Troubleshooting Foreign System Interfaces Inbound

Troubleshooting interfaces require a methodical approach, knowledge of interface messaging, and a good understanding of the *Cerner Millennium* architecture. This document provides you with basic methods to investigate some of the common problems encountered. It details specific strategies and tools for troubleshooting interfaces when receiving a transaction from a foreign system to posting the information in the database. It also provides additional architecture information, which assists in the troubleshooting process.

Overview of the Troubleshooting Process

1. Identify the problem.
2. Perform troubleshooting steps.
3. Resolve the issue or log a service request.

Identify the Problem

When you receive an error, ask the following questions:

- Can you reproduce it?
- Are you the only user that receives the error?
- Do you receive the error on multiple computers?
- Can you reproduce the error in another environment?
- What type of installation does the PC have: local, network, or *Citrix*?
- What type of error is it?
    - Types of errors include script errors, illegal operation errors, and information errors.
        - If you receive a script error, note the script name.
        - If the error contains multiple tabs, copy the data on each tab, or print a report from the error if the print option is available. This information could be useful if you need to log a service request.

Perform Troubleshooting Steps

You have determined the error is reproducible. To reproduce an error, you must use the exact keystrokes that were used when the error was initially received. Begin troubleshooting by asking the following questions:

- If you alter the steps slightly, do you still receive the error?
- Is this the intended use of the application or tool?
- Did you check the eService Knowledge Base?
- Are all servers running?

If you think you will be logging a service request, capture a screen shot of the errors, as this aids in troubleshooting.

Resolve Issue or Log a Service Request

Most of the time you can resolve your own issues, however if assistance is required to achieve resolution you can log a service request.

IRC/SWx Support

If you are unable to resolve an issue, SolutionWorks and the Immediate Response Center (IRC) are available to assist you.

- SolutionWorks is staffed Monday through Friday from 0700 to 1900 (Central Time). You can contact SolutionWorks at (816) 221-9009.
- The Immediate Response Center is staffed 24 hours a day, 7 days a week. It handles critical system issues or noncritical issues that occur when SolutionWorks is not staffed. You can contact the Immediate Response Center at (816) 221-8877.

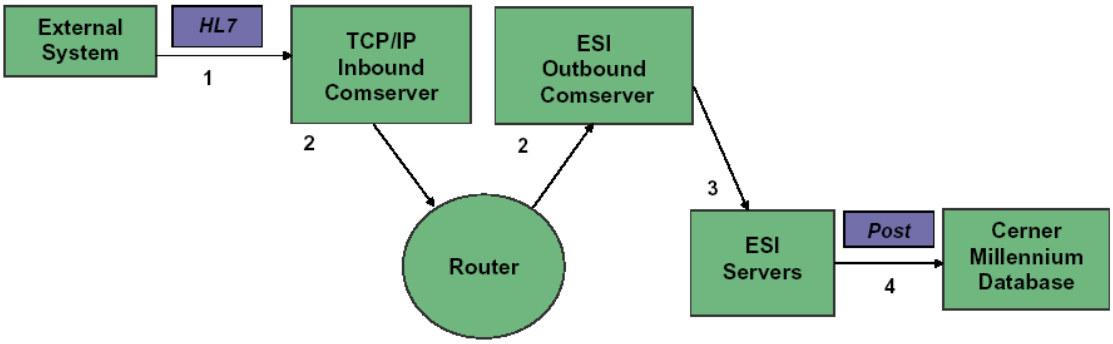
For noncritical issues, send a service request in an e-mail to SVCREQ@cerner.com (a request is logged by a call coordinator and a request number is returned to you), or you can log the request through Cerner.com.

Troubleshooting Workshop

© Cerner Corporation and affiliates. All rights reserved. Contains Cerner confidential and/or proprietary information belonging to Cerner Corporation and/or its related affiliates which may not be reproduced or transmitted in any form or by any means without the express written consent of Cerner. Use may be subject to the "DHMSM License and Distribution Restrictions" in the Terms of Use (http://www.cerner.com/Terms_Of_Use/). The Terms of Use contain restrictions on use and distribution of this content, including use and distribution restrictions applicable to DHMSM and other government users.

Process Flow

The numbered steps in the following flow chart correspond to the steps in the Troubleshooting Workshop below.



When troubleshooting on the inbound, the first step is to determine if the communication is occurring between the foreign system and *Cerner Millennium*. When troubleshooting communications, first determine where the breakdown in communication occurred. Did it occur between the foreign system and the engine, the engine and *Cerner Millennium*, or when there is not an engine between the foreign system and *Cerner Millennium*? Once this is identified, determine if the breakdown was on the foreign system, the interface engine, or the *Cerner Millennium* system.

Steps:

Step	Description
1	Determine if the Transaction Reached the Inbound Communications Server
2	Determine if the Transaction Reached the ESI Outbound Comserver
3	Determine if the CPM ESI Server Processed the Transaction
4	Determine if the Transaction Posted to the Database

Step 1 - Determine if the Transaction Reached the Inbound Communications Server

1. Check the OEN_TXLOG utility.
   When processing transactions, the first thing the Cerner system does is log the transaction to OEN_TXLOG. To make sure *Cerner Millennium* received the transaction, look in Search (the OEN_TXLOG utility) using SI_Manager (SI_Manager.exe) for the transaction. Before viewing the OEN_TXLOG utility, ensure that you know the communications server (comserver) with the issue.
   If the transaction is not in the OEN_TXLOG_VIEW, then the transaction was not received by *Cerner Millennium*. This could be because the issue is on the foreign system, the communication server is not running, or there is a network issue.

2. Verify that the inbound comserver is running.

   To determine if the comserver is not running, look in the Controller screen of OpenView (OpenView.exe) or in the Server Control Panel (SCP). When you log in to OpenView, on the Controller view lists the servers with the domain to which you are logged in. The domain is noted in the lower right corner. Once you are in the correct domain, find the comserver for the interface that is not communicating. If there is a red X to the left of the inbound comserver, it is not running. To start the comserver, right-click the comserver and select **Start** or click the **traffic light**. The red X should be replaced with a green circle. If the green circle is not displayed after a few moments, or if the circle changes back to a red X, there is a problem with the comserver.

3. Check for communication errors.

   Check the MsgView utility (msgview or MsgView.exe) or for communication errors. The error lists the comserver and the communication step in which the error occurred. Communication steps are represented by the letters O, G, I, Q, R or X. See the Open View Help for an explanation of errors and suggested resolutions.

4. For TCP or IP Connections, verify the address and port.

   When using a TCP or IP connection, ensure that the correct TCP or IP address and port are being used and that they are available. To view the TCP or IP address and port being used, right-click the comserver in the Controller view and select **Process Config** on the Communications tab, select the

© Cerner Corporation and affiliates. All rights reserved. Contains Cerner confidential and/or proprietary information belonging to Cerner Corporation and/or its related affiliates which may not be reproduced or transmitted in any form or by any means without the express written consent of Cerner. Use may be subject to the "DHMSM License and Distribution Restrictions" in the Terms of Use (http://www.cerner.com/Terms_Of_Use/). The Terms of Use contain restrictions on use and distribution of this content, including use and distribution restrictions applicable to DHMSM and other government users.

Service Specs option. Ensure that the port, which is all that is needed for inbound, is the same for *Cerner Millennium* as for the foreign system.

If the port needs to be changed, select a new port that is not being used. To determine if a port is being used, use the TCP or IP Tools menu with the OEN_MENU utility. The OEN_MENU utility can be accessed using *Discern Explorer* (CCL). To determine if the new port is available, from the TCP or IP Tools menu, select F**ind a New Unused Socket**. If all the previous options do not work and it is a TCP or IP connection, then a TCP or IP trace can be done on the connection to determine where and what the issue is. See Troubleshoot With TCP-IP Trace for instructions on performing a TCP or IP trace.

Step 2 - Determine if the Transaction Reached the ESI Outbound Comserver

Once it has been determined that the transaction was received, the transaction needs to continue to be followed through the inbound interface processing.

1. Check the OEN_TXLOG utility.

   If transaction logging is turned enabled, then the transaction should log to the OEN_TXLOG utility for the External System Inbound (ESI) comserver. Also, the number of transactions processed through the server can be checked in the Controller view of OpenView.

2. Verify that the ESI outbound comserver is running.

   Is the appropriate ESI comserver running? To determine if the communication server is running, look in the Controller view of OpenView or in the SCP. When you log into OpenView, the Controller view lists the servers with the domain to which you are logged in. The domain is displayed in the lower-right corner.

   Once in the correct domain, find the comserver for the interface that is not communicating. If there is a red X to the left of the inbound comserver, it is not running. To start the comserver, right-click the comserver and select **Start** or click the **traffic light**. The red X should be replaced with a green circle. If the green circle is not displayed after a few moments, or if the circle changes back to a red X, there is a problem with the comserver.

3. Verify that the CPM ESI server (SCP 250) is running.

   Also, the ESI comserver stops if no instances of the CPM ESI server exist. So, if the ESI comserver does not start and it has a transaction queued (either view queued transactions or look at the count in the Controller view), then verify that at least one instance of the CPM ESI server is running. This can be checked in Olympus or in the SCP.

4. Check for communication errors.

   Check the MSGVIEW utility or Olympus for communication errors. The error shows the comserver and the communication step in which the error occurred. Communication steps are represented by the letters O, G, I, Q, R or X. See the Open View Help for an explanation of errors and suggested resolutions.

5. Verify that the OEN Router server (SCP 245) is running.

   If it does not look like the transaction made it to the ESI comserver, then check the status of the OEN Router server. Is the Router server running? This can be checked in Olympus or in the SCP.

6. Verify the routing.

   Verify that the inbound comserver is routed to the appropriate ESI outbound comserver. To check the routing of the inbound comserver, go to Process Config in OpenView for the appropriate inbound comserver. To access Process Config, in the Controller view of OpenView, right-click the inbound comserver and select **Process Config**. On the Services tab, click the route setup. In the Route To box, verify that the appropriate ESI comserver is selected.

Step 3 - Determine if the CPM ESI Server Processed the Transaction

At this point, it needs to be determined if the CPM ESI server processed the transaction.

1. Check the ESI_LOG.

   If the log_table property is set above 0 on the CPM ESI server, the transaction should log to the ESI_LOG table if it had an error. If the log_table property is set to a 4, then all transactions should be logged to the ESI_LOG table.

   You can use SI Manager to search ESI Log in the ESI Troubleshooting section. If you want to see all transactions logged do not filter on a status. You can also use *Discern Explorer* to view the ESI_LOG table by entering, **ESI_LOG** go at the *Discern Explorer* prompt. If you want to see all transactions logged, keep the default log level of 5 selected.

2. Verify that the CPM ESI server (SCP 250) is running.

   If the transaction does not show in ESI_LOG table and the log_table property is set appropriately, then confirm that at least one instance of the CPM ESI server is running. This can be checked in Olympus or in the SCP.

   If the CPM ESI server is not running, then start an instance of the ESI CPM server and see if it processes the transaction. The ESI comserver also probably needs to be restarted. If the CPM ESI server still does not process the transaction - if it either stops or logs an error - refer to Msgview or Olympus for additional error logging.

3. Review the CMB_TEMP file.

© Cerner Corporation and affiliates. All rights reserved. Contains Cerner confidential and/or proprietary information belonging to Cerner Corporation and/or its related affiliates which may not be reproduced or transmitted in any form or by any means without the express written consent of Cerner. Use may be subject to the "DHMSM License and Distribution Restrictions" in the Terms of Use (http://www.cerner.com/Terms_Of_Use/). The Terms of Use contain restrictions on use and distribution of this content, including use and distribution restrictions applicable to DHMSM and other government users.

Also, if debug logging is set above 2, then reviewing the CMB_TEMP file can also be helpful. This file is stored in the CMB_TEMP directory and is called CMB_####_DD.out, where #### is SCP server id (padded with zeros to four digits). So, the CPM ESI server would be CMB_0250_DD.out. The DD stands for the instance of the CPM ESI server. If only one instance of the ESI server is running, it would be CMB_0250_01.out.

When looking at the CMB_TEMP file, the latest version is locked if the ESI server is running. To view the most current file, complete the instructions below. If this is not a production environment, stop the CPM ESI server and view the latest version of the file.

4. First, null the file if recreating the issue.

   For OpenVMS:
   *>cmb_####_DD.out
   Example: >cmb_0250_01.out

5. Then, view the file.

   cat cmb_####_DD.out
   Example: cat cmb_0250_01.out

6. Check SRVRTLVIEW for errors.
   Another place to check for errors is SRVRTLVIEW. This is helpful when the CPM ESI server or one of the comservers is logging *Discern Explorer* errors. SRVRTLVIEW can be accessed through *Discern Explorer*. At the *Discern Explorer*(CCL) prompt, enter **SRVRTLVIEW go**. Once in the program, select the appropriate log file by selecting the appropriate server.

7. If necessary, resend the transaction.

   Once the issue is determined, it is sometimes necessary to replay (resend) the transaction. To replay the transaction, you can use the OEN_REPLAY tool. For OEN_REPLAY to work correctly, transaction logging must be turned on. This can be set through Process Config in OpenView.

   > **Note**
   >
   > OEN_REPLAY is a program that is run from the *Discern Explorer*(CCL) prompt. See Troubleshoot With OEN_REPLAY for more information.

Step 4 - Determine if the Transaction Posted to the Database

At this point, it is known that the transaction made it to the CPM ESI server, but the CPM ESI server wrote an error on the transaction or the transaction did not post to the database.

1. Troubleshoot the ESI_LOG error.

   If the CPM ESI server wrote an error to ESI_LOG, troubleshoot the error to determine what is wrong with the message. This may require reviewing the CMB_TEMP file, the MSGVIEW utility, or SRVRTLVIEW for more information. See the instructions. If it is determined that the transaction posted to the database, but is not viewable in the application, an application configuration issue exists or possibly only part of the transaction was posted to the database. More than likely it is a field that the application requires, but it is not populated.

2. Review the transaction in OEN_TXLOG.

   If the information posted incorrectly to the database, the transaction should be reviewed in OEN_TXLOG to make sure what was thought to have been sent was really sent.

3. Review the scripts.

   If any scripting has been included in the comservers, review the scripts to make sure they are not stripping or manipulating the field you are looking for. All the scripting for the interface should be documented in the site specific specifications.

4. Verify the correct configuration in SI_Manager.

   In SI_Manager verify that the contributor system has been set up according to the site specifications.

Troubleshooting Audits

The troubleshooting audits are described below.

ESI_LOG

ESI_LOG is a *Discern Explorer* (CCL) based reporting utility that extracts information from the ESI_LOG table. It is used to determine which CPM ESI server processed a specific message, whether the message succeeded or failed, and provide statistical information about the transactions processed by the CPM ESI server. The level of logging done by the CPM ESI server and posted to the ESI_LOG table is configured by the logtable_flag.

© Cerner Corporation and affiliates. All rights reserved. Contains Cerner confidential and/or proprietary information belonging to Cerner Corporation and/or its related affiliates which may not be reproduced or transmitted in any form or by any means without the express written consent of Cerner. Use may be subject to the "DHMSM License and Distribution Restrictions" in the Terms of Use (http://www.cerner.com/Terms_Of_Use/). The Terms of Use contain restrictions on use and distribution of this content, including use and distribution restrictions applicable to DHMSM and other government users.

CMB_TEMP Files

Another source of information is the CMB output and error files. There are two standard server error files, the .OUT file and the .ERR file. These files are located in the cmb_temp directory and are listed as cmb_[value]*01.out and cmb*[value]_01.err, where [value] is the SCP server id of the server or interface being investigated.

The .OUT file is used to log informational messages about server activity; it keeps track of what the server did, which scripts it called, and so on. The .ERR file identifies where and what errors were encountered. The CPM ESI server currently logs informational and error messages in both of these log files. Both of these files must be accessed from the back-end, and read using a standard operating system editor.

System Messages

See Troubleshoot FSI System Messages for information on system messages across *Cerner Millennium*, including information on Message Viewer and middleware system messages.

External System Inbound System Messages

Some CPM ESI server system messages are generated as MLG files and are viewable in MessageView. The server-specific standard out and standard error files are in the cmb_temp directory, as indicated above. For detailed information about the system messages generated by the CPM ESI server, see CPM ESI Server.

© Cerner Corporation and affiliates. All rights reserved. Contains Cerner confidential and/or proprietary information belonging to Cerner Corporation and/or its related affiliates which may not be reproduced or transmitted in any form or by any means without the express written consent of Cerner. Use may be subject to the "DHMSM License and Distribution Restrictions" in the Terms of Use (http://www.cerner.com/Terms_Of_Use/). The Terms of Use contain restrictions on use and distribution of this content, including use and distribution restrictions applicable to DHMSM and other government users.