	0x00	0xFFFFFFFF
CMS_JSERVER	0x00	0x00	0x00	0xFFFFFFFF
REPLICATION	0x00	0x0F	0xFF	0xFFF
RTCLIENT	0x00	0x0F	0xFF	0xFFF
RTDIST	0x00	0x0F	0xFF	0xFFF
UPDATEAW	0x00	0x0F	0xFF	0xFFF

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
ISEMAN	0x00	0x00	0x00	0x01

Note The minimum and default trace level for the CMS, CMSJServer and ISE components is 2.

Trace–Router

You can set trace levels on these processes for the Router:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)	Notes
Agi	0x00	0x01	0x07	0x3F	—
ccagent	0x00	0x03	0x0F	0xFF	—
dbagent	0x00	0x01	0xFF	0xFF	—
DBWORKER	0x00	0x01	0xFF	0xFF	—
mdsproc	0x00	0x07	0xFF	0xFF	—
rtr	0x00	0x0F	0xFF	0xFFF	—
ROUTER *	Route Requests	Route Requests	- Network VRU - Trans Route - VRU Bank - CIC Request - Script Select	- Call Queuing - Agent changes - Call Type Real Time	In case of RTRTRACE or RTRTEST Note: If you restart the Router process, the settings return to the default level.

Trace–Logger

You can set trace levels on these processes for the Logger:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3(Debug)
BAIMPORT	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF
CAMPAIGN MANAGER	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF	0xFF EMSUserData = 0xFFFF
CONFIGLOGGER	0x00	0x0F	0xFF	0xFFF
CSFS	0x00	0x00	0x00	0xFF
CW2KFEED	0x00	0x00	0x00	0x07
DTP	0x00	0x04	0x06	0x0F
HISTLOGGER	0x00	0x0F	0xFFF	0xFFF
RECOVERY	0x00	0x0F	0xFFF	0xFFF
REPLICATION	0x00	0x0F	0xFFF	0xFFF

Trace–Peripheral Gateway

You can set trace levels on these processes for the PG:

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
JTAPIGW *	JT_JTAPI_EVENT_ USED JT_TPREQUESTS JT_PIM_EVENT JT_ROUTE_ MESSAGE	JT_CONNECTION *CONF*	JT_JTAPI* JT_HEX JT_ROUTE* JT_TERM* JT_LOW*	JT*
MDSPROC	0x00	0x07	0x0F	0xFF
MSGIS	0x00	0x00	0x00	0x3F
OPC **	Default, cstacerEMSTraceMask = 0x40	agent, inrcmsg, closedcalls, tpmsg, routingEMSTraceMask = 0x40 Note: Remove "default" tracing set in Default(0) level, but include cstacer.	Calls, NCT, simplified EMSTraceMask = 0x40Note:Remove "default" tracing set in Default(0) level, but include Level 1.	Missingdata, halfhour EMSTraceMask = 0x40Note: Remove "default" tracing set in Default(0) level, but include Level 2.

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
PGAGENT	0x00	0x03	0x0F	0xFF
EAGTPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph* jtapi_dialed*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid jtapi*
VRUPIM	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 00000000000000000000 000000000180	EMSTraceMask= 0x0 EMSUserData= 0x71f7e0 00000000000000000000 00000000000000000000 00000000000000000000 000000000180	EMSTraceMask= 0x0EMSUserData= 0xf1fff0 00000000000000000000 00000000000000000000 00000000000000000000 000000000000180
ARSPIM *	tp* precall *event csta* call_object teld_agent_state opcrequest	periph*	autoconfig* teld* call_match_timing timer*	lock* universal* service* threadid
MRPIM	EMSUserData = 0x00 Procmon: > trace mr* /off **Note** Level 2 is the default level for MRPIM.	EMSUserData = 0x40 Procmon: > trace mr* /off > trace mr_msg_comm_session /on	EMSUserData = 0x58 Procmon: > trace mr* /off > trace mr_msg_comm_session /on > trace mr_*_mr /on	EMSUserData = 0x5F Procmon: > trace mr* /off > trace mr_msg_comm_session /on > trace mr_*_mr /on > trace mr_*_inrc /on > trace mr_*_csta /on
CTISRVR	0x000000f0	0x000000f6	0x000000fe	0x000000ff
BADIALER	EMSTraceMask= 0x0000003f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000003f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000007f EMSUserData= 0xFFFF	EMSTraceMask= 0x0000007f EMSUserData= 0xFFFF

Note Ensure that debug mode is not enabled during peak hours to prevent any adverse impact on system efficiency.

Trace–Web Setup

You can set trace levels on the Web Setup process.

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)
Web Setup	EMERGENCY	CRITICAL	WARNING	DEBUG

Websetup uses log4j.net for logging. Websetup uses a XML file (log4j.xml) through which you can set the trace levels. The XML file also contains other information you require for logging.

You can find the log4j.xml file here: <InstallDrive>:\icm\tomcat\webapps\setup\WEB-INF\classes\log4j.xml

Trace–Diagnostic Framework

You can set trace levels on the Diagnostic Framework.

Process	Level 0 (Default - Error)	Level 1 (Warning)	Level 2 (Informational)	Level 3 (Debug)	Notes
Diagnostic Framework	Info	Info	Info	Debug	

When the Diagnostic Framework receives a request for its own trace level, if the trace level is at Info, Level 2 is returned. When the Diagnostic Framework receives a request to be set for Level 0, Level 1, or Level 2, the trace level is set to Info.

Trace–SADLib

You can set trace levels on SADLib.

Process	Trace Level	Trace Value	Description
SADLib	0	NO	No logs are generated.
	1	WARNING	The Warning and Error logs are generated.
	2	INFO	The Warning, Error, and Info logs are generated.
	3	DEBUG	The Warning, Error, Info, and Debug logs are generated.

Reference Tables

Regarding JTAPI logging,

Jtapi uses EMSUserData value default (OX49E2) to control logging, we can enable/disable JT_ bits using procmon (trace command). JT_ maps to below tables values which is masked with EMSUserData to control tracing.

Process	Level 0 (Default - Error)
JT_HEARTBEATS	1
JT_TPREQUESTS	2
JT_HEX	3
JT_JTAPI*	4-7
JT_CONNECTION	8
JT_PIM_EVENT	10
JT_ROUTE*	11-12
JT_LOW_LEVEL*	13-14
JT_CONF_XFER	15
JT_TERM_EVENT_RTP	16
JT_DEBUG	17

Regarding MRPIM logging

Similar to jtapi, mrpim default EMSUserData is 0xD8, we can enable/disable mr* bit using procmon(trace command)

Process	Level 0 (Default - Error)
mr_msg_config	1
mr_msg_comm_session	2
mr_heartbeat_messages	3
mr_msg_incoming_mr	4-7
mr_msg_outgoing_mr	8
mr_msg_incoming_inrc	10
mr_msg_outgoing_inrc	11-12
mr_msg_outgoing_csta	13-14
mr_function_call	15
mr_outgoing_opc	16

EMS Log Compression

To collect logs that span a greater period of time, EMS log files from the following PG components are zipped:

- Router
- OPC-CCE
- OPC-TDM
- CTISVR
- EAGTPIM
- JTAPIGATEWAY
- VRUPIM
- BADIALER
- MRPIM

Note These are the only components that currently support EMS log compression.

Dumplog

Dumplog handles the compressed EMS files and can be used in the general way. Dumplog looks for gzip.exe in <Install Drive>\icm\bin to unzip compressed EMS files before dumping logs. To dump logs from compressed EMS files (with .gz extension) outside of a PG, unzip the EMS files before you use dumplog.

EMS File Compression Control

Use the EMSZipCompressionEnabled registry key in \EMS\CurrentVersion\Library\Processes\<process name> to enable or disable compression of EMS log files. Do not modify this registry key. This key takes effect only on components that support EMS file compression.

Other Registry Keys

The following two other registry keys are also available in …\EMS\CurrentVersion\Library\Processes\<node name>

EMSZipFormat
EMSZipExtension

Note Do not modify these registry keys.

Set Router Tracing

To set the CCE Router, use the Router Trace utility. This utility is a single-form Windows GUI utility that is loaded on the Unified CCE server.

Note The router process must be running before you set router tracing or attempt to retrieve router traces. This requirement applies to any tool which sets or retrieves router tracing, including, for example, RTTEST, RTRTRACE, and System CLI. (The router process must be running because the router trace settings are only stored in memory).

Note Business Hours tracing has to be set or reset using RTR Trace utility or RTTEST utility only. Setting the trace level for Router in Diagnostic portico will not change the Business Hours setting.

All trace settings using “RTRTRACE” take effect immediately in the Router.

You can observe specific status of call routing, call type, skill group, and schedule target variables using the following RTTEST command: `rttest /cust <instance>/node <node>`.

You can monitor a particular variable and determine if its value is incremented or decremented by enabling the RTTEST “watch” command on router logs: `rttest: watch <variable>`.

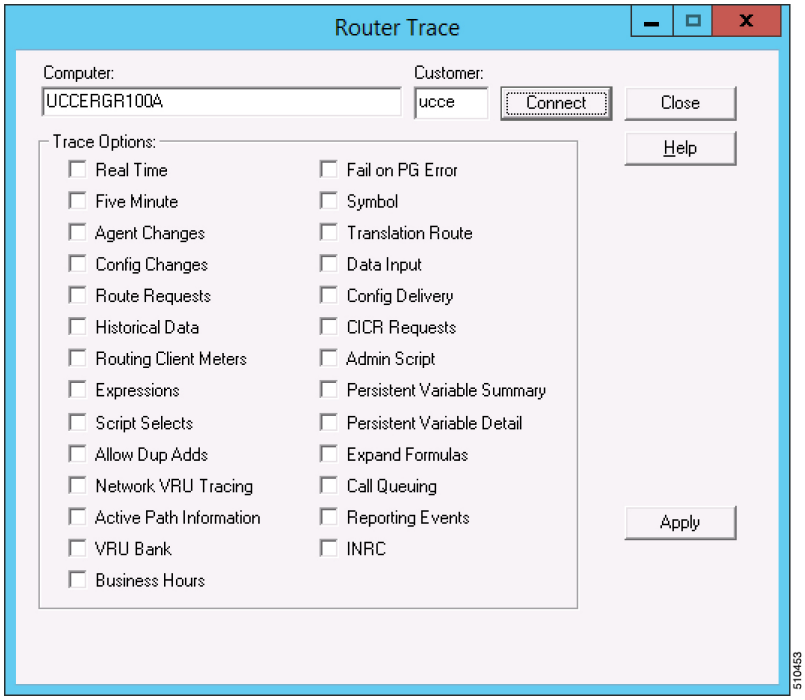
The logs are written only when value is changed.

Procedure

Step 1 Connect to server through remote desktop or go to local console.

Step 2 Run command **C:> \icm\bin\rtrtrace** to invoke RTRTRACE from ICM\BIN

Figure 1: Router Trace Utility



Step 3 Set trace options.

When a call routing failure occurs, the basic traces should at the minimum be “Route Requests” and “Translation Route” if you use translation routing.

Also, enable the other tracing depending on the specific problems you see.

For...	Enable...
Any type of VRU	**Network VRU Tracing**
ICM to ICM Lookup or Contact Director	**CICR Requests**
Suspected queuing issues	**Call Queuing**
Reporting events problems	**Reporting Events**
Agent issues	**Agent Changes**
Business Hours problems	**Business Hours**

Set INCRP NIC and NetworkCIC Tracing

To reset the trace levels for both Unified CCE INCRP NIC and Unified CCE NetworkCIC, use the Microsoft Registry Editor (regedit) and modify the trace mask saved in the Windows registry.

Table 1: Setting INCRP NIC Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems,Inc.\ICM\<instance>\<RouterA/B>\EMS\CurrentVersion\Library\Processes\incrpnic
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\ucce\RouterA\EMS\CurrentVersion\Library\Processes\incrpnic
Item	EMSTraceMask
Value	0 (hex). This is the default value. For debugging call flows, it is 200 (hex).

Table 2: Setting NetworkCIC Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\<RouterA/B>\EMS\CurrentVersion\Library\Processes\cic
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\ucce\RouterA\EMS\CurrentVersion\Library\Processes\cic
Item	EMSTraceMask
Value	0 (hex). This is the default value. For debugging call flows, it is 200 (hex).

How to Set OPC Tracing

To set Unified CCE OPC tracing, use the OPCTEST utility. This is a command-line utility and you require remote desktop or local console access.

Command Syntax (launch):

```
C:> opctest /cust <instance> /node <node>
```

Where <instance> is the Unified CCE instance name and <node> is the desired node name (for example, /cust cust1 /node PG1A).

After you invoke the instance name, you are presented with an opctest: prompt where you can enter commands according to the syntax expected. To display all commands, enter a "?" at the opctest: prompt. However, OPCTEST is a powerful utility and if you use it incorrectly, it can have a negative effect on a production system in operation. Do not run a command against a production system unless you are absolutely certain of the impact it can introduce.

Use the following commands to alter default trace levels. Before using the commands, understand your current utilization to ensure there is sufficient capacity to accommodate the added tracing.

General Diagnostics

```
opctest:debug /on
```

Diagnosing Network Transfer Issues

```
opctest:debug /on
opctest:debug /NCT
```

Note Dialog ID in network transfer call flows appear as a negative number in OPC logs. This is applicable for other components like Router and VRU PIM as well. This is to ensure that Router generated DialogID's do not conflict with DialogID's originated from the pre-routing client (also referred to as NIC DialogID). This pre-routing client can either be a NIC or a VRU PIM integrated with CVP. While the router-assigned DialogID can be any unique number with the most significant bit set, the router will use the expired NIC DialogID value as a troubleshooting aid.

Diagnosing Multimedia Issues

```
opctest:debug /on

opctest:debug /task /passthru
```

Diagnosing VRU PG Issues

```
opctest:debug /on
opctest:debug /passthru
```

The default is:

```
opctest:debug /routing /agent /closedcalls /cstacer /rcmsg /tpmsg /simplified /inrcmsg
```

and

```
EMSTracemask = 0x40
```

EMSTracemask is reset in the Windows registry.

TAC directs you to alter or add additional tracing based upon the analysis of collected logs.

How to Restore Default Trace Levels

```
opctest:debug /on
```

This parameter turns on the /default tracing, modifies the EMSTracemask to 0x40, and turns off all other enabled tracing.

How to Display Trace Levels

```
opctest:debug /showtrace
```

This parameter displays current trace levels enabled on the peripheral.

How to Set Unified CCM PIM Tracing

To reset trace levels with the Unified Communications Manager Peripheral Interface Manager component (for example, “EAGTPIM”), use the ProcMon (process monitoring) utility. This is a command-line utility and you require remote desktop or local console access.

Table 3: Setting Unified CCM PIM Tracing

Command Syntax (launch)	C:> ProcMon <instance> <node> pim<pim number>
Example	C:> ProcMon acme PG1A pim1
Commands	>>>debug /on

How to Set JTAPI Gateway Tracing

To reset trace levels for the Unified Contact Center JTAPI (Java Telephony Applications Programming Interface) Gateway component (for example, "JTAPIGW"), use the ProcMon (process monitoring) utility. This is a command-line utility and you require remote desktop or local console access.

Table 4: Setting JTAPI Gateway Tracing

Command Syntax (launch)	C:> ProcMon <instance> <node> jgw<jtapigw number>
Example	C:> ProcMon acme PG1A jgw1
Commands	>>>trace* /off >>>debug /on

How to Set JTAPI Gateway Default Tracing

The default tracing for JTAPI gateway consists of a set of tracing levels that currently exist.

To enable only the default tracing, enter the following commands in ProcMon:

trace * /off

Note: debug /on does not turn off non-default tracing so you need this first.

debug /on This enables only default tracing.

To turn off debug tracing, enter the following command in ProcMon:

debug /off This turns off only default tracing. All other tracing is not affected.

How to Set CTI Server Tracing

To reset trace levels with the Unified CCE CTI Server (for example, CTI Gateway or CG), use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Table 5: Setting CTI Server Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\<CG#A/B>\EMS\CurrentVersion\Library\Processes\ctisvr
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\CG1A\EMS\CurrentVersion\Library\Processes\ctisvr

Item	EMSTraceMask
Value	F0 (hex) This is the default value. The value of F0 provides sufficient tracing information to troubleshoot most issues.

Setting CTI Server Default Tracing

The default tracing level for CTI Server is EMSTraceMask = 0xF0. Do not enable any other tracing at the default trace level. EMSUserData should be NULL.

ProcMon debug commands:

debug /on sets the EMSTraceMask to the default value of 0xF0 and NULL out EMSUserData. No other command is needed to set default tracing.

debug /off sets EMSTraceMask to 0x00 and NULL out EMSUserData.

Setting VRU PIM Tracing

Resetting trace levels with the Unified CCE VRU Peripheral Interface Manager (PIM) is accomplishing by altering the trace mask and user data values saved in the Windows registry. Use the Windows REGEDIT utility to change these numeric values.

Table 6: Setting VRU PIM Tracing

Registry Key	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\PG<PG number><A or B>\EMS\CurrentVersion\Library\Processes\pim<pim number>
Example	HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\acme\PG2A\EMS\CurrentVersion\Library\Processes\pim1
Item	EMSUserData
Value	7F F7 E0 (hex)
Item	EMSTraceMask
Value	0 (zero)

When you collect the trace logs, collect both VRU PIM trace logs and the VRU trace capture file. To obtain VRU trace capture files, run the VRUTRACE tool in the following directory:

\icm\<inst>\<pg><pg number><a or b>\vrucap

For example: \icm\acme\pg2a\vrucap

Setting VRU PIM Default Tracing

The default tracing for VRU PIM consists of a set of tracing levels that currently exist.

ProcMon debug commands:

debug /off turns off all tracing

debug /on enables default tracing only and turns off any previously enabled tracing

Setting VRU PIM Capture

Normally, the VRU Trace tool can collect only the completed VRU CAP files, not the files that are still in memory or actively being written.

If the VRU CAP file is still being buffered, the file is not present in the directory and cannot be collected by the VRU Trace tool.

To obtain VRU CAP files, do the following:

Procedure

Step 1 Run the VRU TRACE tool in the following directory: `\icm<inst><pg>\vrucap`

Step 2 To obtain the latest VRU CAP files, do the following:

a) Navigate to the VRU CAP directory: `C:\icm\<instance>\<pg><pg number>\vrucap`

b) Flush the buffered data into a VRU CAP file by running the following command: `vrutrace pim<pg number> /debug /last /o`

c) Capture a trace for a specific time window by running the following command: `vrutrace pim<pg number> /debug /bt hh:mm:ss /et hh:mm:ss /o`

Note
Using **/last** ensures that all buffered data is written to the VRU CAP file before you run the timed trace with **/bt**.

Setting Outbound Option Tracing

The utility tools provide centralized control to set up each component trace level. Additionally, you can manually modify the registry key values.

How to Reset CampaignManager Tracing

To reset CampaignManager trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager

Example:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\m3pc1\LoggerA\EMS\CurrentVersion\Library\Processes\CampaignManager

How to Reset baImport Tracing

To reset baImport trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\LoggerA\EMS\CurrentVersion\Library\Processes\baImport

Example:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\m3pc1\LoggerA\EMS\CurrentVersion\Library\Processes\baImport

How to Reset Dialer Tracing

To reset Dialer trace levels, use the Microsoft Registry Editor (regedit) to modify the trace mask saved in the Windows registry.

Registry Key:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\Dialer\EMS\CurrentVersion\Library\Processes\baDialer

Example:

HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\m3pc1\Dialer\EMS\CurrentVersion\Library\Processes\baDialer

Trace File Retention Settings

You can modify several Windows registry values to adjust the trace log retention parameters, for example, increase the amount of trace data – extend the trace retention window. To modify the trace log parameters, use the Microsoft Registry Editor (regedit).

Unified CCE Event Management System (EMS) tracing is stored in a binary format in a set of files in a directory on the local drive following a specific structure.

Trace log file location

[Drive]:\icm*<instance>**<node>*\logfiles

Example

C:\icm\acme\pg1a\logfiles

Trace log file names

Process_YYMMDD_HHMMSS.ems

Example

opc_090713_123025.ems

This is an OPC trace log file that was created 13 July, 2009 at 12:30:25.

Under the control of the Event Management System, the following rules apply while traces are written to the trace log files:

- If the size of this file is greater than or equal to the maximum (configured) size that a single EMS trace log file is allowed, the file is closed and a new file is created.

- If the maximum number of trace log files for this process is greater than the maximum (configured) number of trace log files, then the oldest trace log file is deleted.
- If the total combined size of all process trace log files is greater than or equal to the maximum (configured) total size of all process trace log files, then the oldest trace log files are deleted until the total size is less than the configured maximum size.

Registry Items

You can change the following registry item values to increase or decrease the amount of disk space allocated for a single process.

Registry key

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\<instance>\<node>\EMS\CurrentVersion\
Library\Processes\<process>
```

Example

```
HKLM\SOFTWARE\Cisco Systems,
Inc.\ICM\acme\PG1A\EMS\CurrentVersion\Library\ Processes\opc
```

Items

EMSLogFileMax

The maximum size, in bytes, of a single trace log file for this process.

EMSLogFileCountMax

The maximum number of trace log files permitted for this process.

EMSAllLogFilesMax

The total space allowed for all trace log files (combined size) for this process.

Note EMSLogFileMax multiplied by EMSLogFileCountMax may be greater than EMSAllLogFilesMax and it often is by default; this is to ensure trace log files created by frequent process restarts (where a number of small trace log files are created) are not lost when the max count is exceeded but very little disk space is used. EMSAllLogFilesMax is used to guarantee that under any circumstances, the maximum amount of disk space allocated is never exceeded.

The default values of these items are evaluated with every release of the Unified CCE to determine the optimal limits based on disk usage of the application and typical disk capacity of servers available at the time of release. In nearly all cases, the default values are increased over time as disk drive sizes increase.

Router Full Dump Enabled by Default

In Release 10.0(1), router full dump is enabled by default. This change to the default setting is intended to provide more information to help troubleshoot the issue if a critical process crashes.

The registry key that sets this default is **EMSGenerateSmallMemoryDump**, which is located here: `HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<instanceID>\RouterA\EMS\CurrentVersion\Library\Processes\rtr`.

The value of 0x20000032 for this registry key indicates a router full dump will be generated. To generate a mini-dump rather than a full dump, change the last digit to 1 so that the value is 0x20000031.

The middle six digits of the registry key value determine the number of dumps that are kept. If, for example, these digits are all zeros (0x2**000000**2), CCE by default keeps only the last five generated dumps for any component. For the CCE router, however, only the three latest dumps are kept (0x2**000003**2) by default, since the size of the full dump can be up to 2GB. Keep disk space usage in mind when selecting the number of dumps you want to retain.

If the CCE Router crashes, provide the full dump (the `.mdmp` file generated under the `icm\<instanceid>ra\logfiles` directory), the PDB file (for example, `router.pdb`) from the `icm\bin` directory, and the associated executable (`router.exe`) from the `icm\bin` directory.

Note The registry key value is set to the default value of 0x20000032 on a new install or upgrade, or whenever you run Web Setup.