



PureConnect®

2020 R1

Generated:

30-March-2020

Content last updated:

20-March-2020

See **Change Log** for summary of changes.



Log Viewer

Printed Help

Abstract

Log Viewer is an Interaction Center utility that reads application and subsystem log files. Log files provide a record of processing steps completed and record the status of an application or subsystem at a specific point in time. For this reason Log Viewer is useful for troubleshooting problems and for understanding the internal processing of software applications and IC server subsystems. This document explains how to use Log Viewer to examine IC subsystem and application logs.

For the latest version of this document, see the PureConnect Documentation Library at: <http://help.genesys.com/cic>.

For copyright and trademark information, see https://help.genesys.com/cic/desktop/copyright_and_trademark_information.htm.

Table of Contents

| | |
|--|----|
| Table of Contents | 2 |
| Log Viewer | 7 |
| Overview | 7 |
| What to do first | 7 |
| Log Viewer Procedures | 7 |
| Logging Background | 9 |
| Logs have an .ininlog extension | 9 |
| Other supported file formats | 9 |
| Processes, threads, and time slicing | 9 |
| Types of logging performed | 10 |
| NT event logs | 10 |
| Subsystem logs | 11 |
| Location of IC subsystem logs on the server | 11 |
| Changing the default log folder | 11 |
| Log Size Thresholds | 11 |
| Automatic Log File Compression | 11 |
| Security Considerations | 12 |
| Files in the Logs share | 12 |
| Application logs | 17 |
| Location of application logs on your computer: | 17 |
| Log Viewer Procedures | 18 |
| Access Help Topics | 18 |
| Help > Contents | 18 |
| Help > Index | 18 |
| Help > Search | 18 |
| Access version information | 18 |
| Analyze distinct context attribute values | 18 |
| Columns in the list view | 19 |
| Apply a quick string filter | 20 |
| Clear All Filters | 20 |
| Clear Global Time Range Filter | 20 |
| Clone a log window | 21 |
| To clone a log window: | 21 |
| Close a log file | 21 |
| Colorize columns in the message list | 21 |
| Regular Expressions | 22 |
| Clearing Colors | 22 |
| Control log verbosity | 23 |
| Trace Topics | 23 |
| Trace Levels | 23 |
| Use CIC System Manager to set trace levels | 23 |
| Use Trace Configuration utility to set trace levels | 26 |
| Copy log entries to other applications using the clipboard | 28 |
| Decrypt a log message | 30 |
| To decrypt a log message | 30 |
| Decrypt multiple log messages | 31 |
| Delete a log file | 31 |
| Delete a saved filter | 32 |
| Display log header information | 32 |
| Exit Log Viewer | 32 |
| Export to File | 32 |
| Find Text | 33 |
| Repeat searches | 33 |
| Import Filters | 33 |
| Jump to Matching Scope/Create | 34 |
| Jump to (or near) a specific timestamp | 34 |
| Jump to next/previous thread message | 35 |
| Launch TraceConfig utility | 35 |
| Manage columns in the message list | 35 |
| Logged Columns | 35 |
| Manage Window Settings | 38 |

| | |
|---|----|
| Open a log file | 38 |
| Open latest log file in a series | 40 |
| Refresh the log automatically | 40 |
| Refresh the log manually | 41 |
| Reopen a log file | 41 |
| Replace current log with latest in series | 41 |
| Save the current filter | 41 |
| Search forward or backward on message type | 42 |
| Search forward or backward on message color | 42 |
| Search forward or backward on named expressions | 43 |
| Select all log entries in a message list | 43 |
| Set application options | 43 |
| Set complex filters | 43 |
| Set global time range filter | 44 |
| Set global time range filter begin | 44 |
| Set global time range filter end | 45 |
| Set manual time offset | 45 |
| Manual Time Offset (in ms): | 45 |
| OK button | 45 |
| Cancel button | 45 |
| Set global trace level filter | 46 |
| Show or hide context attributes in message detail | 47 |
| Show or hide function names in log messages | 47 |
| Show or hide related source code | 48 |
| Show or hide the status bar | 48 |
| Show or hide the toolbar | 49 |
| Snip or merge log files | 49 |
| Synchronize timestamps for a time zone | 50 |
| My Local Time Zone | 50 |
| Log Creator's Time Zone | 50 |
| Universal Coordinated Time | 50 |
| Synchronize with other logs | 50 |
| Use Search menu commands to trace call levels | 51 |
| Undo/Redo Filters | 51 |
| Use Bookmarks | 52 |
| Add or remove bookmarks | 52 |
| Jump to next or previous bookmark | 52 |
| View All Bookmarks | 52 |
| Use Stored Filters | 52 |
| Log Viewer User Interface | 53 |
| About dialog | 53 |
| Bookmarks dialog | 53 |
| Bookmark list | 53 |
| Remove Bookmark button | 54 |
| Jump to Bookmark button | 54 |
| Import Bookmarks button | 54 |
| Export Bookmarks button | 54 |
| Done button | 54 |
| Change Columns dialog | 54 |
| Available Columns list | 55 |
| Visible Columns list | 55 |
| Add button | 55 |
| Remove button | 55 |
| Up button | 55 |
| Down button | 55 |
| OK button | 55 |
| Cancel button | 55 |
| Enter Coloring Regular Expressions dialog | 56 |
| Expression text box | 56 |
| OK button | 56 |
| Cancel button | 56 |
| Export Output File dialog | 57 |
| File Open dialog | 57 |
| Shortcut buttons | 57 |

| | |
|---|----|
| File name | 58 |
| Files of Type | 58 |
| Open button | 58 |
| Cancel button | 58 |
| Filter Configuration dialog | 58 |
| Saved Filters list | 59 |
| Ad-Hoc Filters list | 59 |
| File > Save Filters... | 59 |
| Import Filters... | 59 |
| Export Filters | 59 |
| Combine w/AND Combine w/OR | 59 |
| Filter > Create Named Filter | 59 |
| Filter > Create Ad-Hoc Filter | 59 |
| OK button | 60 |
| Cancel button | 60 |
| Apply button | 60 |
| Filter Criterion Choices | 60 |
| Enable This Filter check box | 72 |
| Invert This Filter checkbox | 72 |
| Semi-colon separated list of 'this' pointers to match | 72 |
| OK button | 72 |
| Cancel button | 72 |
| Trust Level | 73 |
| Timestamp Range | 73 |
| Context Attribute | 75 |
| Filename/Line | 76 |
| Within Scope | 77 |
| Lines of Context | 79 |
| Bookmarks | 81 |
| In Exception Unwind | 82 |
| Logical Operations | 83 |
| Clipboard Operations | 83 |
| Find Text dialog | 83 |
| Text to Find drop list | 83 |
| Forward | 84 |
| Backward | 84 |
| Use regular expressions check box | 84 |
| Search in current thread | 84 |
| Ignore invalid encoding characters | 84 |
| Match case | 84 |
| Include function name | 84 |
| OK button | 84 |
| Cancel button | 84 |
| Global Time Range Filter dialog | 85 |
| start time / end time slide controls | 85 |
| OK button | 85 |
| Cancel button | 85 |
| Key Management dialog | 85 |
| Category column | 86 |
| Instance column | 86 |
| Key or passphrase column | 86 |
| Clear button | 87 |
| Set button | 87 |
| Log Header dialog | 87 |
| Log pane | 87 |
| List pane | 87 |
| Detail pane | 88 |
| Name/Value pairs in the List pane | 88 |
| Log Snip/Merge Utility | 89 |
| Add button | 89 |
| Remove button | 90 |
| Don't Restrict Start Time check box | 90 |
| Start Date | 90 |
| Start Time | 90 |
| Don't Restrict End Time check box | 90 |
| Stop Date | 90 |

| | |
|--|-----|
| Stop Time | 90 |
| Destination File | 90 |
| Snip button | 90 |
| Cancel button | 91 |
| Message Decryption Key dialog | 91 |
| Category | 91 |
| Instance | 91 |
| Key or Passphrase | 91 |
| OK button | 92 |
| Cancel button | 92 |
| Options dialog – Misc tab | 92 |
| Automatic log refresh interval (seconds) | 92 |
| Apply bug fix for system menu coloring | 93 |
| Size of File menu MRU list | 93 |
| Set the .ininlog extension association | 93 |
| Close Snipper Monitor on Successful Snip | 93 |
| When starting a new histogram default bucket size to | 93 |
| Options dialog – Perform tab | 93 |
| Use perform to find source files check box | 94 |
| Special Perform server frame | 94 |
| Default Perform server frame | 95 |
| Legacy search drives frame | 95 |
| Save Current Filter As dialog | 96 |
| Filter name | 96 |
| OK button | 96 |
| Cancel button | 96 |
| Select Time Zone dialog | 96 |
| Snipper Monitor dialog | 97 |
| Message list | 97 |
| Close Dialog when Process Completes Successfully | 97 |
| Close button | 97 |
| Timestamp Selection dialog | 98 |
| Slider bar | 98 |
| Date box | 98 |
| Timestamp field | 98 |
| Revisions | 99 |
| PureConnect 2018 R3 | 99 |
| CIC 2016 R1 | 99 |
| CIC 2015 R1 | 99 |
| IC 4.0 Service Update 5 | 99 |
| IC 4.0 Service Update 4 | 99 |
| IC 4.0 Service Update 3 | 99 |
| IC 4.0 Service Update 2 | 99 |
| IC 4.0 Service Update 1 | 99 |
| IC 4.0 GA | 100 |
| Change log | 101 |
| Glossary | 102 |
| Admin Services | 102 |
| Alert Services | 102 |
| Authentication | 102 |
| Client Services | 102 |
| Compression Services | 102 |
| Context Attributes | 102 |
| Customer Interaction Center (CIC) | 102 |
| Data Services | 102 |
| Directory Services | 102 |
| Email Services | 103 |
| Fax Services | 103 |
| Handlers | 103 |
| Host Services | 103 |
| IC Server | 103 |
| Interaction Attendant | 103 |
| Interaction Designer | 103 |
| Interaction Processor | 103 |

| | |
|------------------------------------|-----|
| LogSnipper | 103 |
| Log Snippet | 103 |
| Logs | 103 |
| Notifier | 104 |
| Object | 104 |
| OCR Services | 104 |
| Paging Services | 104 |
| Process | 104 |
| Publish/Subscribe Event Processing | 104 |
| Queue | 104 |
| Queue Manager | 104 |
| Request/Response Processing | 105 |
| Speech Recognition Services | 105 |
| Station Groups | 105 |
| Station Queue | 105 |
| Statistical Services | 105 |
| Telephony Services | 105 |
| Text-to-Speech (TTS) Services | 105 |
| Threads | 105 |
| Time Slicing | 105 |
| Trace Viewer | 106 |
| Trunk | 106 |
| User Queue | 106 |
| Web Services | 106 |
| Wireless Services | 106 |

Log Viewer

This document is for administrators and end-users who are interested in the CIC logging process and the Log Viewer utility in particular. General familiarity with the Customer Interaction Center platform is assumed.

Overview

Customer Interaction Center saves detailed information about the operation of its subsystems in *log files*. Generally speaking, subsystem logs provide a record of completed processing steps and record the status of an application or subsystem at a specific point in time. Subsystem logs are sometimes called *trace logs*, since they trace the execution of software programs. Logs can be analyzed to determine normal and abnormal system functions. For this reason, logs are useful for troubleshooting purposes. This publication introduces the reader to CIC subsystems and the logging process. It explains how to use Log Viewer to set trace levels, snip log files, and filter examine logs.

What to do first

[Open a log file](#)

[Read background information about logging in CIC](#)

[Learn about Log Viewer's user interface](#)

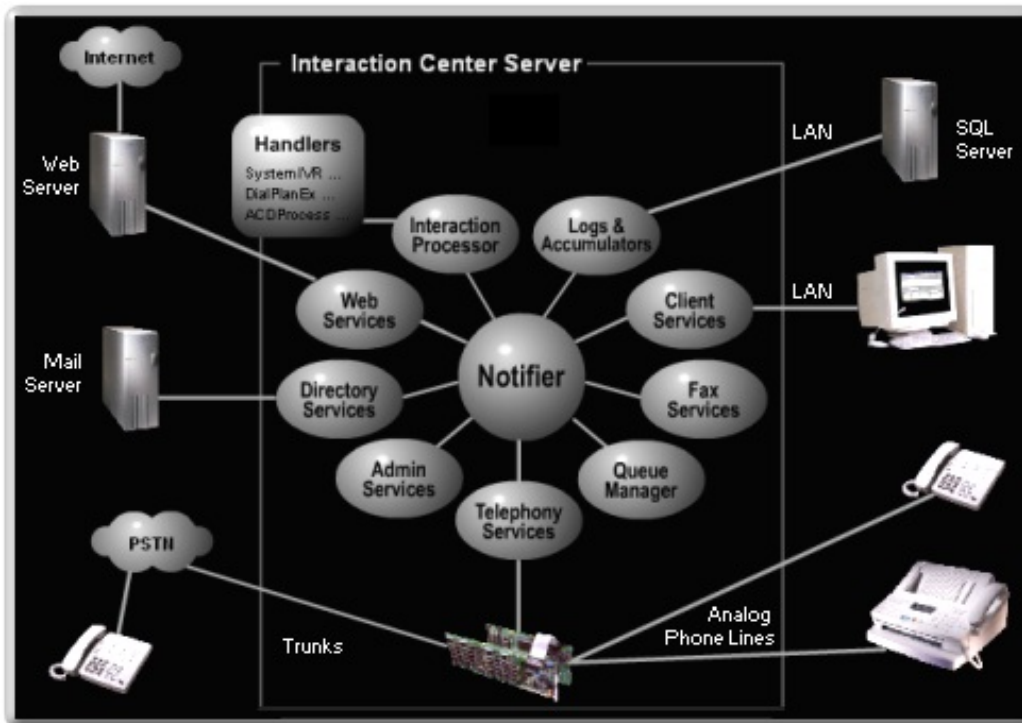
[Find out what is new in Log Viewer](#)

Log Viewer Procedures

| | |
|---|---|
| Access Help topics | Access version information |
| Analyze distinct context attribute values | Apply a quick string filter |
| Clear all filters | Clear global time range filter |
| Clone a log window | Close a log file |
| Colorize columns in the message list | Control log verbosity |
| Copy log entries using the clipboard | Decrypt a log message |
| Decrypt multiple log messages | Delete a log file |
| Delete a saved filter | Display log header information |
| Exit Log Viewer | Export to File |
| Find Text | Import Filters |
| Jump to (or near) specific timestamp | Jump to Matching Scope/Create |
| Jump to next/previous thread message | Launch the TraceConfig utility |
| Manage columns in the message list | Manage Window settings |
| Open a log file | Open the latest log file in a series |
| Refresh the log automatically | Refresh the log manually |
| Reopen a log file | Replace current log with latest in series |
| Save the current filter | Search forward or backward on message color |
| Search forward or backward on message type | Search forward or backward on named expressions |
| Select all log entries in a message list | Set application options |
| Set complex filters | Set global time range filter |
| Set global time range filter begin | Set global time range filter end |
| Set global trace filter | Set manual time offset |
| Show or hide context attributes in message detail | Show or hide function names in log messages |
| Show or hide related source code | Show or hide the status bar |
| Show or hide the toolbar | Snip or merge log files |
| Synchronize timestamps for a time zone | Synchronize with other logs |
| Undo/Redo Filters | Use Bookmarks |
| Use Search menu commands to trace call levels | Use Stored Filters |

Logging Backgrounder

The Customer Interaction Center platform is composed of software components, called subsystems. These components are written in the C++ language to maximize performance. Individual subsystems work together via a central communication hub known as the Notifier. Each subsystem is critical to the overall system, but operates independently.



This modular design logically separates each subsystem so that the system can continue operating if a subsystem ceases to function or performs abnormally. Also, if one component of the product requires an update, only the parts associated with that component are updated—the entire system does not need to be upgraded.

Customer Interaction Center saves detailed information about the operation of subsystems in *log files*. Logs maintain a record of processing steps completed, and record the status of a CIC subsystem at a specific point in time. The information in logs is useful for troubleshooting purposes. System administrators and support representatives often analyze logs to diagnose system behavior.

Logs have an .ininlog extension

- The ".ininlog" extension identifies a trace log file.
- The ".ininlog.ininlog_idx" identifies the index file of a trace log.

Other supported file formats

- VwrLog log files.
- .evt files created by Windows Event Log service, a Control Panel administrative tool.
- .syslog files from any syslog-compatible source, such as telephony driver applications (Intel HMP, Dialogic, etc.).
- .txt logs. Some telephony drivers optionally generate syslog-format files in plain ASCII text format. Log Viewer can open syslog files that have been saved in text format.

Processes, threads, and time slicing

Each CIC subsystem is a Windows *process* that communicates with other subsystems via *threads*. To understand how Customer Interaction Center functions internally, it is important to conceptually understand *processes*, *threads*, and *time slicing*.

- A *process* is the execution of a program. It is a collection of virtual memory space, code, data, and system resources. Each process is a distinct entity, able to execute and terminate independently of all other processes. A 32-bit application has at least

one process and one thread. A processor executes threads, not processes. Prior to the introduction of multiple threads of execution, applications were all designed to run on a single thread of execution.

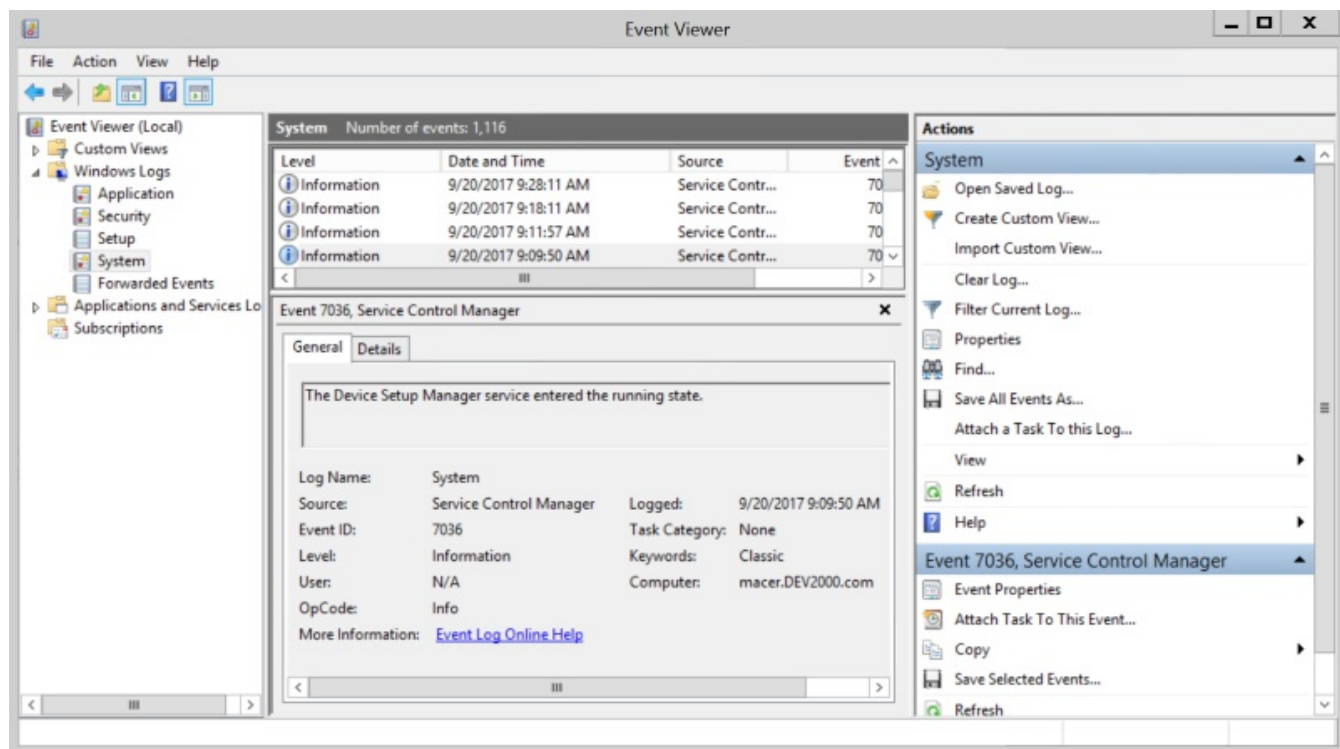
- *Threads* are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process and more than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled. The thread context includes all of the information the thread needs to seamlessly resume execution, including the thread's set of CPU registers and stack, in the address space of the thread's host process.
- *Time Slicing*. A program can allocate processor time to units in its body. Each unit is then given a portion of the processor time. Even if your computer has only one processor, it can have multiple units that work at the same time. The trick is to slice processor time and give each slice to each processing unit. The smallest unit that can take processor time is called a thread. A program that has multiple threads is referred to as a multi-threaded application.

Types of logging performed

- Critical system messages are written to the [Windows Event log](#) on the server.
- Entries that trace the operation of CIC subsystems and applications are written to [CIC subsystem logs](#) on the CIC server.
- [Application logs](#) are saved on the local workstation.

NT event logs

Critical system messages are written to *NT Event Logs*. In general, NT Event logs are reserved for high-priority messages that require the immediate attention of a system administrator.



To view NT Event Logs, use Microsoft's Computer Management application.

Subsystem logs

Subsystem logs document the operation of various CIC subsystems. This type of logging is more verbose than NT Event Logs.

A *subsystem log* is a binary file that stores information about an event of some sort, to record a normal operation or an abnormal condition that affected a subsystem. Subsystem logs are called *trace logs*, since they trace the activities performed by a system.

Most CIC subsystems have a dedicated log that stores information about error conditions, warnings, and other data that helps track the processing behavior of the subsystem. A software subsystem typically logs messages when it passes control to a routine, encounters a problem, or otherwise needs to record work performed. The degree of detail written to logs is configurable for each CIC subsystem.

Location of IC subsystem logs on the server

CIC subsystem logs are stored in the \Logs share on the server. The physical path is \i3\IC\Logs. This folder contains log folders named using the current date, in the form YYYY-MM-DD. See [Files in the Logs share](#) for information about log files stored in this share.

Changing the default log folder

The location of the CIC logs folder is configurable. You can change the log path using the *CIC System Manager utility*.

Log Size Thresholds

If a log file exceeds an internal size threshold, it is broken into separate log files within the folder for that day. Subsequent log files are numbered sequentially. For example, a log that spans two files might be named:

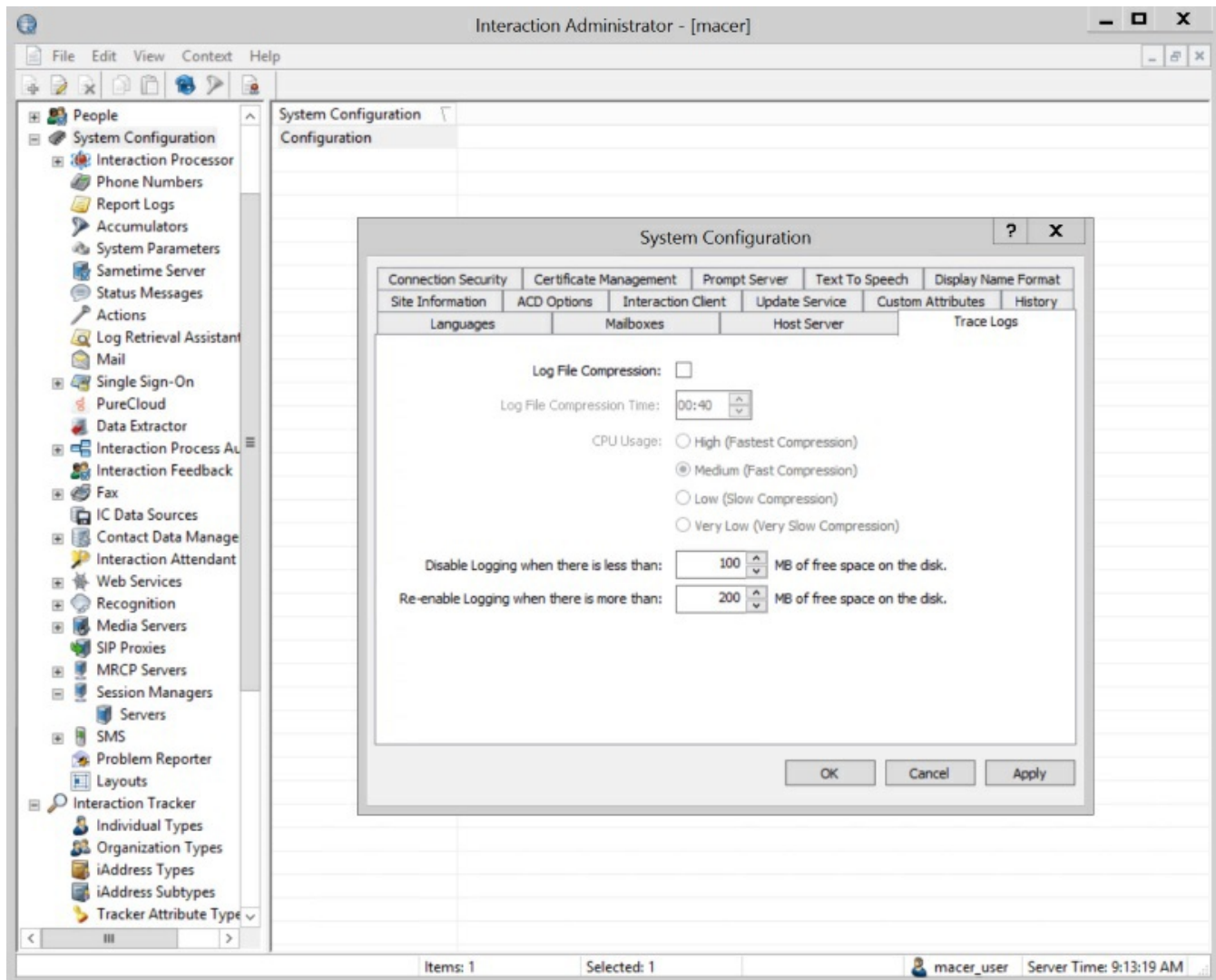
d:\i3\IC\Logs\2011-07-19\ININ.UpdateProviderServiceD.ininlog

d:\i3\IC\Logs\2011-07-19\ININ.UpdateProviderServiceD_1.ininlog

In this example, a second log was created with a "_1" suffix when the original log exceeded its maximum size limit. The log file threshold setting is not configurable.

Automatic Log File Compression

Subsystem log files are zipped by a nightly compression routine. A 24-hour formatted time when compression of log files occurs is configured in Interaction Administrator. To change this time, open Interaction Administrator and select the *System Configuration* container. Double-click the **Configuration** entry. When the **System Configuration** dialog appears, click on the **Trace Logs** tab. Change the log file compression time, and then click **OK**.



Security Considerations

Since trace logs can contain sensitive information, customers are strongly advised to limit access to CIC servers. When tracing is turned up, the content of handler variables is logged when a tool assigns an output parameter. Likewise, information coming and going to databases is also logged.

Verbose logging of normal business logic could potentially be exploited by an attacker who filters logs for a particular call and looks at the individually detected digits. By examining the timestamps of the traces, the attacker might be able to identify menu items, SSNs, account numbers, credit card numbers, expiration dates, and other sensitive data. Genesys provides trace logs for diagnostic purposes only. Customers are responsible for protecting sensitive information in trace logs as part of their overall data management policies.

Another potential concern is the dissemination of log files to off-site partners or support representatives. Customers can address this by providing a temporary terminal service login to the machine that has the Trace Viewer installed.

Files in the Logs share

CIC logs are stored in the \Logs share on the server as zip files. The physical path is \i3\IC\Logs, unless the location of the [default log folder](#) was changed. The table below lists the names of major subsystem and application logs on a CIC server.

| Log File Name | Description |
|--------------------------|---|
| AccServer.ininlog | <p>AccServer</p> <p>\i3\IC\Server\AccServerU.exe</p> <p>This subsystem keeps track of accumulators running in CIC. Accumulators are similar to system registers. They count events as they occur in the CIC's Interaction Processor. Instances of these events are stored in variables and are accessible in report logs or other handlers using the Accumulator tools in Interaction Designer.</p> |
| ACDServer.ininlog | <p>AcdServer</p> <p>\i3\IC\Server\AcdServerU.exe</p> <p>This subsystem allows users and supervisors to define specific circumstances (e.g., average hold time > 10 minutes) under which they are to be alerted and the means by which the alert is to occur (e.g., e-mail, pager, phone call, etc.).</p> |
| AdminServer.ininlog | <p>AdminServer</p> <p>\i3\IC\Server\AdminServerU.exe</p> <p>Admin Services retrieves security and profile information from Directory Services.</p> |
| AlertServer.ininlog | <p>AlertServer</p> <p>\i3\IC\Server\AlertServerU.exe</p> <p>Alert Server allows users and supervisors to define specific circumstances — such as average hold time > 10 minutes — under which they are to be alerted. Alert Server also enables users and supervisors to set the alert method occur such as e-mail, pager, phone call, and so on.</p> |
| BridgeHost.ininlog | <p>BridgeHost</p> <p>\i3\IC\Server\BridgeHostU.exe</p> <p>The IP Bridge Host is the connector between the thin clients and the Session Manager. It translates network protocols, socket-level security checking, and other tasks during a thin client-to-Session Manager exchange.</p> |
| CallLog.ininlog | Record of interactions passing through CIC. |
| ClientServices.ininlog | <p>Client Services</p> <p>\i3\IC\Server\ClientServicesU.exe</p> <p>Client Services keeps track of logged-in users, their status, and their rights based on security configurations. Without Client Services there would not be a client interface, such as the CIC clients.</p> |
| ClusterConnector.ininlog | <p>ClusterConnector</p> <p>\i3\IC\Server\ClusterConnectorU.exe</p> <p>ClusterConnector is a clustering component.</p> |
| CompressorManger.ininlog | <p>Compressor Manager</p> <p>\i3\IC\Server\CompressorManagerU.exe</p> <p>Compression Manager reduces the size of audio recordings (such as voice mail messages) using TrueSpeech and other compression algorithms.</p> |
| DataManager.ininlog | <p>DataManager</p> <p>\i3\IC\Server\DataManagerU.exe</p> <p>Data Manager is the CIC subsystem that services RWP lookup requests, as well as contact directory requests. Data Manager keeps track of data sources used to display Contact Directory and Speed Dial notebook pages in the CIC clients.</p> |

| | |
|-----------------------------------|--|
| DSServer.ininlog | <p>Directory Services</p> <p>\I3\IC\Server\DSServerU.exe</p> <p>Directory Services provides the interface to the proprietary data store (configuration repository) that CIC uses to store system configuration information.</p> |
| DSSink.ininlog | <p>DSSink</p> <p>\I3\IC\Server\DSSinkU.exe</p> <p>DSSink is an CIC clustering component.</p> |
| EMS Server.ininlog | <p>EMS Server</p> <p>\I3\IC\Server\EMSU.exe</p> <p>This server manages Multi-Site functions using on an CIC peer site.</p> |
| FaxServer.ininlog | <p>FaxServer</p> <p>\I3\IC\Server\FaxServerU.exe</p> <p>Fax Services is the CIC subsystem that sends and receives faxes.</p> |
| HostServer.ininlog | <p>HostServer</p> <p>\I3\IC\Server\HostServerU.exe</p> <p>Host Services allow CIC to communicate with mainframes and IBM AS/400 systems using the 3270 and 5250 terminal emulation protocols.</p> |
| Interaction Administrator.ininlog | Application log for Interaction Administrator. |
| Interaction Designer.ininlog | Application log for Interaction Designer. |
| IP.ininlog | <p>IP</p> <p>\I3\IC\Server\IPU.exe</p> <p>Interaction Processor (IP) is the CIC subsystem that processes low-level subsystem events in order to implement higher-level business logic. For example, Interaction Processor starts an instance of a handler in response to an event.</p> <p>Interaction Processor tells the system how to behave based upon any events that occur. An incoming call is just one example of an event that CIC recognizes. Programs called handlers respond to unique events and specify how the system will behave. When the Interaction Processor recognizes an event that it needs to act upon, it turns to the list of handlers to determine which one should respond to that event.</p> <p>It then runs an instance of that handler and any subroutine handlers that are necessary. Multiple instances of handlers can run at the same time, as those multiple events occur. Once the handler has completed its routine, it deletes itself from the system.</p> |
| IPDBServer.innlog | <p>IPDBServer</p> <p>\I3\IC\Server\IPDBServerU.exe</p> <p>IPDB Server connects Interaction Processor to a specified database when Database tools are used.</p> |
| IPServer.ininlog | <p>IpServer</p> <p>\I3\IC\Server\IpServerU.exe</p> <p>IP Server manages helper tasks for Interaction Processor and Report Logging. It logs line activity, and manages part of the Message waiting light processing.</p> |
| | |

| | |
|------------------------------|--|
| Mail Account Monitor.ininlog | <p>Mail Account Monitor</p> <p>\\I3\IC\Server\MailAcctMonU.exe</p> <p>Mail Account Monitor is responsible for syncing external user attributes from Mail accounts or LDAP to Directory Services.</p> |
| Notifier.ininlog | <p>Notifier</p> <p>\\I3\IC\Server\NotifierU.exe</p> <p>The heart of the Interaction Center is the Notifier, which is an internal message-switching hub for event messages. Notifier is a communications hub that communicates with each individual CIC subsystem. Notifier provides three essential services: request/response processing, publish/subscribe event processing and authentication. Notifier makes it possible for components of CIC to be installed on a single server, or on multiple servers. Notifier enhances scalability of CIC by allowing individual components to reside on dedicated hardware when exceptional processing power is required.</p> <p>Notifier directs events and messages throughout the rest of the system. It listens for events generated by other modules and notifies other interested modules that the event has occurred. Notifier makes use of the TCP/IP protocol to communicate with the rest of the Interaction Center Platform. Connections between Notifier and other components can be encrypted for maximum security.</p> <p>Notifier passes information between subsystems in real-time. Notifier reduces overall network traffic by sending event notifications only to components that have subscribed to receive them. This allows applications using the Interaction Center Platform to handle much larger numbers of users and interactions.</p> |
| Optimizer Server.ininlog | <p>Optimizer Server</p> <p>\\I3\IC\Server\OptimizerSvrU.exe</p> |
| OutOfProcCustomDLL.ininlog | <p>OutOfProcCustomDLL</p> <p>\\I3\IC\Server\OutOfProcCustomDllU.exe</p> <p>OutOfProc server is a service that executes DLLs for Interaction Processor without risking the integrity of the IP process. Its size will be a function of any custom activities that might be added by the customer or VAR via these customization interfaces.</p> |
| PostOfficeServer.ininlog | <p>Post Office</p> <p>\\I3\IC\Server\PostOfficeServerU.exe</p> <p>Post Office Server (POS) is the CIC subsystem that provides platform independent access to Email services such as message store access and message delivery. POS also provides support for Email routing, and will initiate a Reverse White Pages lookup request before queuing an incoming email interaction.</p> |
| ProvisionServer.ininlog | <p>Provision Server</p> <p>\\I3\IC\Server\ProvisionServerU.exe</p> |
| RecoSubsystem.ininlog | <p>Reco Subsystem</p> <p>\\I3\IC\Server\RecoSubsystemU.exe</p> <p>Speech recognition services recognize spoken commands and phrases for applications such as speech-enabled IVR (Interactive Voice Response).</p> |
| Recorder Server.ininlog | <p>Recorder Server</p> <p>\\I3\IC\Server\IRServerU.exe</p> <p>Interaction Recorder is an application for managing phone calls, Emails, Faxes, screen recordings, and Web chats recorded within the CIC platform. Interaction Recorder identifies interactions to record and manages the compression, archiving, and storing of the attributes for each type of media recording. Using Interaction Recorder, you can quickly sort and manage large numbers of recordings. Interaction Recorder also includes features for scoring agent interactions and quality monitoring.</p> |

| | |
|-----------------------------|--|
| RemocoServer.ininlog | Application log for Remoco (CIC Console) which manages CIC subsystems when CIC is started as an application, rather than as a service. CIC normally starts as a service, but technical support may ask for startup in application mode to aid in problem determination. |
| SessionManager.ininlog | <p>Session Manager</p> <p>\I3\IC\Server\SessionManagerU.exe</p> <p>The subsystem that keeps track of each user's client status, and other details. Session Manager is a server-side process that enables customers to deploy large numbers of concurrent "thin" CIC clients and enables those clients to gracefully handle low-bandwidth, intermittent connectivity and intelligent caching.</p> <p>The Session Manager server subsystem holds user login data and performs all CIC-related tasks on behalf of thin clients. For example, when a thin client wants to disconnect a call, the request is sent to the Session Manager, and the Session Manager performs the command.</p> |
| SMSServer.ininlog | <p>SMSServer</p> <p>\I3\IC\Server\SMSServerU.exe</p> <p>The CIC subsystem that allows SMS messages to be sent or received. SMS stands for Simple Message Services.</p> |
| statserveragent.ininlog | <p>StatServer subsystem component that handles agent-related statistics.</p> <p>\I3\IC\Server\StatServerAgent[U UD].exe</p> <p>This subsystem tracks statistical information for real-time views and historical reporting.</p> |
| statserverworkgroup.ininlog | <p>StatServer subsystem component that handles workgroup-related statistics.</p> <p>\I3\IC\Server\StatServerWorkgroup[U UD].exe</p> <p>This subsystem tracks statistical information for real-time views and historical reporting.</p> |
| SupervisorA.ininlog | Application log for Interaction Supervisor. |
| Switchover.ininlog | <p>SwitchoverService</p> <p>\I3\IC\Server\SwitchoverU.exe</p> <p>This is CIC's automated switchover system. If an CIC server ever fails, in less than 30 seconds the server can switch control to another mirror image CIC server with minimal phone disruption. In addition, the switchover scheme allows administrators to manually switch the "active" CIC server with no phone disruption.</p> |
| Tracker Server.ininlog | <p>Tracker Server</p> <p>\I3\IC\Server\TrackerSvrU.exe</p> <p>Interaction Tracker is composed of two server-side subsystems: Tracker Server and Tracker Tran Server (also called Transaction Server). Tracker Server listens for specific events from Queue Manager and inserts and updates interaction records.</p> |
| TransactionServer.ininlog | <p>Transaction Server</p> <p>\I3\IC\Server\TranServerU.exe</p> <p>Transaction Server processes insert and update requests from other CIC subsystems, sending those transaction requests to the CIC database server. Transaction Server also inserts, updates, and queries requests from Interaction Tracker Clients. This subsystem was previously called Tracker Tran Server.</p> |

| | |
|------------------------------|---|
| TsServer.ininlog | <p>TsServer</p> <p>\\I3\IC\Server\TsServerU.exe</p> <p>Telephony Services is the CIC subsystem that works with telephony hardware to perform telephony operations, such as phone dialing. The Telephony Services component allows the Interaction Center Platform to detect telephony events (e.g., incoming calls, DTMF digits, call disconnects, etc.) and to perform operations on telephone calls (e.g., transfer them, conference them together, record them, play audio to them, etc.).</p> <p>Telephony Services is the only CIC subsystem that interfaces directly with telephony hardware. Most CIC installations require telephony hardware. The telephony cards are installed in the CIC server and are connected to the Public Switched Telephone Network and all the phones in the company.</p> <p>This software layer provides a line of demarcation between the rest of Interaction Center and telephony hardware. All voice traffic coming from the Public Switched Network goes to the telephony hardware and it stays below that line. The Telephony Services software processes call data and then communicates to the telephony hardware the information necessary to direct the call to the correct party.</p> <p>Telephony Services integrates with analog, T1/E1, ISDN PRI, and IP-based telephone lines and works with international signaling standards such as EuroISDN, R2, Q.SIG, DPNSS, SS7, and so on. It answers incoming calls, places outgoing calls, reports call state information, performs call analysis, and detects answering machines. It captures DTMF digits, retrieves ANI, DNIS, CLID, and other call information, plays audio, and can record, transfer, and conference calls.</p> |
| VoiceXML Host Server.ininlog | <p>VXIHostServer</p> <p>\\I3\IC\Server\VXIHostServerU.dll</p> |
| WebProcessor.ininlog | <p>WebProcessor</p> <p>\\I3\IC\Server\WebProcessorU.exe</p> <p>Web Processor (WP) is the CIC subsystem that handles all incoming web interactions and internal intercom chats. It operates in conjunction with servlet process on a web server and acts as web interface into the CIC system. Web Services integrates with popular Web servers from vendors including Microsoft, Sun/iPlanet, IBM, Apache, and others to provide services such as Web collaboration, text chat, and Web call-back request processing.</p> |

Application logs

Subsystems aren't the only entities that create log files. Applications such as the CIC clients and Interaction Attendant write log files too. Application logs and subsystem logs serve the same purpose, but vary in content.

Location of application logs on your computer:

Application logs on a server are stored with subsystem logs. On a client machine, logs for locally installed CIC applications such as the CIC clients, Interaction Attendant, and so on, are stored in an **inin_tracing** folder in the Windows **%TEMP%** folder. The format of the path is:

%TEMP%\inin_tracing\yyyy_mm_dd

For example, if %TEMP% folder is C:\Windows\Temp, and the current date is 10/23/2016, the path would be:

C:\Windows\Temp\inin_tracing\2016_10_23

Log Viewer Procedures

Log Viewer is the Customer Interaction Center utility that reads application and subsystem logs. Log files provide a record of processing steps completed and they record the status of an application or subsystem at a specific point in time. For this reason, Log Viewer is useful for troubleshooting problems and for understanding the internal processing of software applications and CIC server subsystems.

Log Viewer reads entire trace logs or snips of log files. It can search log files for literal strings, find log entries that occurred at a specific time, locate specific types of log entries, manage bookmarks, color code entries, and filter logs to display only entries of interest. Log Viewer can display multiple logs and optionally synchronizes entries between logs.

The procedures in other topics explain how to perform common tasks in Log Viewer.

Access Help Topics

Log Viewer includes an online help file in HTML Help format.



What's the quickest way to open help? Press the *Help* toolbar button. Alternately, the *Help* menu provides commands that open help topics.

Help > Contents

Opens the online help file with the table of contents pane displayed. This allows you to see the relationship between help topics in the file.

Help > Index

Opens the online help file with the index pane displayed. This allows you to search the file for specific index entries.

Help > Search

Opens the online help file with the search pane displayed. This allows you to perform a keyword search.

Access version information

The **Help > About** command displays version information about Log Viewer. See [About dialog](#) for details.

Analyze distinct context attribute values

Context Attributes tag log entries to identify a data element of some sort, such as a CallId or a specific user name. Subsystems add context attributes to individual log entries to associate a message with a specific item of information that can be used to group or filter data.

The **Tools > Analyze Distinct Context Attribute Values** command allows you to select a context attribute from a list, and view the value of that attribute in all instances contained in the log file. For example, if you click **Analyze Distinct Context Attribute Values > connection.i3inet** on the **Tools** menu, Log Viewer lists all instances of this attribute:

ININ Log Viewer - [Context Attribute connection.i3inet Report]

File Edit View Tools Search Windows Help

Usages of context attribute connection.i3inet in D:\I3\IC\Logs\2017-12-05\recorder server.ininlog:

| Value | First Seen (C) | Last Seen (C) | Count |
|-------|----------------|----------------|-------|
| 2044 | 00:02:44.83... | 00:03:12.83... | 2 |
| 2045 | 00:07:44.84... | 00:08:12.85... | 2 |
| 2046 | 00:12:44.86... | 00:13:12.86... | 2 |
| 2047 | 00:16:17.48... | 00:16:45.49... | 2 |
| 2048 | 00:17:44.87... | 00:18:12.88... | 2 |
| 2049 | 00:22:44.89... | 00:23:12.89... | 2 |
| 2050 | 00:27:44.90... | 00:28:12.91... | 2 |
| 2051 | 00:32:44.92... | 00:33:12.92... | 2 |
| 2052 | 00:37:44.94... | 00:38:12.94... | 2 |
| 2053 | 00:42:44.96... | 00:43:12.96... | 2 |

Done.

Message Detail (\$Id: //core/main_systest/int/src/i3trace/binlog_sink.cpp#8 \$:387)

BinLogSink::create_log() : D:\I3\IC\Logs\2017-12-05\recorder server.ininlog

To close this view, click on the close box in the parent window, or use one of the jump commands in the toolbar to move to a specific instance of the attribute in the file.

Columns in the list view

Value column

This column lists the value of the context attribute for a log message.

First Seen column

The time when an attribute with this name and value was first found in the log.







Last Seen column

The time when an attribute with this name and value was last found in the log.

Count column

The number of instances of this context attribute with this value.

When the list of context attributes is displayed, the toolbar options are:

| Icon | Shortcut | Command |
|---|----------|---|
|  | Ctrl+O | Open log file invokes the File Open dialog , so that you can open another log. |
|  | F4 | Jump to First Seen Time jumps to the location in the log file where this context attribute value was found for the first time. |
|  | Shift+F4 | Jump to Last Seen Time jumps to the location in the log file where this context attribute value was found for the last time. |
|  | F5 | Refresh Display performs a manual refresh of the log. |
|  | none | Toggles display of the Source View pane, which displays source code from the function that wrote the selected log entry (feature is available for Genesys internal use only). |
|  | None | Displays application help file. See Access Help Topics . |

Apply a quick string filter


It's easy to select only those entries that contain a literal string. The command is:

| Keyboard | Menu Command |
|----------|------------------------------|
| Ctrl-F | Filter > Quick String Filter |

See [Find Text](#) for details.

Clear All Filters


This command removes all filters except for [global time range filters](#).

| Toolbar | Menu Command |
|---|----------------------------|
|  | Filter > Clear All Filters |

Clear Global Time Range Filter

This command removes a global time range filter that you have [set](#) to exclude all log entries that fall outside of specified start and end times. Once you set a global time range filter, you can apply additional filters to narrow down results.

Unlike regular filters, global time range filters are not removed By the [Clear All Filters command](#). You must use this command to remove global time range filters. To clear a global time range filter, use one of the following methods:

| Toolbar | Menu Command |
|---|---|
|  | Filter > Clear Global Time Range Filter |

Clone a log window

Log Viewer provides a Multiple Document Interface (MDI), meaning that its primary window hosts document windows for each open log. Cloning a log window creates a new instance of the currently open file, using identical filter criteria.

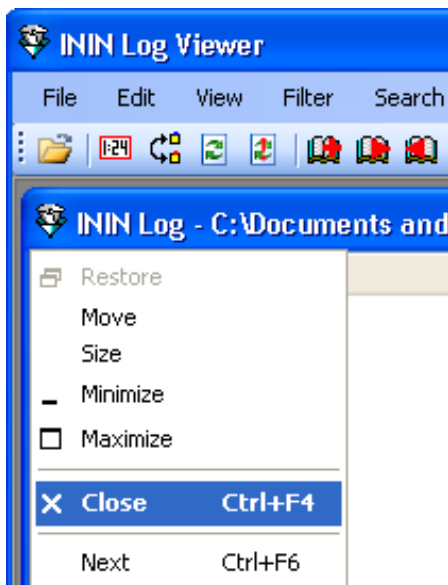
To clone a log window:

1. Click on the log file to clone.
2. On the File menu, click **Clone Log Window** (or press Ctrl-N). A new window appears with identical contents. This allows you to experiment with filter and trace settings without affecting the contents of the original window.

Close a log file

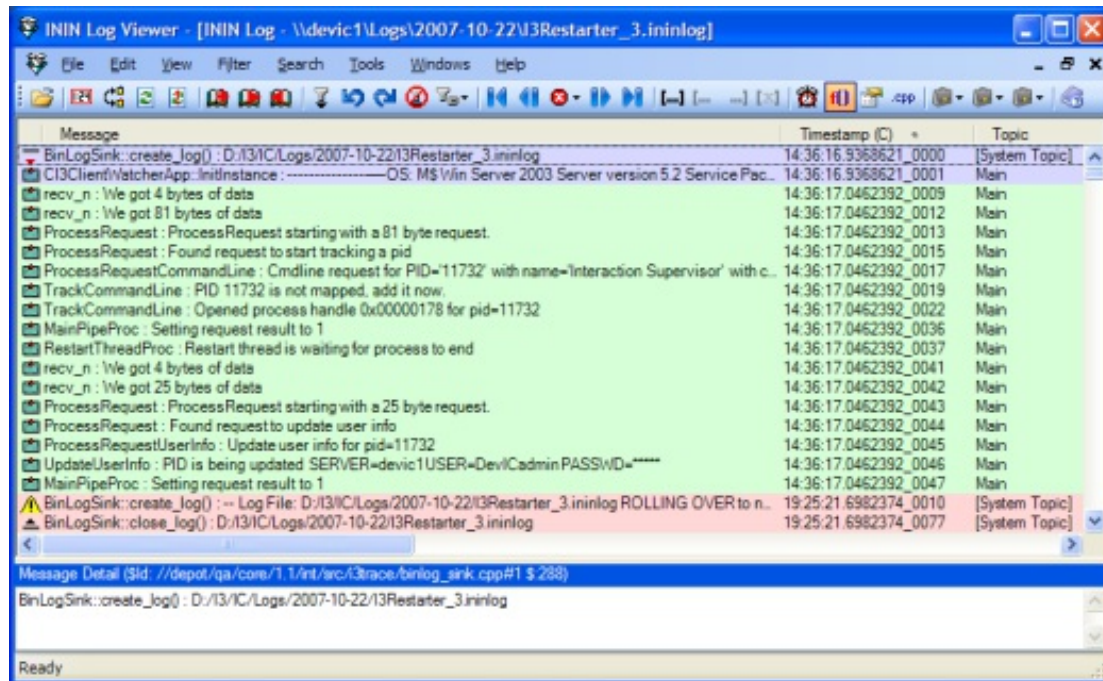
There are several ways to close an open log file.

1. If multiple log files are open, click on the file you want to close, to give it focus.
2. On the **File** or **Control** menu, click **Close**.



Colorize columns in the message list

Clicking on a column heading colorizes messages by type, to make messages easier to identify. For example, if you click on the timestamp column, messages are color-coded to group each 1-second tick of the clock. The time interval is configurable—see [Options Dialog – Misc tab](#).



Colorizing does not change the order of entries in the messages list. It merely changes the background color of each entry, based on a column or regular expression.

Note: Individual colors do not have any special significance. Color is used in log viewer to group related data and to distinguish log entries. There is no correlation between a given log color and any particular type of data.

If you click **Color Column** on the **View** menu, you can select a column to colorize by from a context menu. If the message list contains many columns, it is easier to use the menu command than it is to scroll the list horizontally to locate a column to click on.

Regular Expressions

If you click **By Regular Expression** on the context menu, the [Enter Coloring Regular Expressions](#) dialog will appear. This dialog allows you to define a pattern of text to search for and colorize.

Clearing Colors

To remove coloring, on the **View** menu, click **Color Column > None**. This changes the background color for all messages to white.

Related Topics

- [Enter Coloring Regular Expressions dialog](#)
- [Search forward or backward by message color](#)

Control log verbosity

The degree of detail written to logs is determined by setting *trace levels* for *topics* in each subsystem. A subsystem typically logs messages when it passes control to a routine, encounters a problem, or otherwise needs to record work performed.

Care must be taken to use an appropriate level of verbosity, since logs can quickly grow large and add overhead to the system. The CIC utilities that manage log verbosity are *CIC System Manager* and *Trace Configuration Utility*. Each is discussed later in this document.

Trace Topics

The routines that write messages are called **trace topics**. Trace Topics correspond to subroutines invoked by a subsystem, or to some type of major functionality provided by an application. Every subsystem and application has its own set of trace topics.

Trace Levels

Each topic has a numeric **trace level** setting that controls the verbosity of messages written about that topic. Not all messages are equally important. Messages from some routines are more important than others.

Trace levels are sometimes called *topic levels*, since people tend to combine both terms. *Topic* is the subject traced and *level* controls to what degree the topic is traced.

Trace levels are numeric values that determine which messages are logged for a topic, based upon the severity of the message. The table below shows the range of numeric values that correspond to common trace settings. For example, a trace level in the 0-10 range would log only critical errors, while a trace setting of 100 would log every message generated by the topic.

| Severity | Range | Description |
|----------|-------|--|
| Critical | 0-10 | Only critical errors (those impacting features) will be logged. |
| Error | 11-20 | Any error conditions will be logged. |
| Warning | 21-40 | Any warning conditions will be logged. |
| Status | 41-60 | Operations are logged. |
| Notes | 61-80 | Operations including details are logged. |
| Verbose | 81-99 | Sub-operation details are logged. |
| All | 100 | All trace statements within the program are enabled (This will generate very large log files.) |

The higher the trace level, the more information will be logged. With a few exceptions, most subsystems start with the default tracing level configured to "Status" level (which includes status messages, warnings, and errors) or lower. Each trace level includes all levels below it.

A trace level of "Status" or lower will return some log information, but usually not enough for a support engineer to determine the root cause of a problem. Tracing usually must be at Notes level or higher for support engineers to troubleshoot an CIC system accurately.

Without question, logs make it easier to troubleshoot an CIC system. Genesys support professionals use logs to locate the source of system malfunctions. Customers can also view logs to examine the inner workings of the system.

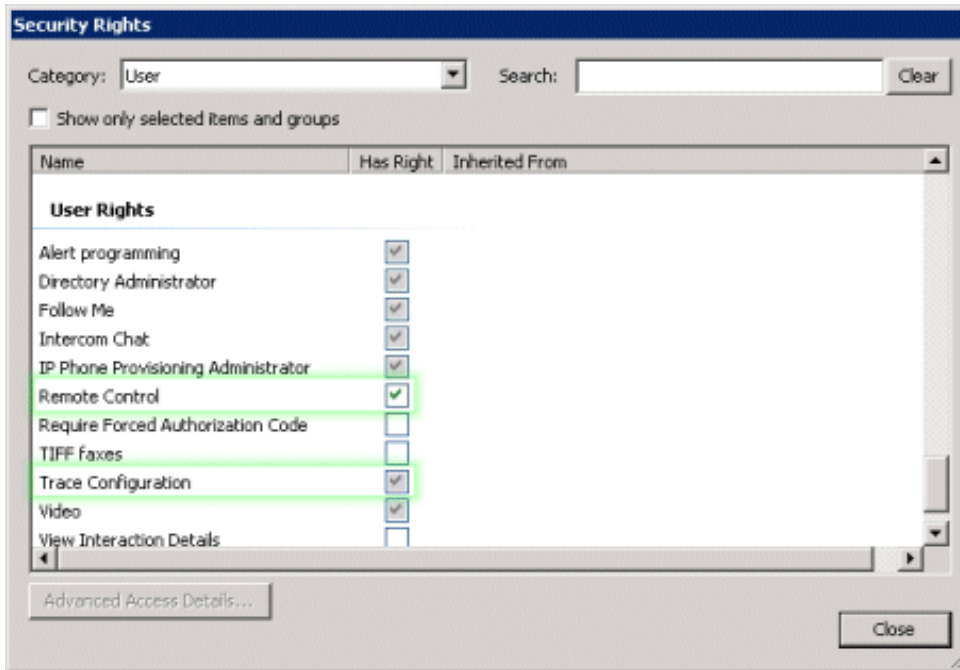
Use CIC System Manager to set trace levels

The level of detail logged is set by the [CIC System Manager](#) utility or the [Trace Configuration Utility](#). If tracing is set to a verbose mode or if many actions are logged, the log files can grow to be very large.

Grant permission to run IC System Manager

To set trace levels for subsystem topics, a user must have permission to access IC System Manager. Permission must be granted in Interaction Administrator, on the **User Rights** tab of a **User Configuration** entry:

1. Start Interaction Administrator.
2. Expand the **People** container, and then click on the **Users** container.
3. Double-click the name of the user who needs the access rights. The **User Configuration** dialog appears.
4. Click **Security Rights**. Scroll down to the **User Rights** group.



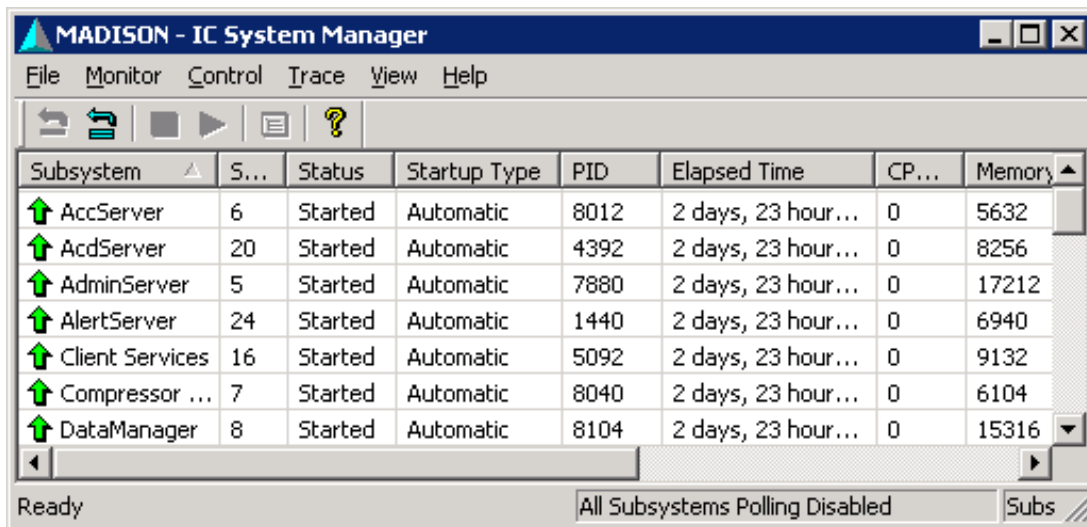
5. Select the **Remote Control** check box to allow the user to run IC System Manager. IC System Manager is a tool used to configure tracing.
6. Select the **Trace Configuration** check box to allow the user to configure tracing using IC System Manager or the Trace Configuration utility.
7. Click **Close** to dismiss the **Security Rights** dialog.
8. Click **OK** to dismiss the **User Configuration** dialog.
9. Close Interaction Administrator.

Use CIC System Manager to set trace levels

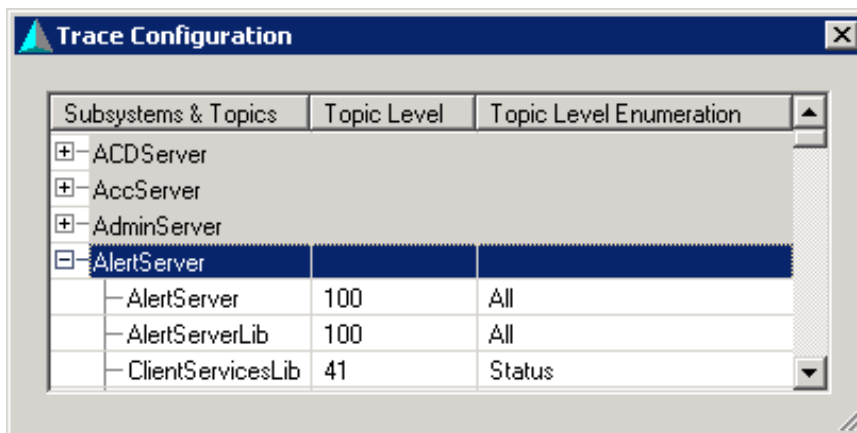
When you launch Customer Interaction Center, each subsystem starts based on its location within the CIC process tree. CIC System Manager acts as a graphical user interface to Remoco Server when Customer Interaction Center is running as a service. CIC System Manager can query, stop, restart, and trace the CIC server subsystems.

To change the tracing level:

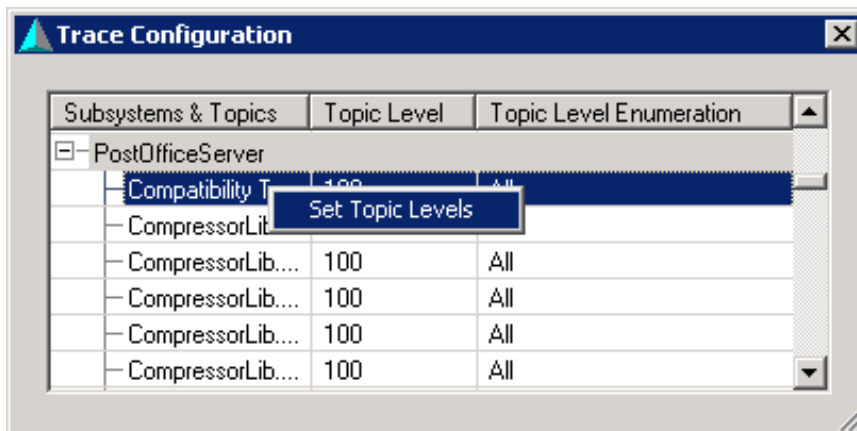
1. Start **IC System Manager** if it is not already running. To do this, click **Start**, and then select **Programs > PureConnect > CIC System Manager**.



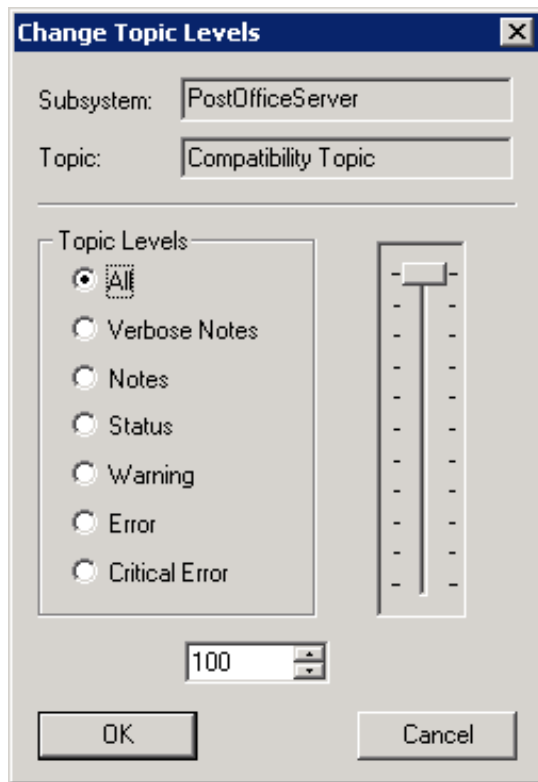
- By default, CIC System Manager lists only subsystems that are controlled by Remoco Server. To view the complete list of subsystems on the CIC server, on the **Trace** menu, click **All Trace Configuration**. A secondary **Trace Configuration** window lists the additional items.



- Click a subsystem to expand its list of trace topics.
- Right-click the Topic whose trace level you want to change, and then select **Set Topic Levels** from the context menu.



This opens the **Change Topic Levels** dialog. The Topic Level can be set using the slider control, by selecting a radio button, or by using the spin control to set a value. Each trace level includes all levels below it.



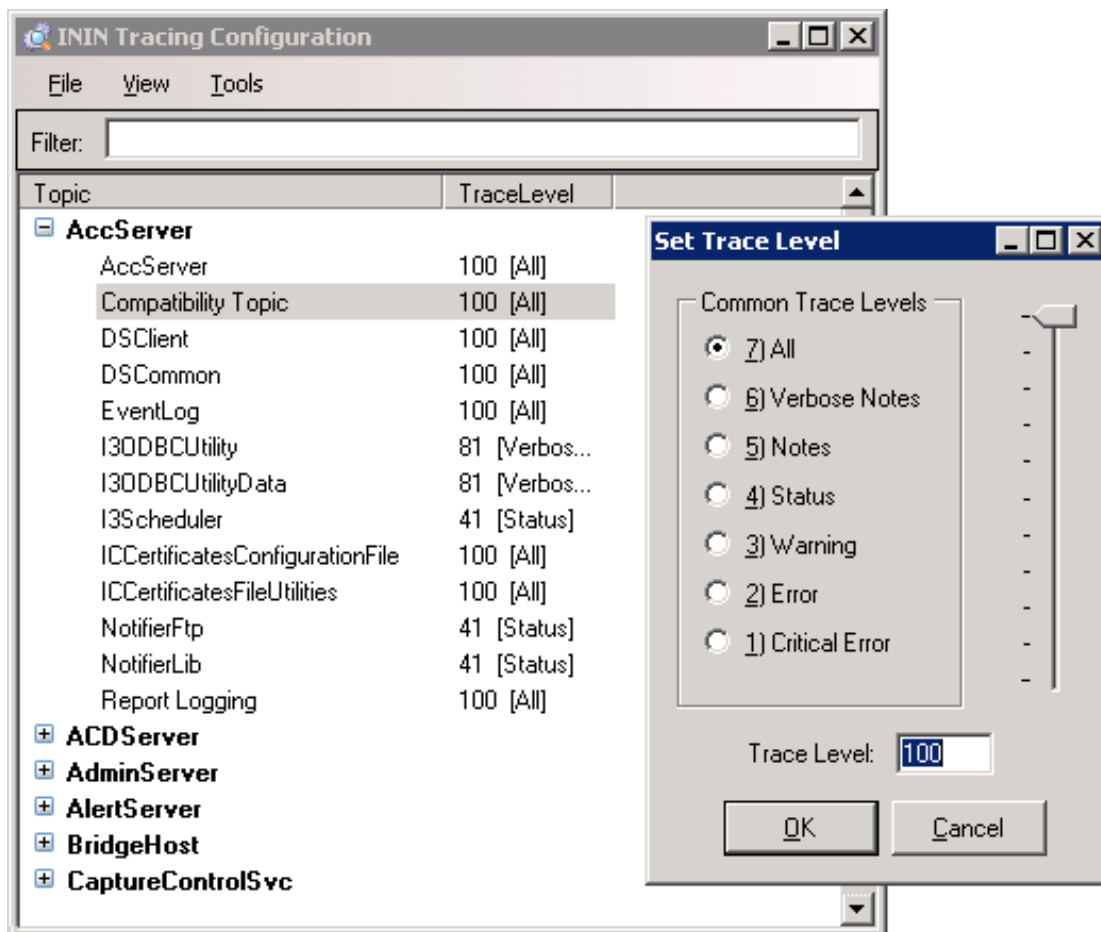
| Severity | Range | Description |
|----------|-------|--|
| Critical | 0-10 | Only critical errors (those impacting features) will be logged. |
| Error | 11-20 | Any error conditions will be logged. |
| Warning | 21-40 | Any warning conditions will be logged. |
| Status | 41-60 | Operations are logged. |
| Notes | 61-80 | Operations including details are logged. |
| Verbose | 81-99 | Sub-operation details are logged. |
| All | 100 | All trace statements within the program are enabled (This will generate very large log files.) |

Be careful. "Notes" level tracing or higher should only be activated when troubleshooting a system. Notes level or higher returns large amounts of log data. This requires more processing power from the system and more hard drive space to store the additional log information. Only increase the trace levels on subsystems that the support engineer has requested. Once a problem has been identified and fixed, the trace levels should be returned to the original settings for each subsystem.

6. When you finish, click **OK**.
7. Close the **Trace Configuration** dialog box, or repeat steps 3-5 to change the trace setting for another topic.
8. Close **CIC System Manager**.

Use Trace Configuration utility to set trace levels

The **Trace Configuration Utility** (Trace Config for short) sets trace log verbosity (trace levels) and determines which topics are logged. These settings greatly affect the size of a log file and its contents.



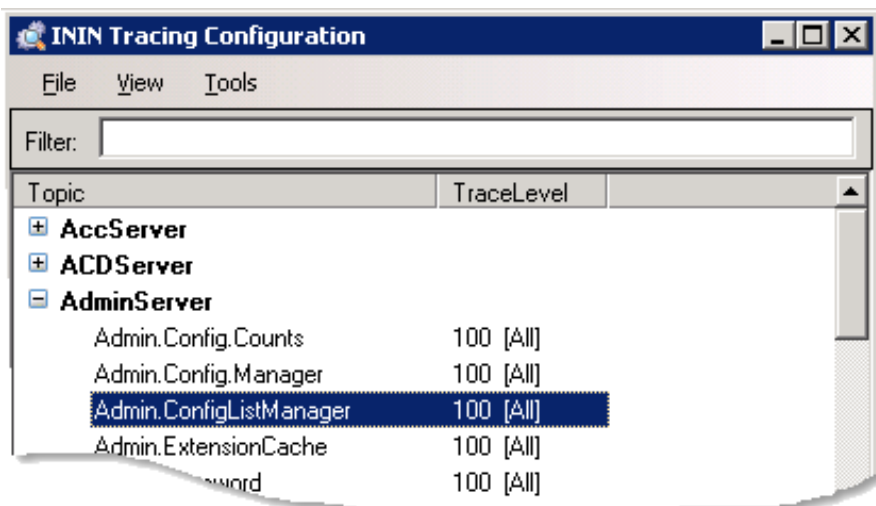
The executable name of this utility is:

"D:\I3\IC\ININ Trace Initialization\inintraceconfig-w32r-1-2.exe"

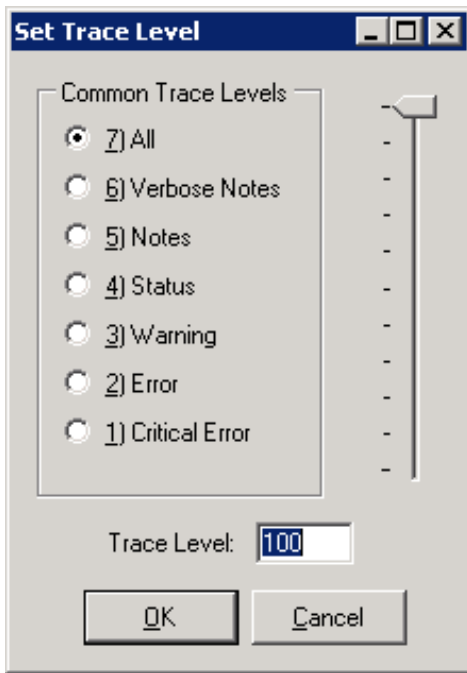
How to set Trace Level using Trace Config

To set a trace level using Trace Config, follow these steps:

1. If you are running Log Viewer, on the **Tools** menu, click **Launch TraceConfig**.
2. Click a subsystem to expand its list of topics.



3. Double-click a topic to edit its trace level:



4. Use the slider, spin control, or radio buttons to change the trace setting. Use the table below as a guide:

| Severity | Range | Description |
|----------|-------|--|
| Critical | 0-10 | Only critical errors (those impacting features) will be logged. |
| Error | 11-20 | Any error conditions will be logged. |
| Warning | 21-40 | Any warning conditions will be logged. |
| Status | 41-60 | Operations are logged. |
| Notes | 61-80 | Operations including details are logged. |
| Verbose | 81-99 | Sub-operation details are logged. |
| All | 100 | All trace statements within the program are enabled (This will generate very large log files.) |

5. Click **OK** to close the **Trace Level** dialog box.
6. Repeat steps 2-4 to set other trace levels for another topic or subsystem. When you finish, on the **File** menu, click **Exit** to close the Trace Configuration utility.

Related Topics

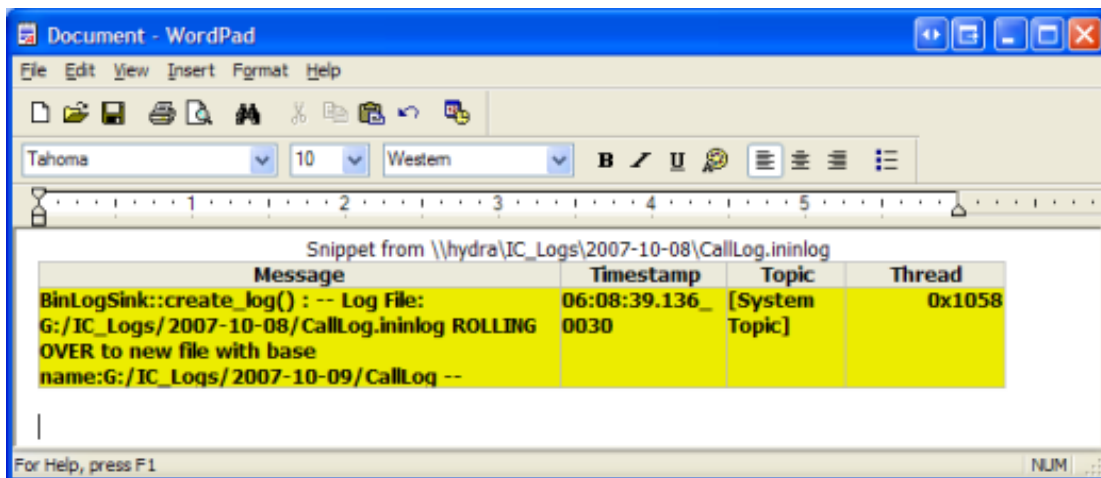
- [Control Log Verbosity](#)
- [Launch TraceConfig](#)

Copy log entries to other applications using the clipboard

This topic explains how to copy log entries to the clipboard in various formats, so that you can paste data into other applications. Log Viewer provides clipboard support for plain text, RTF, HTML tables, and CSV (Comma-Separated-Values).

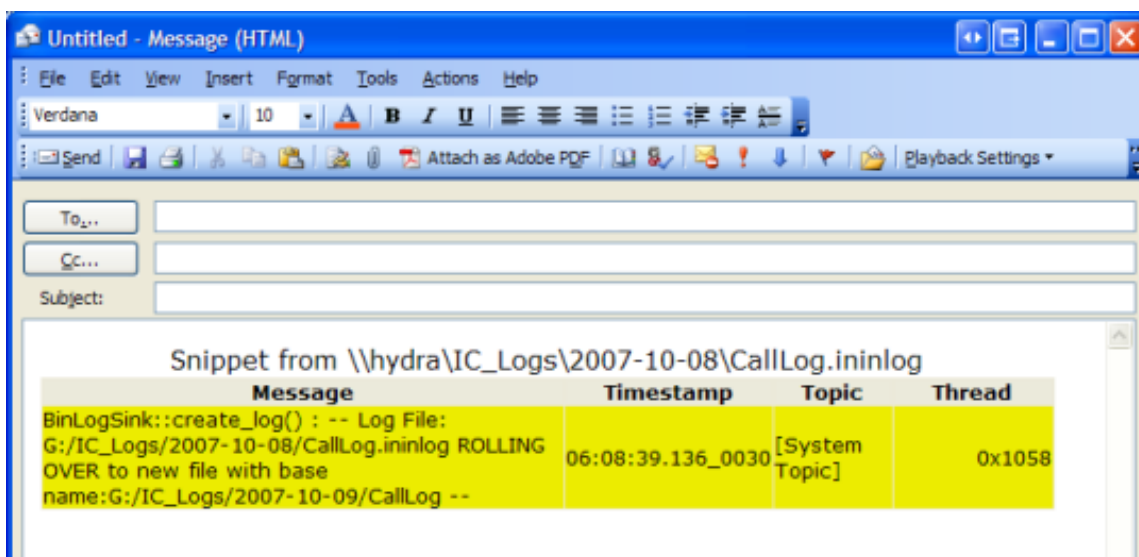
1. Select one or more log entries.
2. On the **Edit** menu, click **Copy** or **Copy As**.

If you select **Copy** or **Copy As > Rich Text**, the entry is stored on the clipboard in Rich Text format. When you paste it into an application that recognizes the RTF format, it looks something like this:

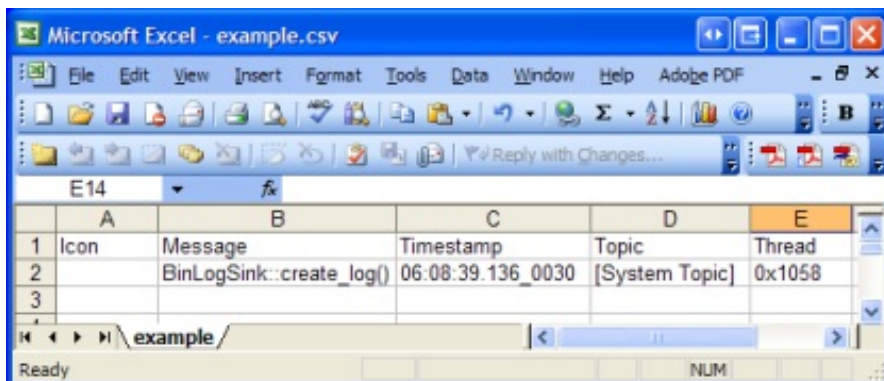


To place a selection on the clipboard as Plain Text, select **Copy As > Simple Text** from the **Edit** menu. Almost any application can accept plain text from the clipboard.

To place a selection on the clipboard in HTML Table format, select **Copy As > HTML Table** from the **Edit** menu. Then, you can paste the content into applications that support HTML, such as Microsoft Office Outlook:



To place a selection on the clipboard in CSV (comma-separated values) format, select **Copy As > CSV Text** from the **Edit** menu. The resulting plain text is stored on the clipboard using commas to delineate columns in the log entry. If you paste CSV text into Notepad and save the file with a .csv extension, you can open it in Excel:



3. Paste the text into any application that supports the selected clipboard format.

Decrypt a log message

Logs are not encrypted, but some log elements in a log (passwords for example) can be encrypted by a subsystem. Here's what an encrypted log entry looks like:

| Message | Encryption Key Id |
|---|-------------------|
| main() : Trace out an encrypted message[*** DATA ENCRYPTED - KEY NEEDED! ***] | database password |

In this example, the encrypted portion of the message is displayed as [*** DATA ENCRYPTED - KEY NEEDED! ***]

To decrypt a log message

1. Select the encrypted log message.
2. Look in the *Encryption Key Id* column for a hint to the keyword or pass phrase needed to decode the message. Encryption key Id is a string that indicates what key should be used to decrypt. For example, the Encryption Key Id might be "login password", "database password", or some other hint. If the *Encryption Key Id* column isn't visible, you may need to [add that column](#) to the display.
3. Right-click the message and select *Decrypt Message* from the context menu. The [Message Decryption Key dialog](#) will appear.
4. Enter the key or passphrase needed to decode the entry, based on hints in the Encryption Key Id column. Then press OK. If a valid value was entered, the log will display the unencrypted value in place of "[*** DATA ENCRYPTED - KEY NEEDED! ***]".

Related Topics

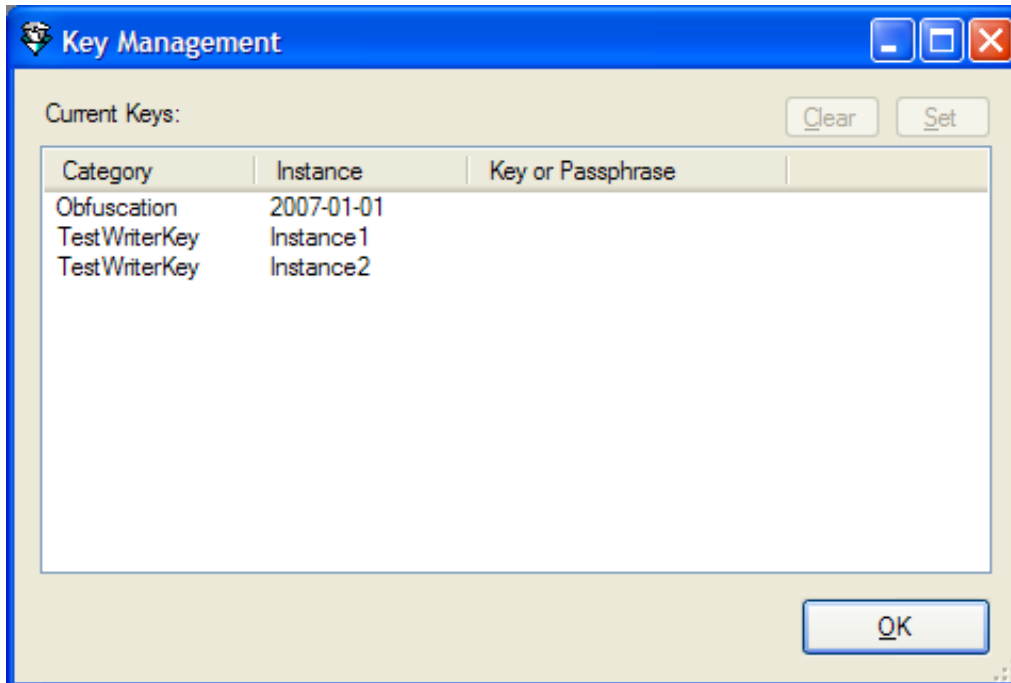
- [Message Decryption Key dialog](#)
- [Manage Columns in the message list](#)
- [Decrypt multiple log messages](#)

Decrypt multiple log messages

If a log contains many entries with encrypted elements, you have the option to enter keys and passphrases for multiple entries, without having to locate entries in the message list.

To decrypt multiple messages, follow these steps:

1. On the **Tools** menu, click **Key Management**. The [Key Management dialog](#) appears, listing category and instance values that hint at the key or passphrase needed to decrypt each entry.



2. Click **Set** or double-click a row in the list of current keys to open the [Message Decryption Key dialog](#).



3. Type the needed key or passphrase in the **Key** or **Passphrase** field, and then click **OK**.

Delete a log file

To delete the currently open log file.

1. Click on the window to give it focus.
2. On the **File** menu, click **Delete Log**.
3. When the confirmation message appears, click **Yes**.

Delete a saved filter

Once you have [saved a filter](#), its name appears in the **Filter** menu under **Saved Filters**. To remove a saved filter, follow these steps:

1. On the **Filter** menu, click **Saved Filters > Delete Saved Filter**.
2. Select the name of the filter to remove from the context menu.

Display log header information

The **View > Log Header** command displays information about the current log file.

Related Topics

- [Log Header dialog](#)

Exit Log Viewer

Closing Log Viewer ends the application and closes any open logs.

To close Log Viewer, do one of the following::

- On the **File** menu, click Exit.
- Click the Log Viewer's close box:



Export to File

File > Export to File exports messages that match the current filter to a new log file. This allows you to save the results of a filter to a new file.

1. Open a log file.
2. Apply filters as needed to select a subset of log entries.
3. On the **File** menu, click **Export to File**.
4. When the [Export Output File dialog](#) appears, type a name for the log, and then click **Save**.

Find Text

Log files are easy to search for literal strings or patterns of text using regular expressions:

1. Open the [Find Text dialog](#). There are two ways to do this, depending upon whether you want to search forward for backward through the file.
 - To search forward, type **Ctrl-F** or select *Search Forward* from the **Edit** menu.
 - To search backward, type **Ctrl-Shift-F** or select *Search Backward* from the **Edit** menu.
2. Type a search string in the **Text to Find** field. If you select the **use regular expressions** check box, you can enter the pattern for an expression in this field.
3. Set other options, such as whether or not the search should be case-sensitive.
4. Click **OK** to start the search. If the search succeeds, a search result is selected in the message view. Otherwise a beep sounds to indicate an unsuccessful search.

Repeat searches

To search forward again, press **F3** or select **Search Forward Again** from the **Edit** menu. To search again in a backward direction, press **Shift+F3** or select **Search Backward Again** from the **Edit** menu.

Change search criteria

Press **Ctrl-F** to re-open the **Find Text** dialog box.

Import Filters

Filters are saved in .xml files that you can import from a local directory or network share. Importing filters adds the names of saved filters to your list of saved filters, which appears below the *Filter* menu under *Saved Filters*.

To import filters:


1. On the **Filter** menu, click **Saved Filters > Import Filters From**.
2. In the [File Open dialog](#), navigate to the directory that contains saved filters.
3. Click **OK**.

Jump to Matching Scope/Create

Scope refers to the range of messages between matching "enter scope" and "exit scope" messages.

| Timestamp (C) | Message | |
|-----------------------|---|--|
| 20:11:46.3355811_0004 | create_log_file() : Construct Object 0x#00#00 | |
| 20:11:46.3355811_0005 | create_log_file() : Destruct Object 0x#00#00 | |
| 20:11:46.3355811_0006 | create_log_file() : | |
| 20:11:46.3355811_0007 | create_log_file() : | |
| 20:11:46.3355811_0008 | create_log_file() : END SECTION USERMESSAGE TYPEMATCH | |
| 20:11:46.3355811_0009 | create_log_file() : BEGIN SECTION FUNCTION NAME MATCH | |
| 20:11:46.3355811_0010 | create_log_file() : Function Name Test message | |
| 20:11:46.3365577_0000 | create_log_file() : END SECTION FUNCTION NAME MATCH | This is an enter scope message |
| 20:11:49.3366729_0000 | create_log_file() : BEGIN SECTION CALL LEVEL MATCH | |
| 20:11:49.3366729_0001 | create_log_file() : Level 0 | |
| 20:11:49.3366729_0002 | helper_call_level_match_foo() : Level 1 | |
| 20:11:49.3366729_0003 | helper_call_level_match_bar() : Level 2 | |
| 20:11:49.3366729_0004 | helper_call_level_match_bar() : | |
| 20:11:49.3366729_0005 | helper_call_level_match_bar() : | |
| 20:11:49.3366729_0006 | helper_call_level_match_bar() : | |
| 20:11:49.3366729_0007 | helper_call_level_match_bar() : | |
| 20:11:49.3366729_0008 | create_log_file() : END SECTION CALL LEVEL MATCH | This is an enter scope message too (a nested scope) |
| 20:11:52.3367881_0000 | create_log_file() : BEGIN SECTION TRUST LEVEL MATCH | |
| 20:11:52.3367881_0001 | create_log_file() : Default Trust Level | |
| 20:11:52.3367881_0002 | create_log_file() : Trust Level 20 | |
| 20:11:52.3367881_0003 | create_log_file() : Trust Level 20 again | |
| 20:11:52.3367881_0004 | create_log_file() : Trust Level 20 yet again | |
| 20:11:52.3367881_0005 | create_log_file() : Trust Level 140 | |
| 20:11:52.3367881_0006 | create_log_file() : END SECTION TRUST LEVEL MATCH | This is the matching exit scope for the nested scope |
| 20:11:55.3369033_0000 | create_log_file() : BEGIN SECTION THREAD ID MATCH | This is the matching exit scope message |

The enter/exit messages have a unique icon that looks like an arrow. If you open a log and put the focus on an "enter scope" message and clic **Jump to Matching Scope**, the focus jumps to the matching enter/exit scope, whether that is forward or backward from the current position. If you are on a regular Note, Warning, or Error message, then that action has no matching twin and a beep sounds.

| Toolbar | Keyboard | Menu Command |
|---|----------|--|
|  | Ctrl+E | Search > Jump to Matching Scope/Create |

The "create" part refers to the "start logging" and "stop logging" messages. If you're in a standard log an on the first message (the 'start logging' message) and press the button it jumps to the last line where the log is closed. That is not very interesting, but if you [snip or merge log files](#), then this command has more meaning.


Related Topics

- [Use Search menu commands to trace call levels](#)

Jump to (or near) a specific timestamp

If you know when an event occurred, you can navigate to a specific point in time. Here's how to select the message entry that exactly (or most nearly) matches a timestamp:

1. Use any of the methods below to issue the Jump To Specific Timestamp command.

| Toolbar | Keyboard | Menu Command |
|---|----------|-------------------------------------|
|  | Ctrl+T | Search > Jump to Specific Timestamp |

2. Use the [Timestamp Selection dialog](#) to select a date and time.
3. Click **Jump**.

Related Topics

- [Use Search menu commands to trace call levels](#)
- [Jump to next/previous thread message](#)

Jump to next/previous thread message

Threads are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process. More than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled.

The commands below allow you to navigate between message threads:

| Keyboard | Menu Command |
|----------|--|
| F4 | Search > Jump to Next Thread Message |
| Shift+F4 | Search > Jump to Previous Thread Message |

Related Topics

- [Use Search menu commands to trace call levels](#)
- [Jump to \(or near\) a specific timestamp](#)

Launch TraceConfig utility

The **Tools > Launch TraceConfig** command opens the [Trace Configuration Utility](#). It sets trace log [verbosity](#) (trace levels) and determines which topics are logged. These settings greatly affect the size of a log file and its contents.

Manage columns in the message list

Use the **View > Manage Columns** command to control which columns are visible in the message list. This command opens the [Change Columns](#) dialog, so that you can select columns to view from a list of available columns. See [Logged Columns](#) for definitions of each column.

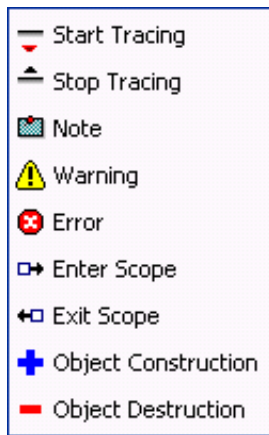
1. From the **View** menu, select **Manage Columns**.
2. The [Change Columns](#) dialog box appears.
3. Do any of the following:
4. To make a column visible, select an item from the **Available Columns** list, and then click **Add**.
5. To hide a column, select an item from the **Visible Columns** list, and then click **Remove**.
6. Use the **Up** and **Down** buttons to reorder the items left-to-right in the **Visible Columns** list.
4. Click **OK** to apply the changes.

Logged Columns

The table below describes columns in a log file. To control the visibility and order of columns, see [Manage Columns in the Message List](#).

Icon

Icons describe the type of log message. The icons are:



Message

The message text.

Timestamp

The time when the message was logged, in hh:mm:ss:mmm_nnnn format. This notation stands for hours, minutes, seconds, milliseconds, and nanoseconds, in up to 9 digits of precision. However, time slices smaller than 15 ms have little meaning, since the overhead of the operating system must be considered. Timestamps are also incremented using series numbers to relate entries within a time span.

Topic

The routines that write log messages are called trace *topics*. Trace topics correspond to subroutines invoked by a subsystem, or to some type of major functionality provided by an application. Every subsystem and application has its own set of trace topics.

Level

Each topic has a numeric *trace level* setting that controls the verbosity of messages written about that topic. Not all messages are equally important. Messages from some routines are more important than others.

Trace levels are sometimes called topic levels, since people tend to combine both terms. Topic is what is traced, level controls how much. Trace levels are numeric values that determine which messages are logged for a topic, based upon the severity of the message.

Thread

Threads are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process and more than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled. The thread context includes all of the information the thread needs to seamlessly resume execution, including the thread's set of CPU registers and stack, in the address space of the thread's host process.

Type

The *Type* column is the textual equivalent of the *Icon* column. The message types are *Start Tracing*, *Stop Tracing*, *Note*, *Warning*, *Error*, *Enter Scope*, *Exit Scope*, *Object Construction*, and *Object Destruction*.

Subsystem

The name of the CIC subsystem that wrote the log entry. The Interaction Center platform is composed of software components, called subsystems. These components are written in the C++ language to maximize performance. Individual subsystems are coordinated by a central communication hub known as the Notifier.

Call Level

Call Level (or call stack, if you prefer) is an indicator of functions calling other functions. The first calling function is level 0. If the

main function calls a helper function, the helper is considered to be at call level 1, and so forth. Call levels help trace the flow of control from one function to another.

In Exception

This Boolean flag is True when if the module was in an exception handler when the message was logged. Since exceptions alter a program's flow of control, this flag helps indicate that customary statements may not have been written due to an exception.

Function

Function indicates the name of the source code subroutine (called function) that wrote the log entry, in the form: Library:Class:Subroutine. For example: DispatcherLib::JobWaitlist::EnqueueJob()

Filename

The path to the source code file in the code management system.

Line

The line number in the source code file that corresponds to the message entry.

Trust Level

The level of trust assigned to an assembly, which affects what system resources the function had access to.

Logfile

The fully qualified path to the log file.

Encryption Key Id

This column displays the string that was used to encrypt a portion of the log entry. Logs are not encrypted, but some log elements in a log (passwords for example) can be encrypted by a subsystem. Here's what an encrypted log entry looks like:

| Message | Encryption Key Id |
|---|-------------------|
| main() : Trace out an encrypted message[*** DATA ENCRYPTED - KEY NEEDED! ***] | database password |

Encryption key Id is a string that indicates which key should be used to decrypt. For example, the Encryption Key Id might be "login password" or "database password". To decrypt the entry, the user would have to enter the appropriate password for the user account or database.

In this example, the encrypted portion of the message is displayed as [*** DATA ENCRYPTED - KEY NEEDED! ***], and the Encryption Key Id is "database password".

The topic titled [Decrypt a log message](#) explains how to decode messages.

Thread Name

The name of the thread, if the thread has a name.

This pointer

The pointer to a data structure internal to the code. If you are operating on a function that is part of a data object, *this pointer* indicates which data object.

Dynamically Assigned Columns

You may see columns other than those that are listed here. Some columns are dynamically defined for a particular type of log, if the column has meaning only in the context of that log type.

Manage Window Settings

Commands in the **Windows** menu allow you to manage the position of open log file windows, and perform other functions, such as closing several windows at once.

Windows > Cascade

This command arranges windows so that they slightly overlap one another. This makes it easy to activate a window by clicking on its title bar.

Windows > Tile Vertical

This command resizes and positions windows vertically to appear side by side.

Windows > Tile Horizontal

This command resizes and positions windows horizontally to appear side by side.

Windows > Close All

Closes all open windows.

Windows > Close Others

Closes all windows except the window that has focus.

Windows > Arrange Icons

This command arranges minimized windows within the parent application window.

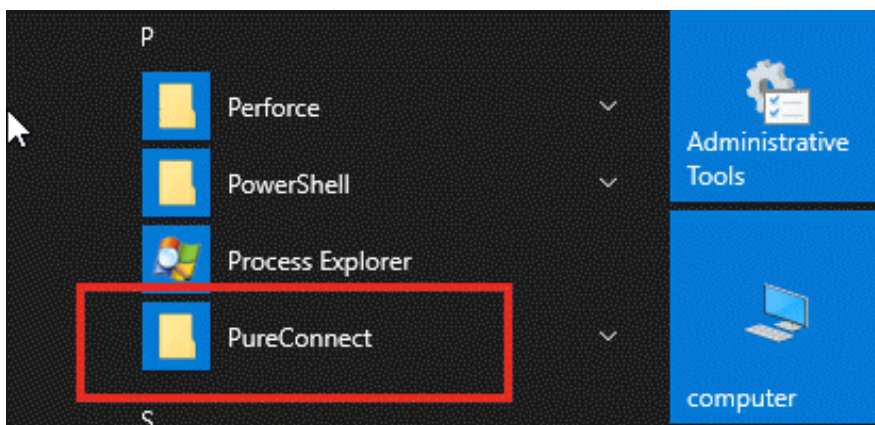
Activate a Log Window

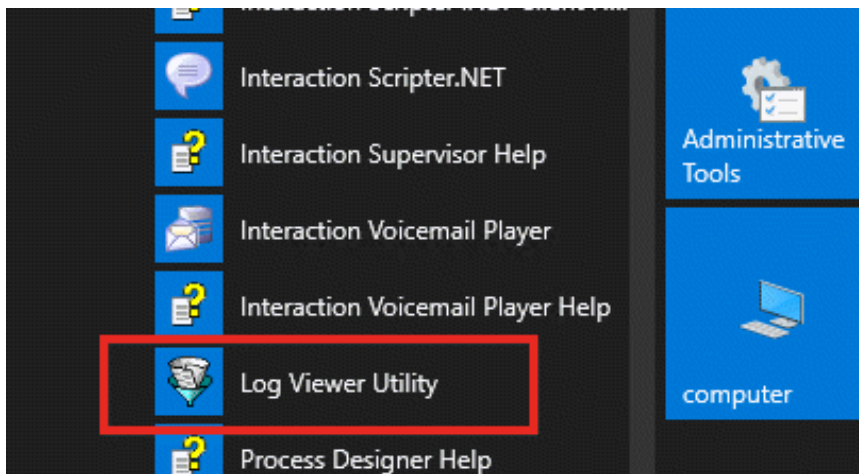
A numbered list at the bottom of the menu allows you to select an open window to make topmost.

Open a log file

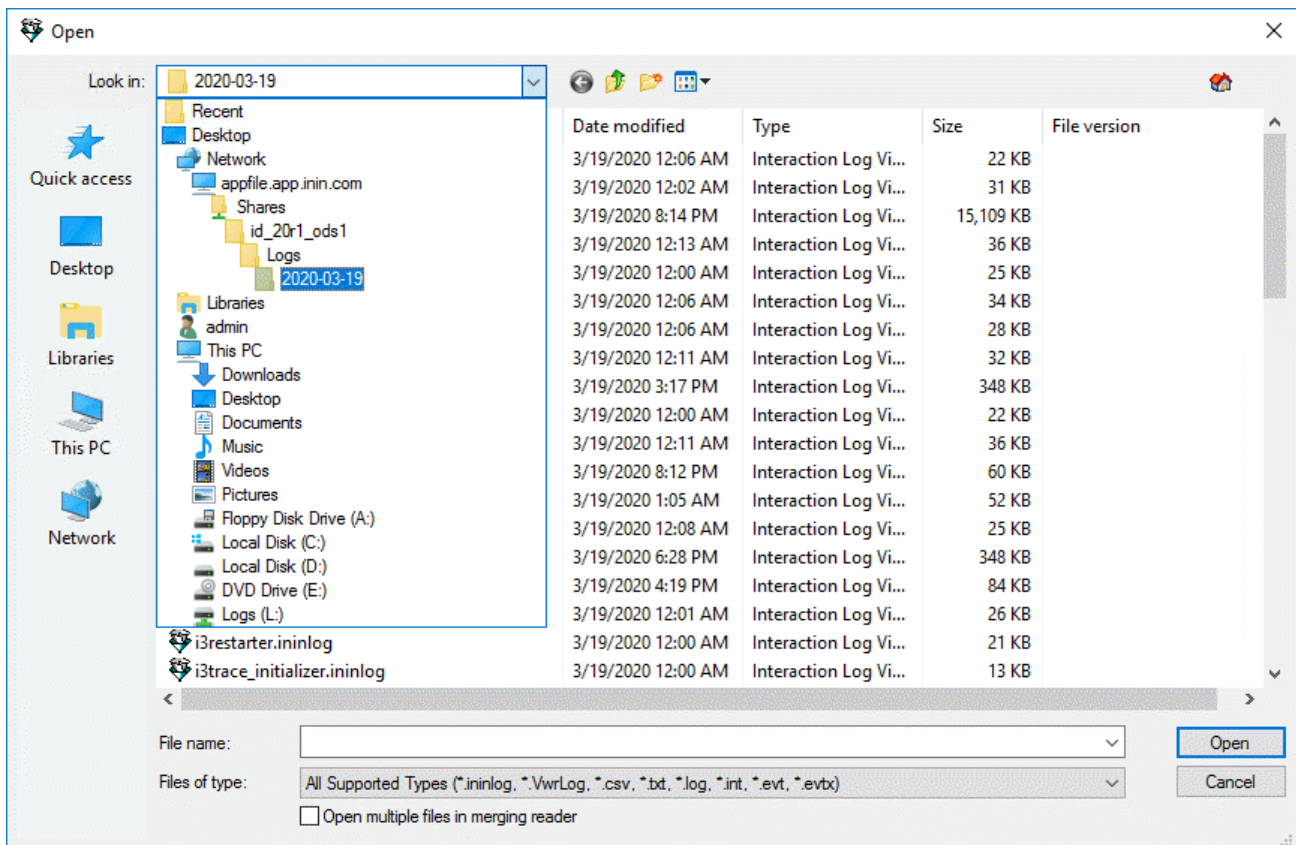
To display a log file in Log Viewer:

1. Select **PureConnect** from the **Start** menu, then select **Log Viewer Utility**.





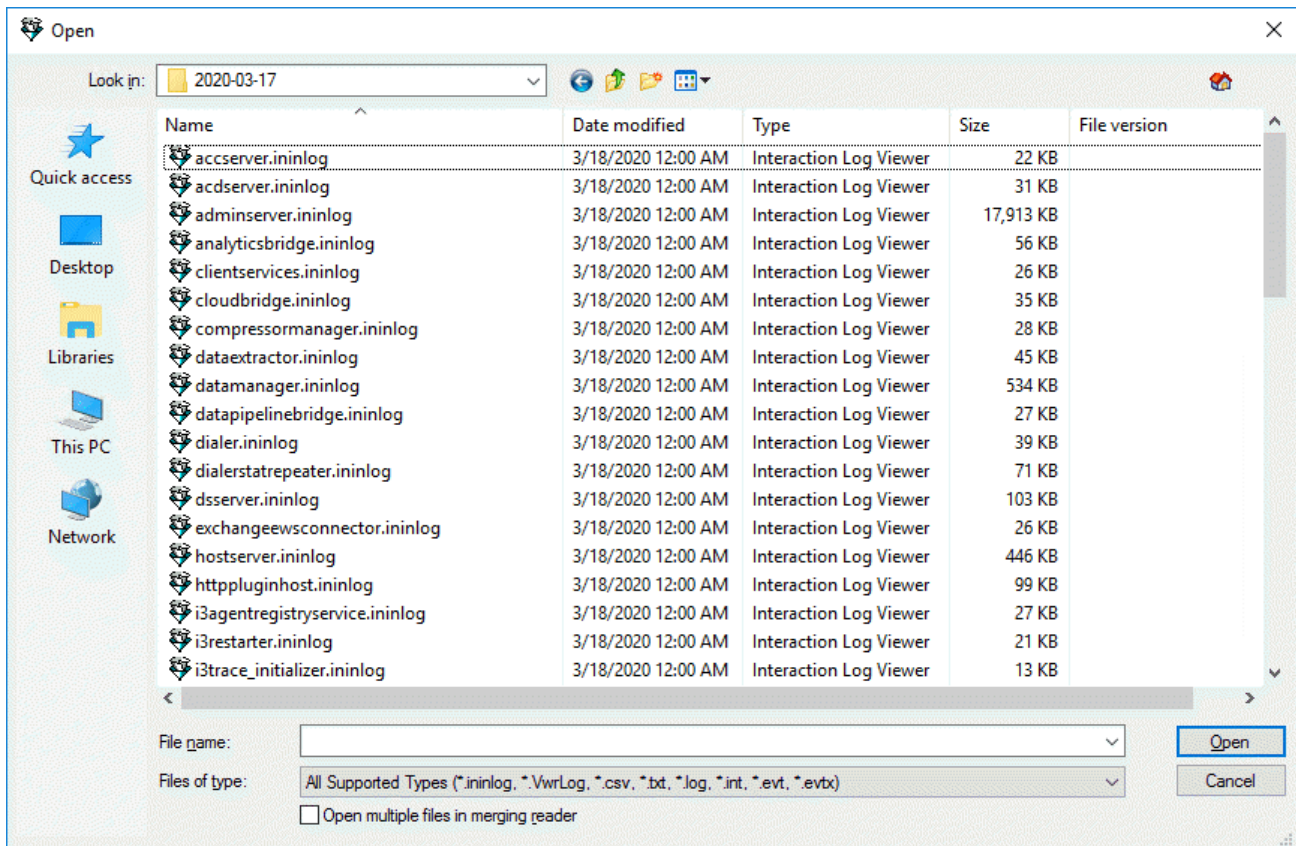
2. Click **File > Open**.
3. Navigate to a drive and folder that contain log files.



Trace log folders are named using their creation date, using a YYYY-MM-DD format. For example, 2020-03-19.

- Trace logs for **CIC subsystems** are stored in the **\Logs** share on the server. The default physical path is **\i3\IC\Log**s.
- On a client PC, logs for locally installed client applications (such as CIC client or Interaction Attendant) are stored in the **C:\Program Files\Interactive Intelligence\Interaction Logs** folder.
- Phone logs are named using the phone's MAC Address. Logs are created when a phone is rebooted.

3. Select a log file. Trace log files have an .ininlog extension. The index for a trace log has an .ininlog.ininlog_idx extension.



4. Click **Open**.

Open latest log file in a series

When an application or subsystem is restarted, a new log file is created. The name of the log file is suffixed with a series number. Logs that are split after exceeding size thresholds also use series numbers. Consequently, the log folder for a given day may contain a series of log files.

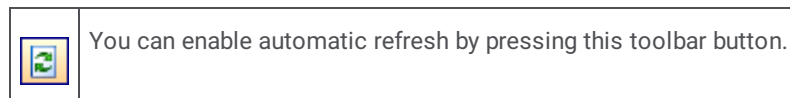
If you have a log file open, the **File > Open Latest in Series** command opens the most recent log file in the series. The equivalent keyboard shortcut is Ctrl+Shift+N. Note that this command opens the latest log file in the series, not the next sequentially numbered file in the series.

For example, if the Interaction Administrator log has seven log files in series, the **Open Latest in Series** command opens Interaction Administrator_7.ininlog if any other logs in the series are open.

Refresh the log automatically

Since applications and subsystems write log entries frequently, Log Viewer offers refresh features that reload the current log. Refreshing picks up new entries that have been written to the log since it was last fetched by Log Viewer. However, automatic refreshing does not begin until you enable it using the command below.

The **View > Auto Refresh Log** command starts automatic refreshing of the log in accordance with the refresh interval. To change the interval between automatic log refreshes, see "Automatic log refresh interval" on the [Options dialog – Misc tab](#).



Related Topics

- [Refresh Log Manually](#)

Refresh the log manually

The **View > Refresh Log** command refreshes the current log immediately. Refreshing picks up new entries that have been written to the log since it was last fetched by Log Viewer.



You can manually refresh a log by pressing this toolbar button, or by pressing F5.

Related Topics

- [Refresh Log Automatically](#)

Reopen a log file

Log Viewer stores the location of recently used log files. To reopen one of these files:

1. From the **File** menu, select **Open**.
2. Type the number of the log file that you want to reopen.

By default, Log Viewer remembers the last six files opened. The number of *most recently used* (MRU) files is configurable. To change the number of files that Log Viewer will remember, pull down the **Tools** menu and select **Options**. Then change **Size of File menu MRU list** to a different value. See [Options dialog – Misc tab](#).

Replace current log with latest in series

Use the **File > Replace with Latest in Series** command (or press Ctrl+Alt+N) to close the current log and open the latest log in a series.

Save the current filter

Once you apply a filter to narrow down message entries, you can save filter criteria so that you can easily reapply filter settings to this log or to another log.

To save current filter settings:

1. On the **Filter** menu, click **Saved Filters > Save Current Filter As**.
2. When the [Save Current Filter As dialog](#) appears, type a descriptive name in the **Filter Name** field.
3. Click **OK** to save the filter. From now on, its name appears in the **Filter** menu under **Saved Filters**.

Related Topics

- [Delete a saved filter](#)
- [Import Filters](#)
- [Use Stored Filters](#)

Search forward or backward on message type

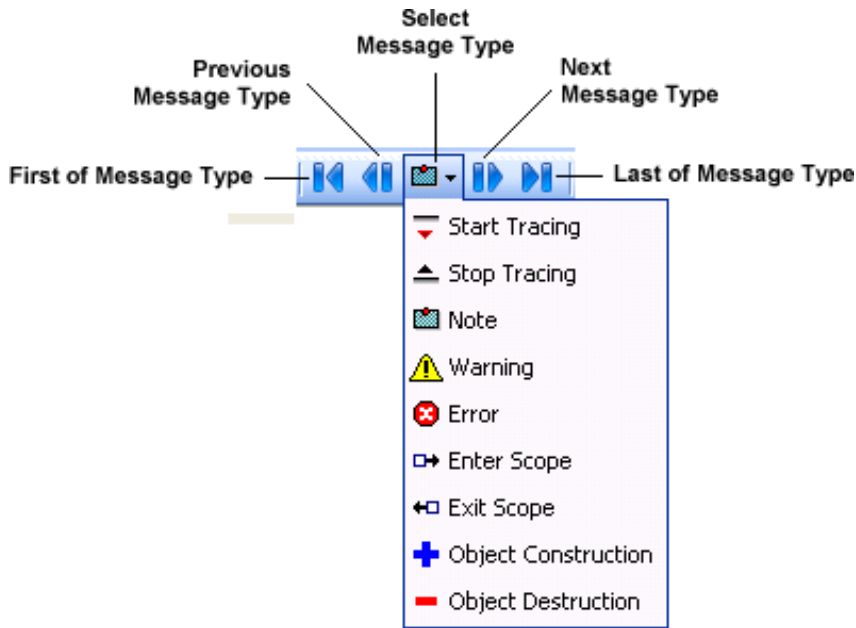
The message types are Start Tracing, Stop Tracing, Note, Warning, Error, Enter Scope, Exit Scope, Object Construction, and Object Destruction. You can search forward or backward using menu commands or by pressing VCR-style buttons on the toolbar. The menu commands are:

- **Search > Search Forward on Message Type**
- **Search > Search Backward on Message Type**

The menu commands open a submenu that selects the message type to search for.

Message Type Toolbar buttons

Message Type toolbar buttons work in a similar fashion. Once you select the message type from the list, you can move forward, backward, or to the first or last instance of the message type.



Search forward or backward on message color

If you have [colorized columns in the message list](#), two menu options allow you to search forward or backward for messages in the color of the currently selection.

| Keyboard | Menu |
|-----------------------|---|
| Ctrl+Shift+Down Arrow | Search > Search Forward on Message Color |
| Ctrl+Shift+Up Arrow | Search > Search Backward on Message Color |

Individual colors do not have any special significance. Color is used in log viewer to group related data and to distinguish log entries. There is no correlation between a given log color and any particular type of data.

Search forward or backward on named expressions

A *named expression* is a filter that you have saved by name. (See [save the current filter](#).) Search by expression commands prompt for the name of a saved filter, and move the selection to the next or previous message in the filter result, but without clearing other messages. This allows you to step through the results of a filter while reviewing other messages in the file.

To search forward:

1. On the **Search** menu, click **Search Forward on Named Expression**.
2. On the submenu, click the name of a saved filter.

To search backward:

1. On the **Search** menu, click **Search Backward on Named Expression**.
2. On the submenu, click the name of a saved filter.

Related Topics

- [Save the current filter](#)

Select all log entries in a message list

To select all displayed entries in a message list, press **Ctrl+A**, or on the **Edit** menu, click **Select All**. You can [copy the selected entries to the Clipboard](#) in a variety of formats so that you can paste data into other applications.

Set application options

Log Viewer allows you to configure options that affect the behavior of the program and whether or not it should interface with the Perforce source code management system. To set options, on the **Tools** menu, click **Options**. The Options dialog box appears.

The dialog box has two tabs:

- The [Options dialog - Misc tab](#) manages settings affecting color, log refresh interval, file size, file extensions, and time limits.
- The [Options dialog - Perforce tab](#) manages settings that determine whether or not Log Viewer checks out code from the Perforce source code management system, to display source from the application that wrote the selected log entry.

Set complex filters

The [Filter Configuration dialog](#) allows you to set up complex filters that apply multiple criteria and [logical operations](#) (AND, OR) to select messages from a log file.

To set a complex filter:

1. On the **Filter** menu, click **Filter Configuration**.



You can click this toolbar button to open the Filter Configuration dialog.

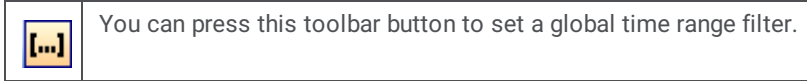
2. Select a [logical operation](#) or a [filter criteria](#) from the **Filter Criterion** list.
3. Complete the property page for the selected criteria. If you right-click an item in the Filter Operations pane, you can use [clipboard operations](#) to copy and paste filter criteria.
4. Click **OK** to apply the filter.

Set global time range filter

A *global time range* filter excludes all log entries that were logged outside of specified start and end times. Global filters persist until they are manually removed using the [Clear Global Time Range Filter command](#). Use global time filters to other filters focus on messages in a specific time period. Once a global time range filter is in effect, you can apply additional filters to narrow down the search.

To set a global time range filter:

1. On the **Filter** menu, click **Set Global Time Range Filter**.



2. When the [Global Time Range Filter dialog](#) appears, click and drag the start time or end time slide controls to set start and end times.
3. Click **OK**.
4. Apply other filters as needed to narrow down the selection.

Related Topics

- [Set global time range filter begin](#)
- [Set global time range filter end](#)
- [Clear global time range filter](#)
- [Global time range filter dialog](#)

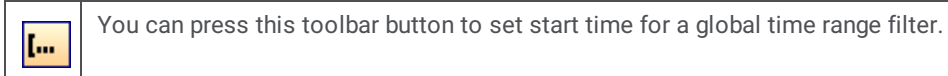
Set global time range filter begin

A *global time range* filter excludes all log entries that were logged outside of specified start and end times. Global filters persist until they are manually removed using the [Clear Global Time Range Filter command](#). Use global time filters to other filters focus on messages in a specific time period. Once a global time range filter is in effect, you can apply additional filters to narrow down the search.

You can set begin and end times by clicking on entries in the message list. Many people find this easier than using slide controls on the [Global Time Range Filter dialog](#) to set a global filter.

To set a start time for a global time range filter:

1. Click a row in the message list.
2. On the **Filter** menu, click **Set Global Time Range Filter Begin**. The timestamp for the selected message is used as the start time for the global filter.



3. If you have not already set a global end time, do so now.

Related Topics

- [Set global time range filter end](#)
- [Clear global time range filter](#)
- [Global time range filter dialog](#)
- [Set global time range filter](#)

Set global time range filter end

A *global time range* filter excludes all log entries that were logged outside of specified start and end times. Global filters persist until they are manually removed using the [Clear Global Time Range Filter command](#). Use global time filters to other filters focus on messages in a specific time period. Once a global time range filter is in effect, you can apply additional filters to narrow down the search.

You can set begin and end times by clicking entries in the message list. Many people find this easier than using slide controls on the [Global Time Range Filter dialog](#) to set a global filter.

To set the end time for a global time range filter:

1. Click a row in the message list.
2. On the Filter menu, click **Set Global Time Range Filter End**. The timestamp for the selected message is used as the start time for the global filter.



You can press this toolbar button to set start time for a global time range filter.

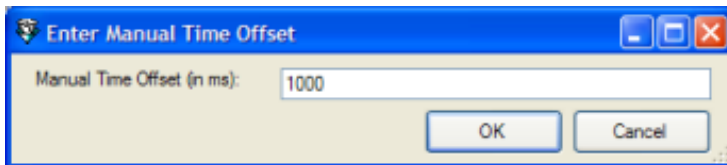
3. If you have not already set a global start time, do so now.

Related Topics

- [Set global time range filter begin](#)
- [Clear global time range filter](#)
- [Global time range filter dialog](#)
- [Set Global time range filter](#)

Set manual time offset

The **View > Set Manual Time Offset** command prompts for a time (in milliseconds) that is added to every log message, effectively shifting the entire log a little.



This feature has two main uses:

- If someone sends you a log and says "something happened around noon, and my system clock is 3 minutes off" then you can use this feature to offset the log by 3 minutes so that you don't have to mentally add or subtract timestamps for a clock disparity while examining the log.
- If you have logs open from different machines, such as two media servers that are handling media from the same conference call, you can use other data to figure out the clock difference between them and apply that offset to one of the logs to correlate times.

Manual Time Offset (in ms):

Enter an amount of offset time in milliseconds, to skew the log file by. For example, enter 2000 to offset by two seconds.

OK button

Closes the dialog and updates the specified offset value.

Cancel button

Closes the dialog without updating the specified offset value.

Set global trace level filter

Not all messages are equally important. Each message is associated with a trace level setting that identifies the severity of the message. You can set a trace level filter to display only those messages that belong to a particular level.

To clear a global trace level filter, use the [Clear All Filters command](#), or [Undo the filter](#).

To set a trace level filter:

1. On the **Filter** menu, click **Set Trace Level Filter**.



You can press this toolbar button to set a global trace level filter.

2. Choose one of the following levels:

All

Selects all trace levels.

Verbose Notes

Selects notes that include details of sub-operations.

Notes

Selects operations including details.

Status

Selects operations only.

Warning

Selects only warning conditions.

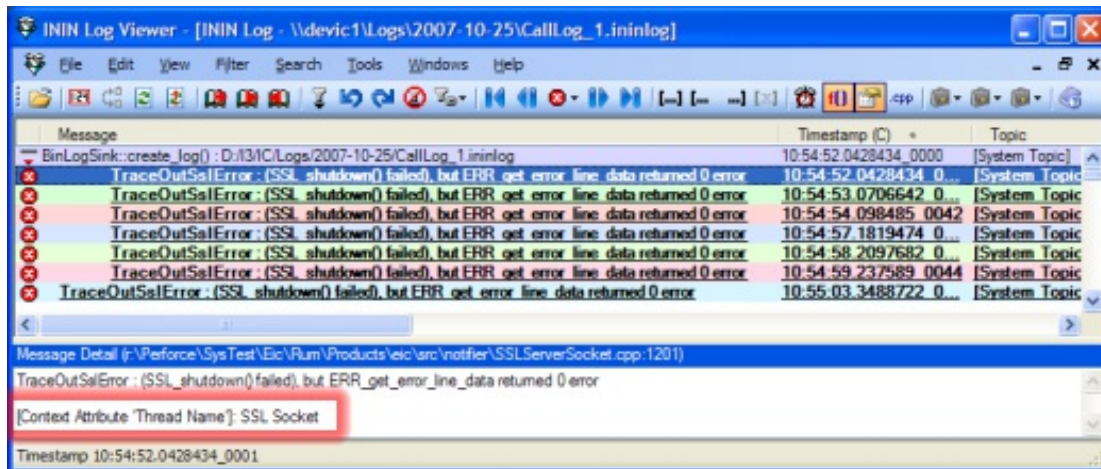
Error

Selects only error conditions.

Critical Error

Selects critical errors only.

Show or hide context attributes in message detail



Use the **View > Show Context Attributes in Message Detail** command to toggle display of context attributes in the **Message Detail** pane.

Context attributes tag message entries to identify a data element of some sort, such as a CallId or a specific user name. Subsystems add context attributes to individual log entries to associate a message with a specific item of information that can be used to group or filter data. Each subsystem has its own set of context attributes.

When Context attributes are displayed, a name/value pair appears at the end of the Message Detail list. For example:
[Context Attribute 'Ctx Attrib 1']: 1101812695

In this example, the name of the attribute is "Ctx Attrib 1", and its value is 1101812695.



You can toggle display of Context Attributes by pressing this toolbar button.

When context attributes are toggled off, no additional information is appended to the Message Detail list.

Show or hide function names in log messages

You can toggle the display of the name of the function that wrote a log message, using the **View > Show Function Names** command. This command prefixes the name of the subsystem or application routine in front of the message. For example, when function names are turned on, a log message might look like this:

CDeallocator::PerformDeallocations : 10:34:20: Connected

In other words, the "Connected" log entry was written by a function named *CDeallocator*. When function names are turned off, the message entry would be:

10:34:20: Connected



You can toggle display of function names by pressing this toolbar button.

When function names are hidden in message entries, they still appear in the **Message Detail** pane at the bottom of the window.


Related Topics

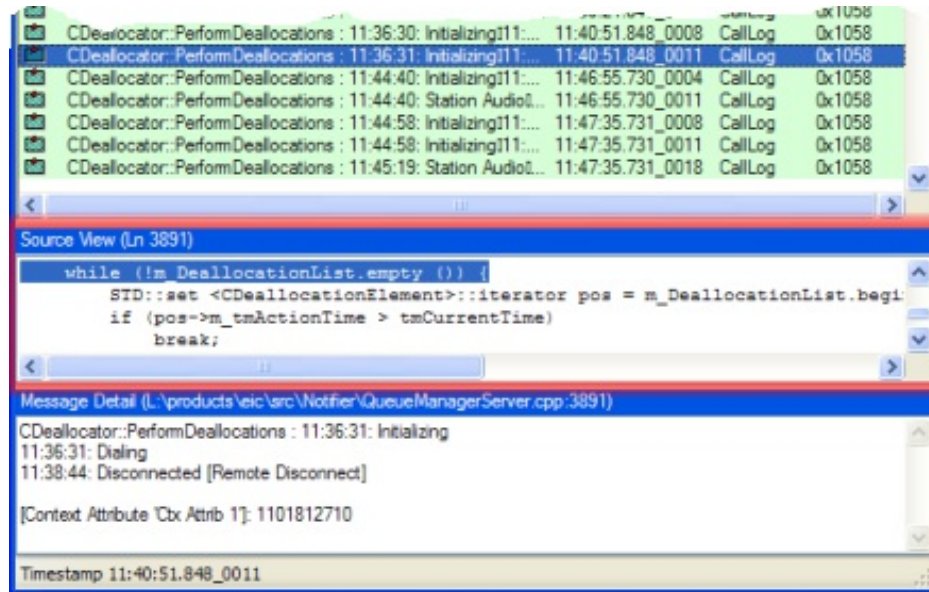
- [Show or hide related Source Code](#)

Show or hide related source code

This feature is for Interactive Intelligence internal use. You can configure Log Viewer to display source code from the function that wrote the selected log entry. Lines of code for the function appear in the **Source View** pane.

On the **View** menu, click **Source View** to show or hide the **Source View** pane.

 You can toggle display of the Source View pane by pressing this toolbar button.



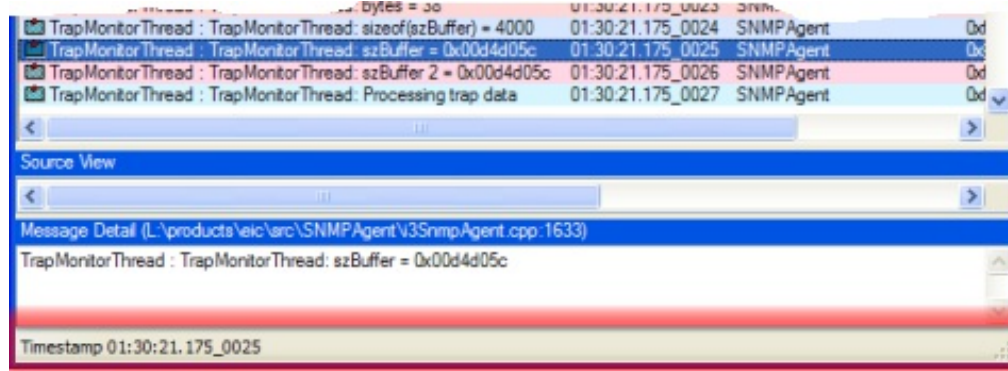
You can configure Log Viewer to automatically check out source code from the Perforce source management system. See [Options dialog - Perforce tab](#) for more details.

Related Topics

- [Show or hide function names in log messages](#)

Show or hide the status bar

The status bar appears at the bottom of the **Log View** window. It displays messages, such as the timestamp of the current entry. On the **View** menu, click **Status Bar** to toggle the status bar on or off. The figure below shows the status bar highlighted in red.



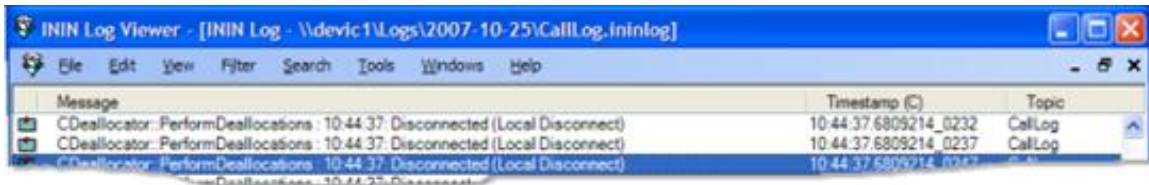
Show or hide the toolbar

The Log Viewer toolbar is visible by default. To hide the toolbar, on the **View** menu, click **Toolbar**. Click the menu option again to show the toolbar.

Toolbar On



Toolbar Off



Snip or merge log files

The Log Snip/Merge Utility snips (copies) all or part of a log file to a new file. It can also merge entries from multiple logs into a new log file.

To run the utility:

1. On the **File** menu, click **Snip/Merge Log File(s)**. This menu option opens the [Log Snip/Merge Utility](#).
2. Click **Add** to open the [File Open](#) dialog box so that you can select a log file to snip entries from, or merge to a new log file.
 - If you select a single file, the utility copies (snips) all or part of it to a new file.
 - When multiple files are selected, snips from each file are written (merged) to a new file.
3. Repeat step 2 to select additional files, if necessary.
4. By default, the **Don't Restrict Start Time** check box is selected, meaning that the snip/merge operation should start at the beginning of the file. If you clear the check box, you can set the start date and time to specific values.
5. By default, the **Don't Restrict End Time** check box is selected, meaning that the snip/merge operation should continue until an end-of-file condition is reached. If you clear this check box, you can set an end date and time.
6. Enter a fully qualified path and log file name in the **Destination File** field, or click the browse button to open a dialog that sets the destination folder and file name.
7. You may be asked to specify a time zone to normalize log entries to. If the [Select Time Zone dialog](#) appears, select a time zone and click **OK**.
8. Click **Snip**. The [Snipper Monitor dialog](#) appears to display status messages about the operation. When processing is complete, you can close this dialog box unless Log Viewer is configured to close it automatically—see [Options dialog – Misc tab](#) for details.

The new file opens automatically in Log Viewer once all files are processed.

Synchronize timestamps for a time zone

By default, time values in the *Timestamp* column are formatted for the log creator's time zone, meaning that the time reflects the time zone of the server or workstation that wrote the log entry. Log Viewer allows you to display Timestamp values using your local time zone, or in UTC format.

To do this, use the **View > Time Zone Setting** menu command to format the Timestamp column for one of the following time zones:

My Local Time Zone

Displays Timestamp values using the time zone of the local workstation.

Log Creator's Time Zone

Displays Timestamp values using the time zone of the server or workstation that wrote the log entry.

Universal Coordinated Time

Displays Timestamp values in Universal Coordinated Time, otherwise known as Greenwich Mean time or GMT.

Synchronize with other logs

Sometimes the need exists to examine more than one log to review entries for a particular time. Log Viewer makes it easy to synchronize multiple logs, based on timestamps. This helps an administrator trace an event through different subsystems.

This feature allows administrators to follow events and actions from log to log and can help to pinpoint how CIC processed events from subsystem to subsystem.

To synchronize log files

1. Maximize the Log Viewer window.
2. Open two or more log files.
3. On the **Windows** menu, click Tile Vertical to arrange the windows for optimal display.
4. Select an entry of interest in one of the logs.
5. Pull down the View menu and select Synchronize Now with Other Logs.









You can synchronize logs by pressing this toolbar button.

6. Each of the logs will display entries by coordinating timestamps.

Use Search menu commands to trace call levels

Directionally paired commands in the *Search* menu trace execution of code through *call levels* in various ways. *Call level* (or call stack, if you prefer) is an indicator of functions calling other functions. The first calling function is level 0. If the main function calls a helper function, the helper is considered to be at call level 1, and so forth. Call levels help trace the flow of control from one function to another.



| | | | |
|---|--|---|---|
|  | Step Over Next Call Level (F10) jumps to the next message of the same or lower call level, skipping all the messages of higher call levels. |  | Back Over Next Call Level (Shift+F10) does the opposite of <i>Step Over Next Call Level</i> . It jumps to the previous message of the same or lower call level, skipping all the messages of higher call levels. |
|  | Step into Next Call Level (F11) jumps to the next message, regardless of call level. |  | Back into Next Call Level (Shift+F11) is the opposite of <i>Step into Next Call Level</i> . It jumps to the previous message, regardless of call level. |
|  | Jump Out of Current Call Level (F12) jumps to the next trace statement of lower call level. |  | Back Out of Current Call Level (Shift+F12) is the opposite of <i>Jump Out of Current Call Level</i> . It jumps to the previous trace statement of higher call level. |

Related Topics

- [Jump to Matching Scope/Create](#)
- [Jump to specific timestamp](#)
- [Jump to next/previous thread message](#)

Undo/Redo Filters

Filters exclude entries from a log to focus on particular areas of interest. If applying a filter setting does not achieve the desired result, you can undo the filter change. Conversely, you can redo a filter change. These commands are available via menu, toolbar, and keyboard shortcuts.


| Toolbar | Keyboard | Menu |
|---|----------|-----------------------------|
|  | Ctrl+Z | Filter > Undo Filter Change |
|  | Ctrl+Y | Filter > Redo Filter Change |

Use Bookmarks

You can bookmark log entries so that you can return to them later. Once you add a bookmark, you can return to it or jump to the next or previous bookmark in the currently open log file.

Add or remove bookmarks

1. To add a bookmark, select one or more log entries.
2. Press Ctrl-F2 to bookmark the selected entries. To remove the selected bookmarks, press Ctrl-F2 again.





You can toggle bookmarks on or off by pressing this toolbar button, by pressing Ctrl-F2, or by choosing Toggle Bookmark from the Search menu.

Bookmarks persist if you close and re-open a log file.

Jump to next or previous bookmark

When more than one entry is marked, you can navigate to the next or previous bookmark in the list, relative to your current position. The table below shows how to do this using the toolbar, keyboard shortcuts, and menu commands.


| Toolbar | Keyboard | Menu Command |
|---|------------|------------------------------------|
|  | F2 | Search > Jump to Next Bookmark |
|  | Shift + F2 | Search > Jump to Previous Bookmark |

View All Bookmarks

The Bookmarks dialog box displays a list of bookmarked entries so that you can easily jump to or remove marked entries.

1. On the **View** menu, click **Show Bookmarks**.
2. The [Bookmarks dialog](#) will appear.
 - To remove a bookmark, select one or more entries, and then click **Remove Bookmark**. Removing a bookmark does not remove the entry from the log.
 - To navigate to a selected log entry, click **Jump to Bookmark**. This button is enabled when a single bookmark is selected.
3. When you are finish, click **Done** to close the **Bookmarks** dialog box.

Use Stored Filters



Store the Current Filter Here
Apply this Stored Filter
'OR' this Stored Filter with Current
'AND' this Stored Filter with Current
Clear this Stored Filter

You can store the current filter in a toolbar control. Up to three filters can be stored for the duration of the log session. Each log can have its own set of stored filters, which persist until the log file is closed.

A stored filter can be applied, replacing other filter results, or it can be applied "on top" of another filter using logical AND or OR operators.

Clearing a stored filter removes the filter from the toolbar, but does not change filter criterion applied to the log.

Log Viewer User Interface

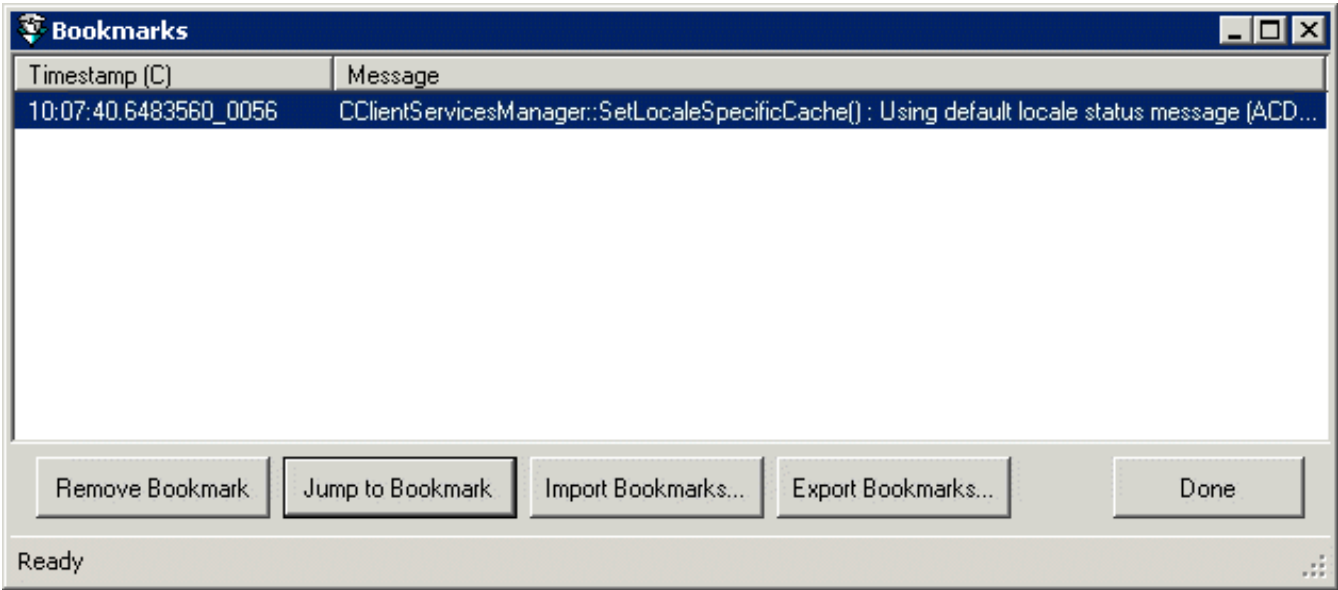
This reference section describes dialog boxes and other user interface options.

| Dialogs | |
|---|---|
| About dialog | Log Snip/Merge Utility |
| Bookmarks dialog | Message Decryption Key dialog |
| Change Columns dialog | Options dialog – Misc tab |
| Enter Coloring Regular Expressions dialog | Options dialog – Perforce tab |
| Export Output File dialog | Save Current Filter As dialog |
| File Open dialog | Select Time Zone dialog |
| Filter Configuration dialog | Snipper Monitor dialog |
| Find Text dialog | Timestamp Selection dialog |
| Global Time Range Filter dialog | |
| Key Management dialog | |
| Log Header dialog | |

About dialog

The **About** dialog displays version information and other details about Log Viewer. This dialog appears when you click **About** on the **Help** menu.

Bookmarks dialog



The Bookmarks dialog displays a list of bookmarked messages, so that you can navigate to bookmarks or remove bookmarks from selected entries. To display this dialog, pull down the **View** menu and select *Show Bookmarks* (or press Alt+F2).

Bookmark list

Bookmarked entries are listed at the top of the dialog.

Remove Bookmark button

To remove a bookmark, select one or more entries. Left-click to select a single item, or Ctrl-click to select multiple items, or Shift-click to select multiple contiguous entries. Then press the Remove Bookmark button. Removing a bookmark does not remove the entry from the log.

Jump to Bookmark button

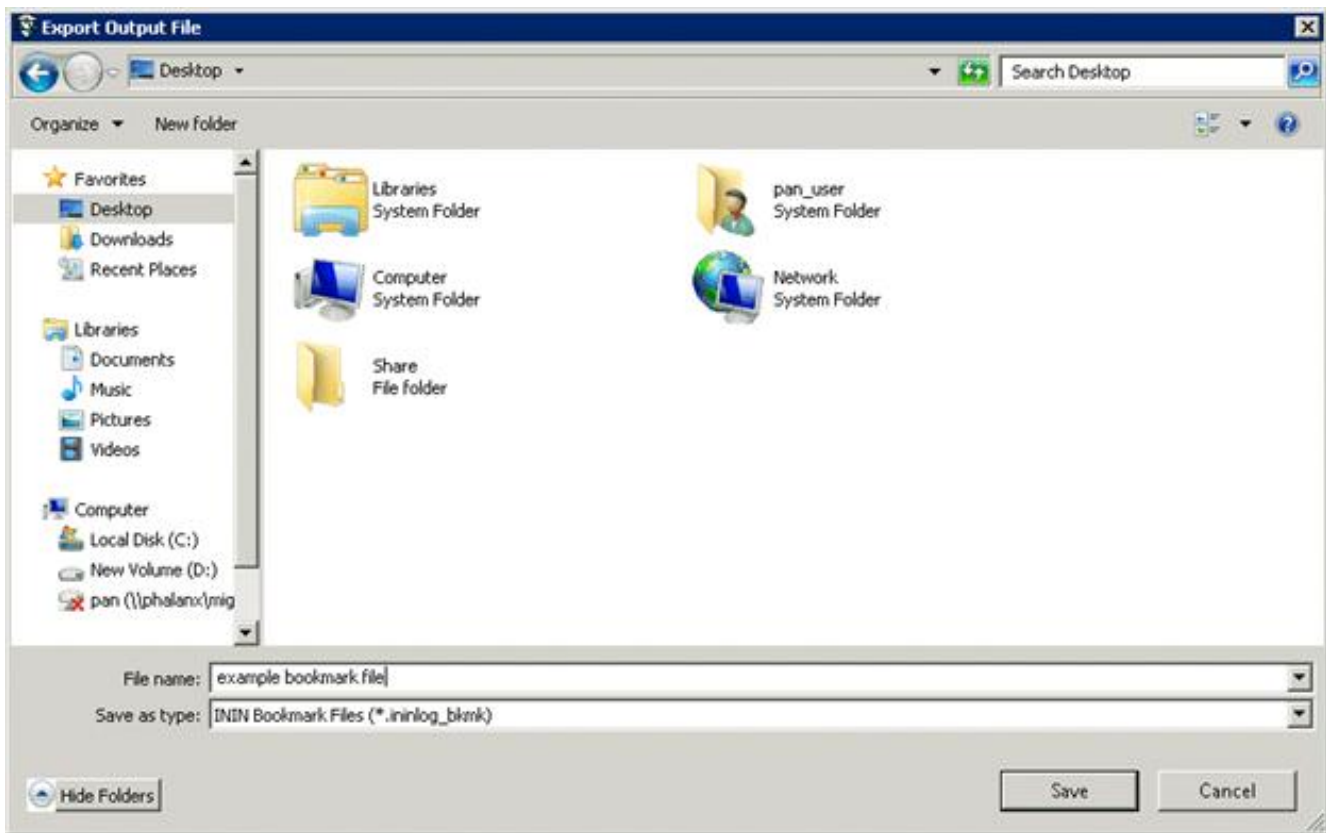
This button is enabled when a single bookmark is selected. Use it to navigate to the selected log entry.

Import Bookmarks button

Prompts to select a saved Bookmarks file (*.ininlog_bkmk). Navigate to a file. Then press Open. The bookmarks contained in that file will appear in the Bookmarks dialog.

Export Bookmarks button

Opens the Export Output file dialog so that you can name a file to save the bookmarks you have selected in the Bookmarks dialog. Bookmark files have an extension of .ininlog_bkmk.



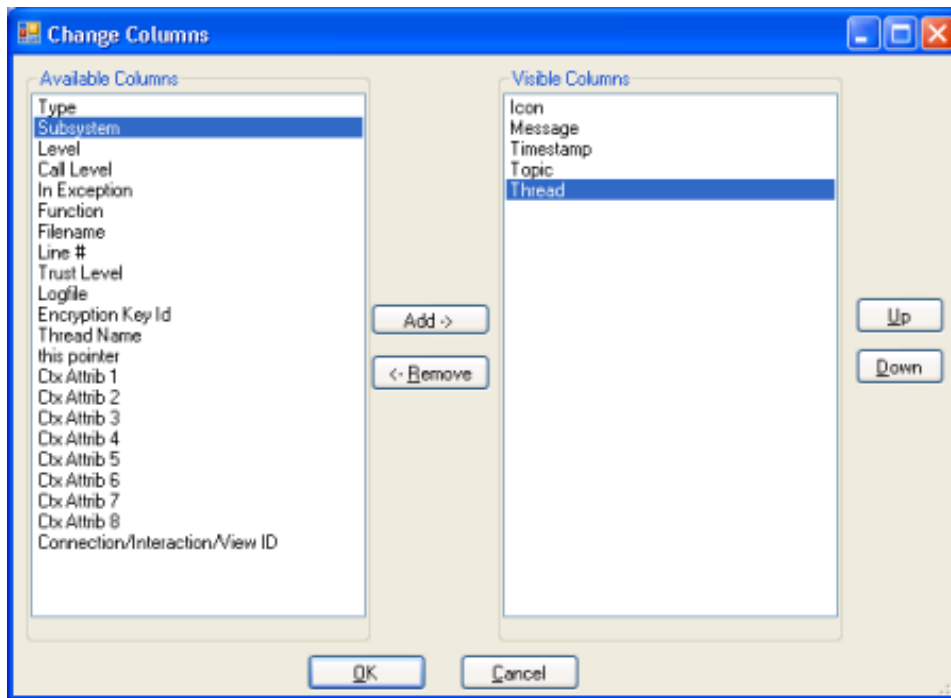
Done button

Closes the **Bookmarks** dialog box.

Related Topics

- [Use Bookmarks](#)

Change Columns dialog



The *Change Columns* dialog manages the visibility of columns in the message list.

Available Columns list

The list on the left contains columns which are not currently shown in the view. See *Logged Columns* for a description of each column type.

Visible Columns list

This list on the right displays columns that are visible, and allows the order of appearance to be changed.

Add button

To make a column visible, select an item in the list on the left. Then press *Add*.

Remove button

To hide a column, select an item in the list on the right. Then press *Remove*.

Up button

By arranging the top-down order of items in the Visible Columns list, you can control the left-to-right order of columns in the message list. Use the Up button to move a column higher (more leftmost) in the message list.

Down button

Moves the selected column lower (more rightmost in the message list).

OK button

Closes the dialog and puts column selection and sequence options into effect.

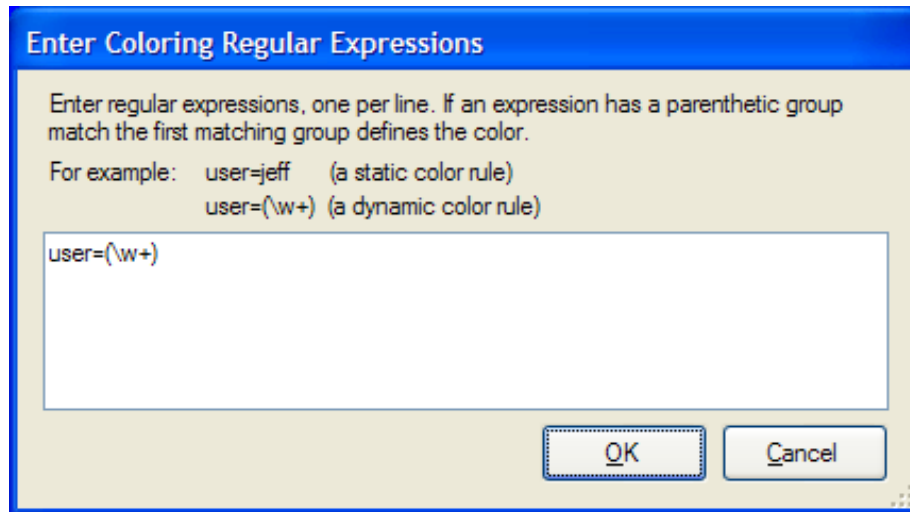
Cancel button

Closes the dialog without changing the message list.

Related Topics

- [Manage Columns in the Message List](#)

Enter Coloring Regular Expressions dialog



This dialog appears when you select **Color Column > By Regular Expression** from the **View** menu. A *regular expression* is a sequence of characters that defines a pattern to search for. A regular expression locates patterns of text. For general information about regular expressions, see <http://www.regular-expressions.info/>.

Expression text box

Type a regular expression into this box, and then click **OK**.

OK button

Closes the dialog, evaluates the regular expression, and colorizes matching entries in the message list.

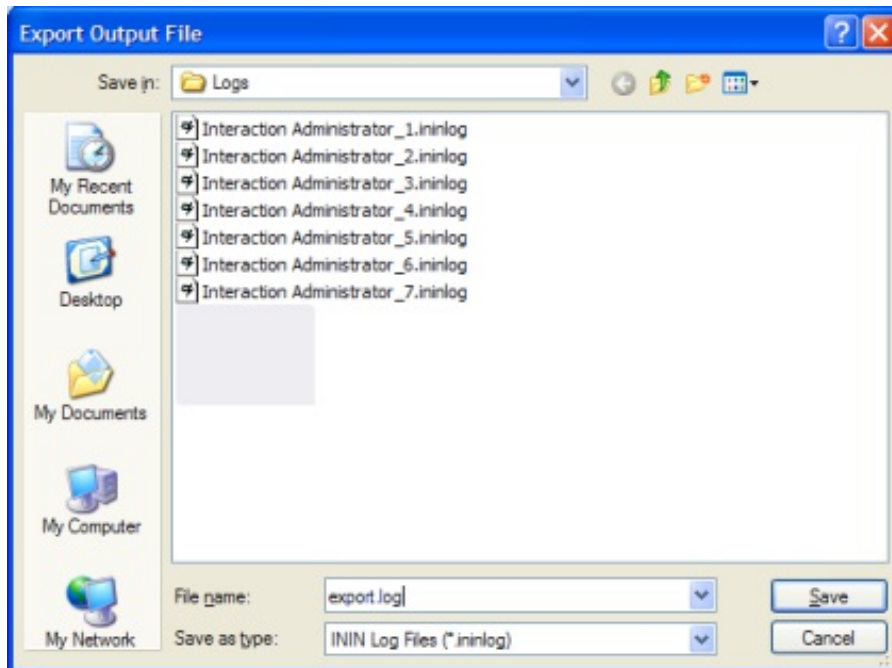
Cancel button

Closes the dialog without evaluating text entered in the text box.

Related Topics

- [Colorize columns in the message list](#)

Export Output File dialog



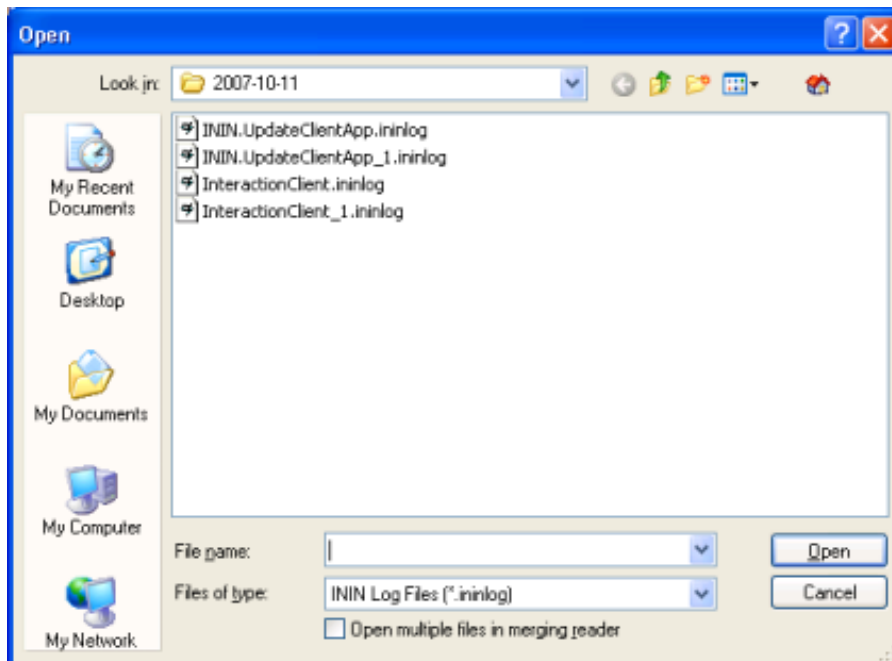
This dialog prompts for the name of an exported log file. It is a standard Windows **Save As** dialog box. Type a new name in the **File name** field, and then click **Save**. An .ininlog extension is automatically added to the file name..

Related Topics

- [Export to File](#)

File Open dialog

This dialog is invoked by pressing Ctrl+O or by selecting *Open* from the *File* menu. Use this dialog to navigate to the folder that contains a log file you want to open.



Shortcut buttons

The shortcut buttons on the left navigate to standard Windows locations, such as the desktop, personal documents folder, etc.

File name

This field displays the name of a file selected using the dialog, or typed by the user.

Files of Type

Selects a file type that Log Viewer can choose using this dialog.

| File Type | Extension |
|----------------------------|-----------|
| ININ Log file | *.ininlog |
| VwrLog Log file | *.VwrLog |
| Comma Delimited File | *.csv |
| Plain Text File | *.txt |
| Syslog File | *.log |
| Install Log File | *.int |
| Application Event Log file | *.evt |
| System Event Log file | *.evt |
| Security Event Log File | *.evt |
| Enhanced Event Log file | *.evtx |

Open button

Opens the selected file for display in Log Viewer.

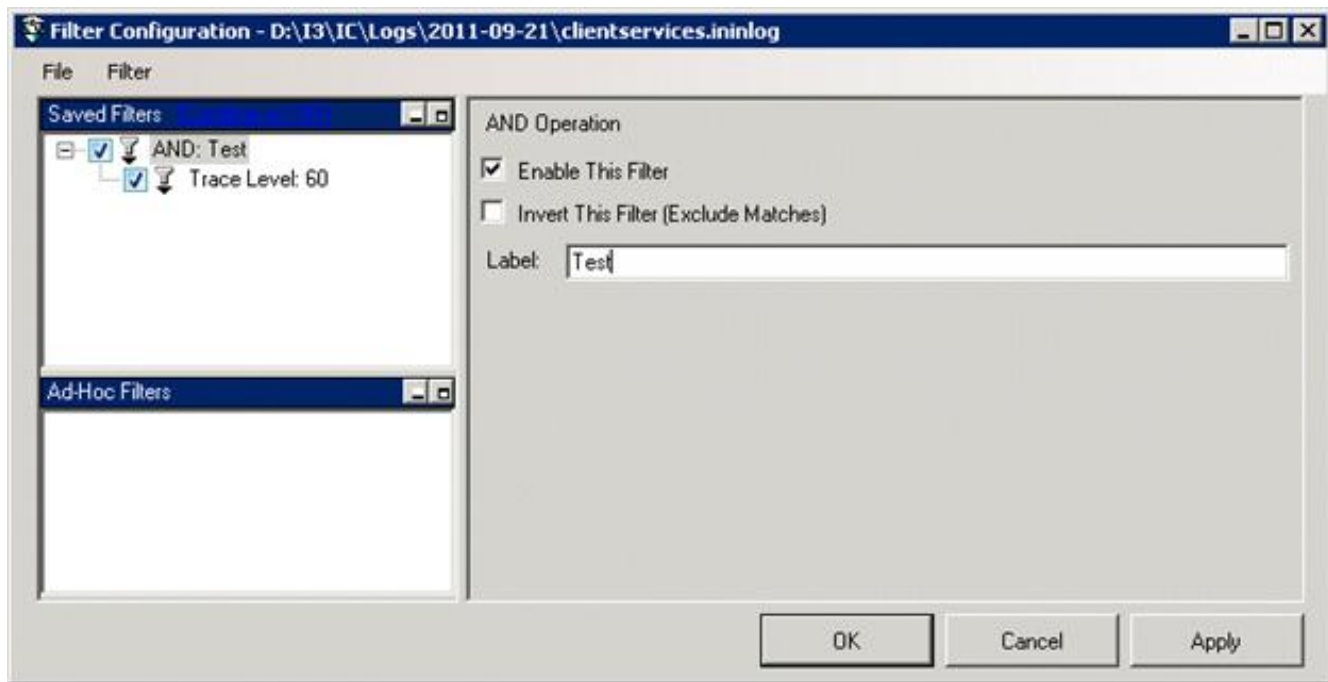
Cancel button

Closes the dialog without opening any files.

Related Topics

- [Open a Trace Log File](#)

Filter Configuration dialog



The *Filter Configuration* dialog is Log Viewer's most powerful tool for drilling through log file data. It creates filters based on multiple criterion that use logical operators (AND, OR) to evaluate messages in a log. To use this dialog effectively, you need to understand its user interface elements:

Saved Filters list

This list contains filters that you have saved, allow you to selectively apply them.

Ad-Hoc Filters list

This list displays filters that you have created on the fly while using this dialog.

File > Save Filters...

Saves all filters you have created while using the Filter Configuration dialog.

Import Filters...

Opens a dialog allowing selection of a saved filter file to import.

Export Filters

Opens a dialing allowing an Ad-hoc filter to be saved to disk.

Combine w/AND | Combine w/OR

Works as a toggle to apply a logical AND or logical OR to selected filters in the Saved Filters list.

Filter > Create Named Filter

Creates a new Named Filter based on your selection of criterion. You must select a type of filter operation, such as a string match or specific trace level setting. See [Filter Criterion Choices](#) for information about each option in this list. Once you make a selection, you can tune filter settings by changing filter properties in the right pane.

Filter > Create Ad-Hoc Filter

Creates a new Ad-Hoc filter based on your selection of criterion. You can further tune filter settings by making selections in the right pane.

OK button

Dismisses the dialog after applying changes.


Cancel button

Dismisses the dialog without applying filter changes.

Apply button

Applies filter selections but does not dismiss the dialog.

Filter Criterion Choices



String Match

Thread ID

Message Type

Function Name

Topic Name

Topic/Level

Call Level

Trace Level

this Pointer

Trust Level

Timestamp Range

Context Attribute

Filename/Line

Within Scope

Lines of Context

Bookmarks

In Exception Unwind

AND

OR

Swap AND/OR Filter

Copy Filter to Clipboard

Paste Filter from Clipboard

The **Filter Criterion** list displays filter operations, logical operators, and clipboard commands.

Use the *Filter Criterion* drop list to select a filter operation. The filter operations are:

[String Match](#)

[Thread Id](#)

[Message Type](#)

[Function Name](#)

[Topic Name](#)

[Topic/Level](#)

[Call Level](#)

[Trace Level](#)

[this Pointer](#)

[Trust Level](#)

[Timestamp Range](#)

[Context Attribute](#)

[Filename/Line](#)

[Within Scope](#)

[Lines of Context](#)

[Bookmarks](#)

[In Exception Unwind](#)

You can select [logical operations](#):

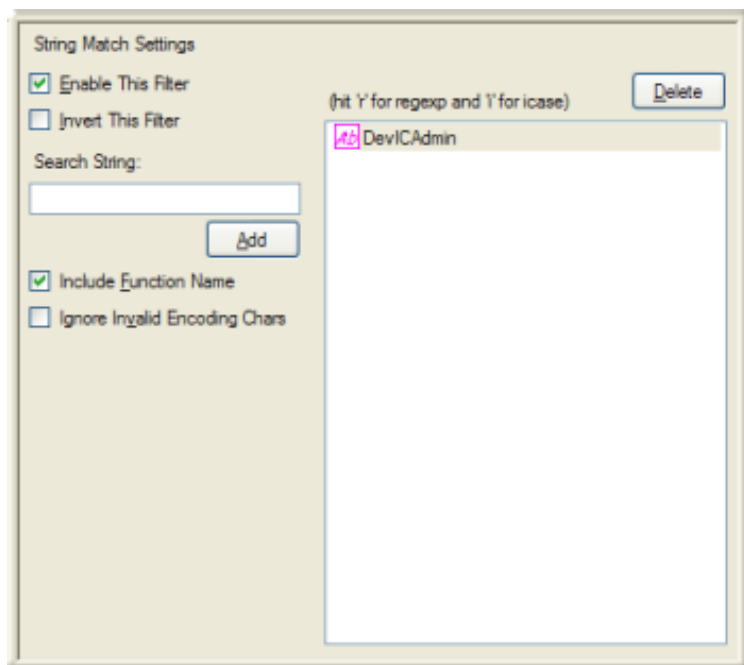
- AND
- OR
- Swap AND/OR Filter

Or perform [Clipboard Operations](#) on Filters:

- Copy Filter to Clipboard
- Paste Filter from Clipboard

These options are discussed in subsequent topics.

String Match



A string match looks for entries that contain a literal string of characters.

To configure a string match:

1. Type a string in the **Search String** box.
2. Click **Add**.

User interface options

Enable This Filter checkbox

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Search String field

Type the text to search for, or a regular expression in this field. Press Add. Then type "r" or "i" to indicate whether the text is a regular expression, or a simple string search. Pressing "i" works like a toggle switch to indicate whether the search should be case-sensitive. An icon next to the string indicates your string processing preference:

| | |
|----|---------------------------------------|
| ab | case-sensitive search |
| Ab | ignore case |
| re | evaluate text as a regular expression |

Add button

Adds the contents of the Search String field to the String list box. A single String Match can look for any number of strings in the file.

Include Function Name checkbox

This checkbox determines whether Function Names are evaluated. The default is true.

Ignore Invalid Encoding Chars checkbox

Trace statements sometimes accidentally contain ASCII strings that are not always legal UTF-8, especially in multi-byte Japanese languages. When this option is checked, log message that contain an illegal UTF-8 byte sequence are considered to be corrupt and will never match anything.

Delete button

Press this button to remove the entry selected in the String list box.

String list box

This box lists all strings that you have defined, and uses the icons discussed above to indicate string processing preferences.

OK button

Closes the Filter Configuration dialog and applies the filter.

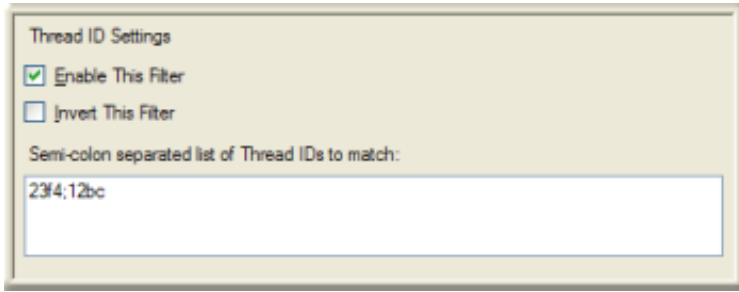
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Thread Id



Threads are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process and more than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled. The thread context includes all of the information the thread needs to seamlessly resume execution, including the thread's set of CPU registers and stack, in the address space of the thread's host process.

Log messages have corresponding thread ID numbers that you can use as filter criteria. These numbers are displayed in the Thread column in hexadecimal format (e.g. 0x23f4). If the Thread column isn't visible in the message list, use the [Manage Columns](#) command to display it.

Enable This Filter checkbox

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Semi-colon separated list of Thread IDs to match

Type thread IDs in this box, separated by semi-colons. For example, to exclude all messages except those for threads 0x23f4 and 0x12bc, you would type 23f4;12bc.

OK button

Closes the Filter Configuration dialog and applies the filter.

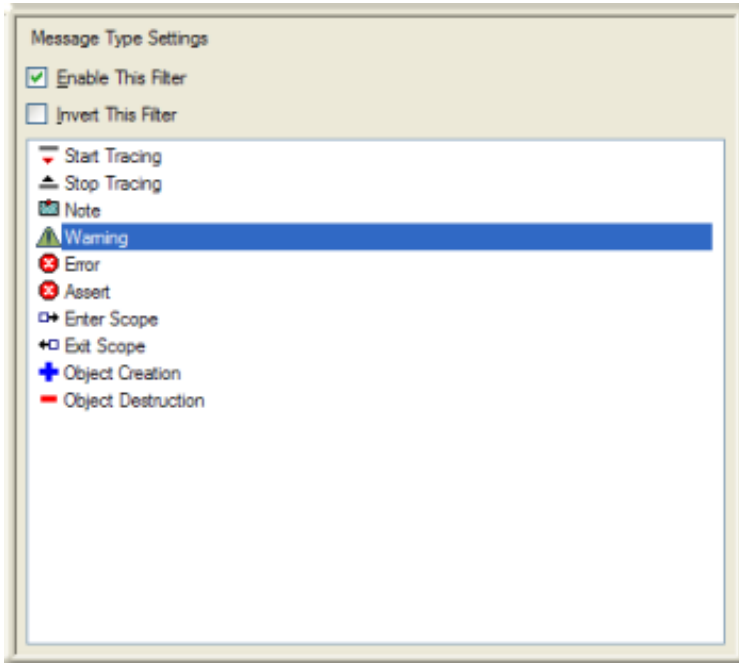
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Message Type



This criteria filters for messages of a particular type: *Start Tracing*, *Stop Tracing*, *Note*, *Warning*, *Error*, *Enter Scope*, *Exit Scope*, *Object Construction*, or *Object Destruction*.

Enable This Filter checkbox

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Message Type

To set a message type to search for, click on a row in this list.

OK button

Closes the Filter Configuration dialog and applies the filter.

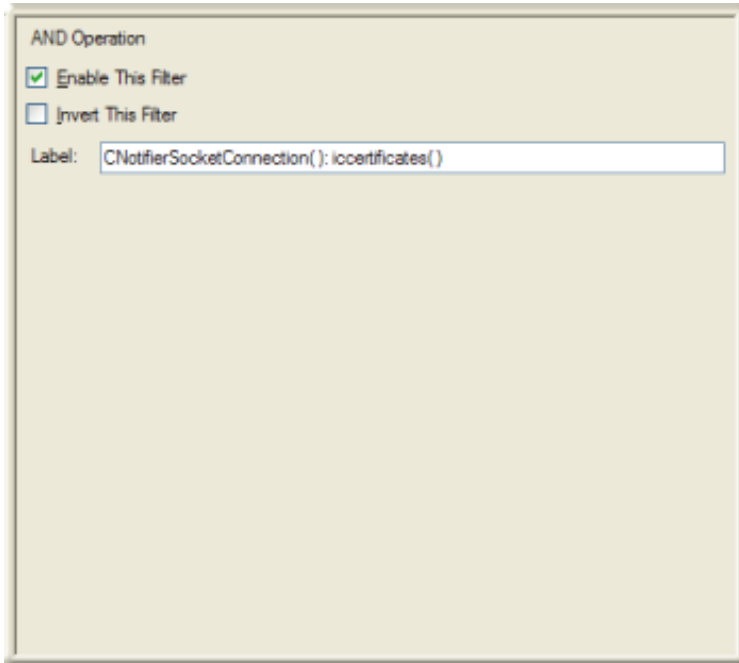
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Function Name



The screenshot shows a dialog box titled "AND Operation". It contains two checkboxes: "Enable This Filter" which is checked, and "Invert This Filter" which is unchecked. Below these is a text field labeled "Label:" containing the text "CNotifierSocketConnection(); locertificates()".

This criteria filters for the name of the function that wrote a log message. To look up a function name, you may need to [toggle on the display of function names in the message list](#).

Enable This Filter check box

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Semi-colon separated list of function names to match

Type function names in this field, delimited by semi-colons. Be sure to include "(" at the end of the function name, including arguments, if need be.

OK button

Closes the Filter Configuration dialog and applies the filter.

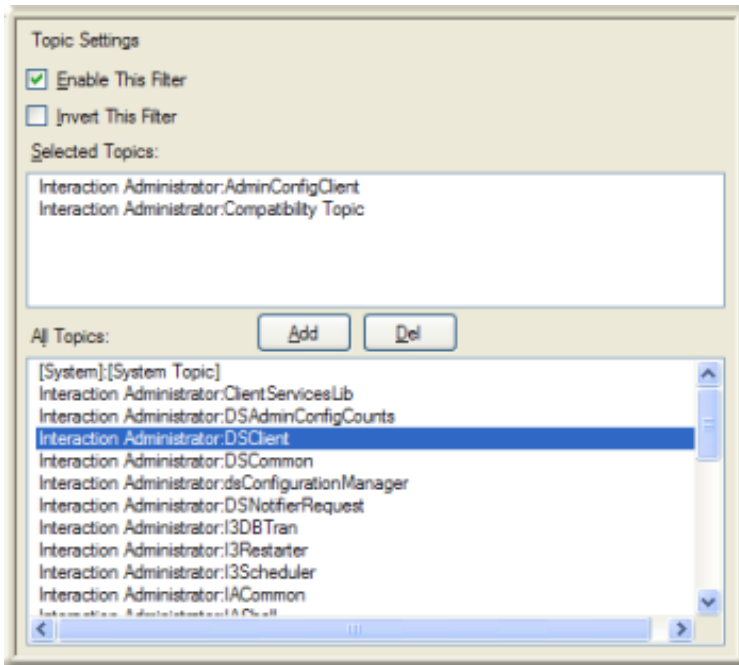
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Topic Name



The routines that write messages are called *trace topics*. Trace topics correspond to subroutines invoked by a subsystem, or to some type of major functionality provided by an application. Every subsystem and application has its own set of trace topics. This criteria allows you to specify topics to filter by.

To filter by topic name:

1. Select an entry in the **All Topics** list.

About [System]:[System Topic]

The first choice in the *All Topics* list is [System]:[System Topic]. It configures the filter to look for messages that were generated by the trace code itself. Items such as "Start Tracing" messages fall into this category. These "automatic topics" are generated by the trace system before the application has initialized its topics. For that reason there is no application-specific topic that could be used for "Start Tracing" messages. If the log contains corrupt messages, they show up as System topics too, because the messages are too corrupt to determine their proper topic.

2. Click **Add**.
3. Repeat steps 1-2 to filter on additional topic names.
4. Click **OK**.

User interface options

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear the check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this box. The filter selects all entries that do not match the criterion.

Selected Topics list

List of topics that were added from the **All Topics** list.

Add button

Adds the topic selected in the **All Topics** list to the **Selected Topics** list. This selects a topic for filtering.

Del button

Removes the topic selected in the **Selected Topics** list. This de-selects a topic for filtering.

All Topics list

This list contains the names of topics supported by the current log. Topic names vary from log to log.

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

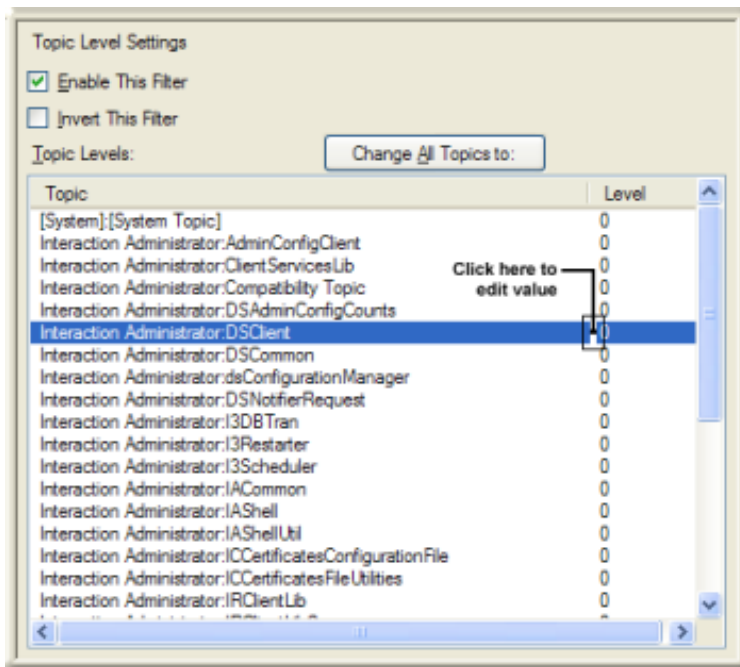
Cancel button

Closes the dialog box, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Topic/Level



This criteria allows you to filter by *topic* and *trace level*. *Topic* is the name of the routine that wrote the message. *Trace level* is a number that determined the verbosity of messages written about that topic. Topic is what was traced, level indicates how much was written about the trace.

To filter for specific topics with specific levels

1. Click a row in the **Topic** list to select a topic.

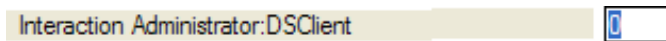
About [System]:[System Topic]

The first choice in the **Topic** list is [System]:[System Topic]. It configures the filter to look for messages that were generated by the trace code itself. Items such as "Start Tracing" messages fall into this category. These "automatic topics" are generated by the trace system before the application has initialized its topics. For that reason there is no application-specific topic that could be used for "Start Tracing" messages. If the log contains corrupt messages, they show up as System topics too, because the messages are too corrupt to determine their proper topic.

- The default trace level is 0, which excludes all but critical errors. To enter a value for topic level, you have to put the **Level** column in edit mode. To do so, click the white space that separates the **Topic** column from the **Level** column:



- The **Value** field becomes available. Type a different value using the table below as your guide:



| Severity | Range | Description |
|----------|-------|--|
| Critical | 0-10 | Only critical errors (those impacting features) will be logged. |
| Error | 11-20 | Any error conditions will be logged. |
| Warning | 21-40 | Any warning conditions will be logged. |
| Status | 41-60 | Operations are logged. |
| Notes | 61-80 | Operations including details are logged. |
| Verbose | 81-99 | Sub-operation details are logged. |
| All | 100 | All trace statements within the program are enabled (This will generate very large log files.) |

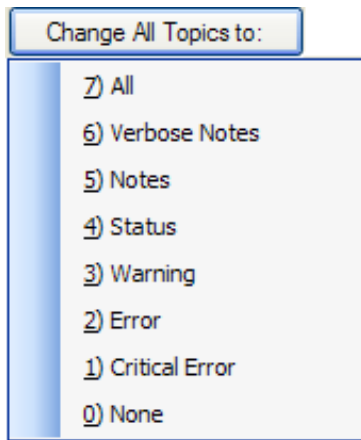
The higher the trace level, the more information will be returned by the filter. With a few exceptions, most subsystems start with the default tracing level configured to "Status" level (which includes status messages, warnings, and errors) or lower. Each trace level includes all levels below it.

A trace level of "Status" or lower will return some log information, but usually not enough for a support engineer to determine the root cause of a problem. Tracing usually must be at Notes level or higher for support engineers to troubleshoot an CIC system accurately.

Repeat steps 1-3 for other topics. When you are finished, press OK.

To filter all topics at a particular trace level

1. Click the **Change All Topics** to list.



2. Select one of the default topic levels. This configures the filter to search for all topics that have the selected trace level.
3. Click **OK**.

User interface options

Enable This Filter check box

This check box is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Topic Levels list

This list displays the names of all topics and the current topic level selection setting.

Change All Topics to drop list

Changes the level of all topics in the Topic Levels list to a preset verbosity range.

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

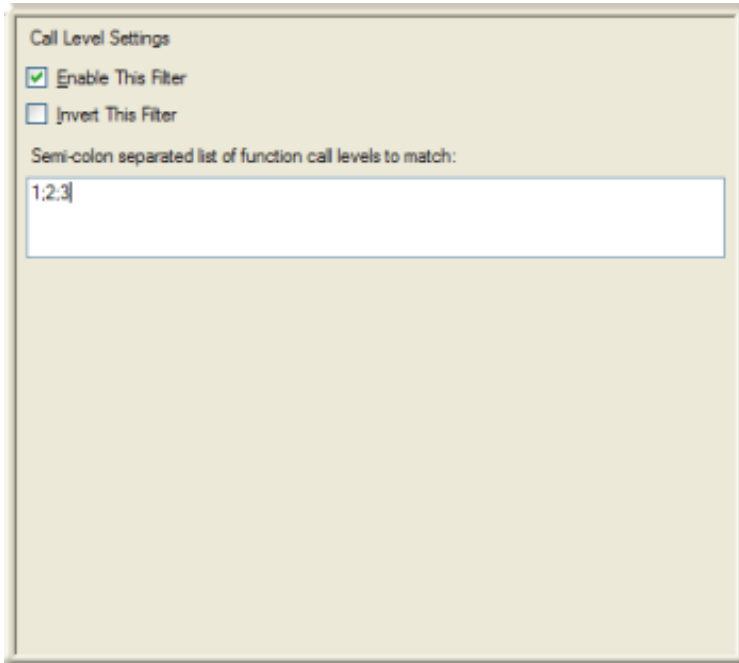
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Call Level



Call Level Settings

☒ Enable This Filter

☐ Invert This Filter

Semi-colon separated list of function call levels to match:

1;2;3

This criteria filters by call level. Call level (or call stack, if you prefer), is an indicator of functions calling other functions. The first calling function is level 0. If the main function calls a helper function, the helper is considered to be at call level 1, and so forth. Call levels help trace the flow of control from one function to another.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this check box. The filter selects all entries that do not match the criterion.

Semi-colon separated list of function call levels to match

Enter call level numbers delimited by semicolons. For example:

1;2;3

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

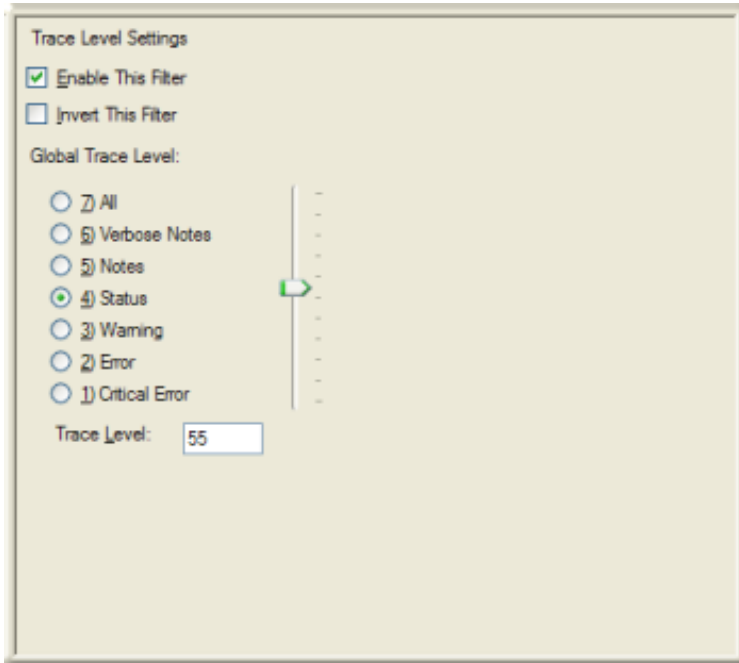
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Trace Level



This criteria filters all topics by a particular trace level, the number that determines the verbosity of messages written to the log.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this check box. The filter selects all entries that do not match the criterion.

Global Trace Level

The option buttons set the trace level to a predefined boundary. The slider control provides more granularity in numeric values. You can also type a level number directly in to the text box.

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

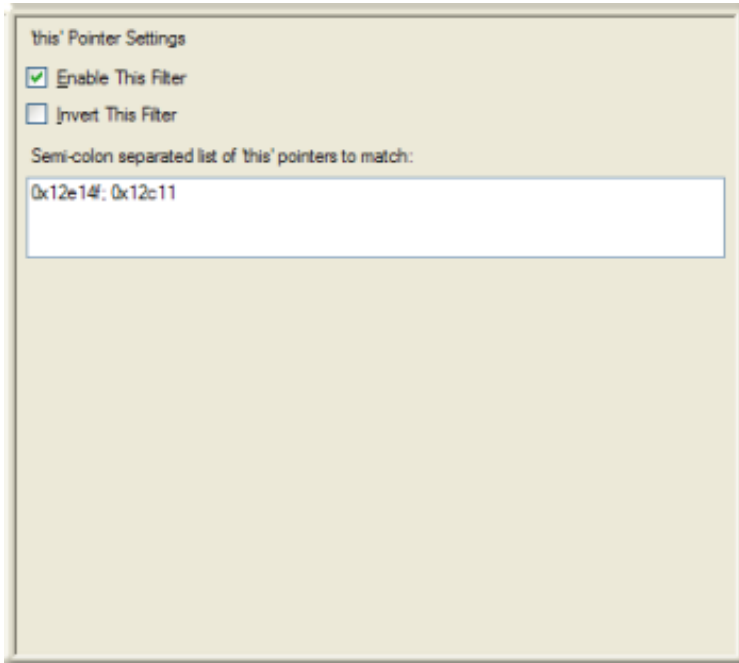
Cancel button

Closes the dialog box, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

This Pointer

The image shows a dialog box titled "this' Pointer Settings". It contains two checkboxes: "Enable This Filter" which is checked, and "Invert This Filter" which is unchecked. Below these is a text label "Semi-colon separated list of 'this' pointers to match:" followed by a text input field containing the hexadecimal values "0x12e14f; 0x12c11".

This criteria filters by pointer to a data structure internal to the code. If you are operating on a function that is part of a data object, *this pointer* indicates which data object. Pointers are hexadecimal values.

If the *this Pointer* column isn't visible in the message list, use the [Manage Columns](#) command to display it. This indicates pointer values that you can filter for.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter selects all entries that do not match the criterion.

Semi-colon separated list of 'this' pointers to match

Enter a semi-colon delimited list of hexadecimal pointer values. You do not need to prefix "0x", but that is allowed.

OK button

Closes the Filter Configuration dialog and applies the filter.

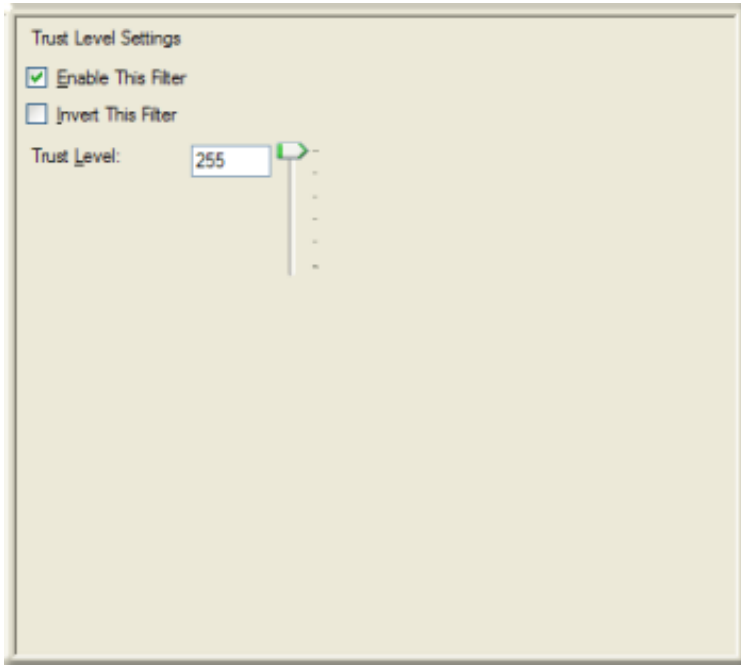
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Trust Level



This criteria filters by *level of trust* assigned to an assembly, a numeric value affecting what system resources the function had access to. Trust levels range from 0-255.

If the **Trust Level** column isn't visible in the message list, use the [Manage Columns](#) command to display it. This indicates pointer values for which you can filter.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear the check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, select this check box. The filter selects all entries that do not match the criterion.

Trust level

Enter or use the slider control to enter a value in the range 0-255.

OK button

Closes the **Filter Configuration** dialog and applies the filter.

Cancel button

Closes the dialog box, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Timestamp Range

Timestamp Range Settings

☒ Enable This Filter

☐ Invert This Filter

Options

☐ Specify an absolute date/time

☒ Specify a date-less time

Specify times in Log creator time

Time

☐ Don't Restrict Start Time ☐ Don't Restrict End Time

Start Time: 2007-10-24 11:39:47.9249

End Time: 2007-10-24 11:39:48.1725

Use this criteria to filter messages based on timestamp values.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Specify an absolute date/time

Indicates that you want to select both date and time values.

Specify a date-less time

Indicates that you want to filter using start and end times, but not any particular date.

Specify times in drop list

By default, time values in the *Timestamp* column are formatted for the log creator's time zone, meaning that the time reflects the time zone of the server or workstation that wrote the log entry. Log Viewer allows you to display Timestamp values using your local time zone, or in UTC format.

- Choose *Log creator time* to display timestamp values using the time zone of the server or workstation that wrote the log entry.
- Choose *Local time* to display timestamp values using the time zone of the local workstation.
- Choose *Universal time (UTC)* to display timestamp values in Universal Coordinated Time.

Don't Restrict Start Time checkbox

Check this box when you want to specify specific starting date and time values.

Start Time text boxes

These text boxes prompt for start date in the form yyyy-mm-dd, and for start time in the form hh:mm:ss:mmmm.

Don't Restrict End Time checkbox

Check this box when you want to specify specific ending date and time values.

End Time text boxes

These text boxes prompt for end date in the form yyyy-mm-dd, and for end time in the form hh:mm:ss:mmmm.

OK button

Closes the Filter Configuration dialog and applies the filter.

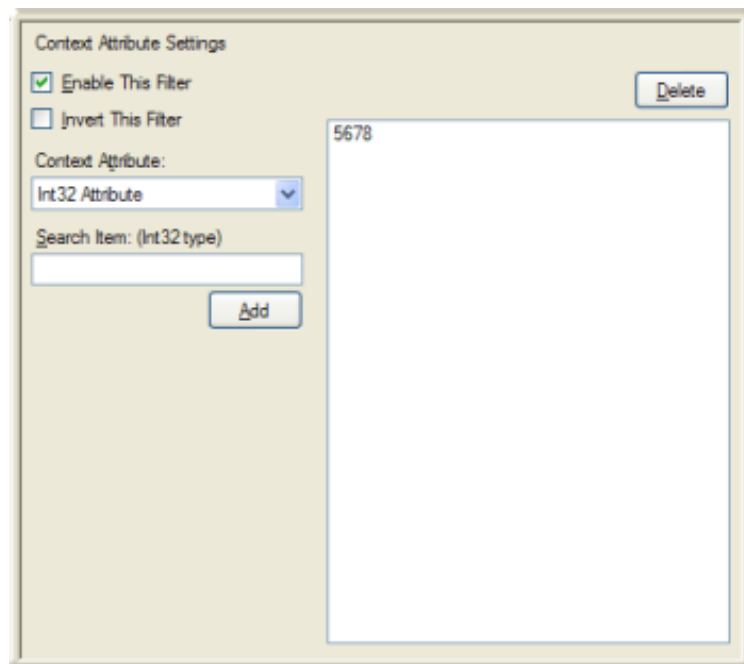
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Context Attribute



The image shows a dialog box titled "Context Attribute Settings". It contains the following elements:

- Two checkboxes: "Enable This Filter" (checked) and "Invert This Filter" (unchecked).
- A "Delete" button in the top right corner.
- A "Context Attribute:" label followed by a dropdown menu showing "Int32 Attribute".
- A "Search Item: (Int32 type)" label followed by a text input field.
- An "Add" button below the search input field.
- A large list box on the right side containing the value "5678".

This criteria filters by the value of specific *context attributes*. Context attributes tag log entries to identify a data element of some sort, such as a CallId or a specific user name. Subsystems add context attributes to individual log entries to associate a message with a specific item of information that can be used to group or filter data.

Enable This Filter checkbox

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

Context Attribute drop list

List of context attributes supported by this log file.

Search item text field

Enter a value for the attribute selected in the Context Attribute drop list. Then press Add.

Add button

Adds a context attribute name/value to filter on, to the list on the right side.

Delete button

Removes the selected entry from the list of attributes to filter.

OK button

Closes the Filter Configuration dialog and applies the filter.

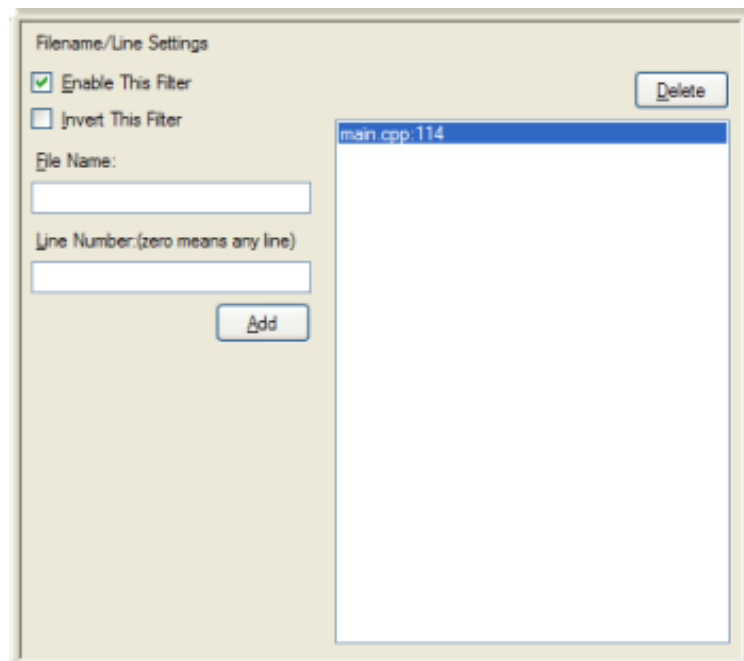
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Filename/Line



This feature is for internal use by Genesys. It filters for log entries written by a particular source code file, with the option to look for entries written by particular lines of code.

Enable This Filter checkbox

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

File Name text box

Specifies the name of the source code file.

Line Number

Specify 0 for any line of code in the file, or type a line number corresponding to a code statement.

Add button

Adds the File Name/Line Number pair to the list of items to filter.

Delete button

Removes the selected entry from the list of items to filter.

OK button

Closes the Filter Configuration dialog and applies the filter.

Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Within Scope

Within Scope Settings

☒ Enable This Filter

☐ Invert This Filter

File Name:

Line Number:

Add

Delete

NOTE: filenames that are not Enter Scope/Exit Scope messages will be ignored!

The *Within Scope* filter matches "Enter Scope" and "Exit Scope" type log messages and also matches all other log messages that occur between them on the same thread. The scope is identified by the filename/line pair that the scope messages have. This filter provides a useful view of everything that happened during the time the scope was active.

Enable This Filter checkbox

This checkbox is enabled by default, which causes this filter criteria to be evaluated when the filter is applied. Uncheck this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter checkbox

To invert the filter result, check this box. The filter will select all entries that do not match the criterion.

File Name text box

Specifies the name of the source code file. Filenames that are not Enter Scope/Exit Scope messages will be ignored.

Line Number

Specify 0 for any line of code in the file, or type a line number corresponding to a code statement in the file.

Add button

Adds the File Name/Line Number pair to the list of items to filter.

Delete button

Removes the selected entry from the list of items to filter.

OK button

Closes the Filter Configuration dialog and applies the filter.

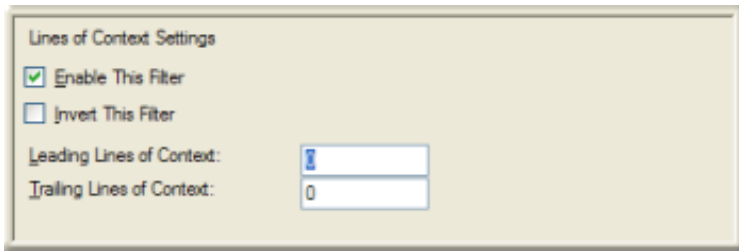
Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Lines of Context



This criteria filters for messages that appear within a number of lines preceding or following the result of some other filter criterion. This is best explained by example. Suppose that a log contained the following lines of data:

```
Hello
Goodbye
January
December
Halloween
```

And, suppose that you previously defined a regular expression string match (^J.*) to match all messages that start with the letter J. That string match would return a result set of:

```
January
July
```

If you were to define one leading line of context, the result set would return:

```
Goodbye   returned because it is one line before January
January   returned because it matched the regular expression
Halloween returned because it is one line before July
July      returned because it matched the regular expression
```

As you can see, one line before each match is included in the result set. This is very useful if you have a log message that is simply "Catching general exception" from an exception handler. If you filter the log for that statement it tells you there was an exception, but not what that exception was. If you print ten or so leading lines of context, then your log filter matches all of the exceptions, but print out the previous ten lines before each and you can tell what the exception was.

If you create a Lines of Context node as a parent node, you can build a sub-filter below it. The Lines of Context criteria is applied to the result of the sub-filter.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this check box. The filter selects all entries that do not match the criterion.

Leading Lines of Context

The number of preceding lines to include in the filter result.

Trailing Lines of Context

The number of trailing lines to include in the filter result.

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

Cancel button

Closes the dialog box, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Bookmarks



This criteria filters for bookmarked messages. It provides an easy means to select messages that are bookmarked throughout a log.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear this option to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this check box. The filter selects all entries that do not match the criterion.

OK button

Closes the **Filter Configuration** dialog and applies the filter.

Cancel button

Closes the dialog, but does not change filter settings.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

In Exception Unwind



This criteria filters for messages that were written while an exception unwind was in effect. Exception Unwind is a programming term. It indicates that a log record was traced, but not as part of the normal trace operation. Instead, it was traced prematurely because an exception was thrown and the code jumped up the call stack to locate a suitable catch handler for the exception type.

Enable This Filter check box

This check box is selected by default, which causes this filter criteria to be evaluated when the filter is applied. Clear the check box to temporarily exclude this criteria when the filter is applied.

Invert This Filter check box

To invert the filter result, select this check box. The filter selects all entries that do not match the criteria.

OK button

Closes the **Filter Configuration** dialog box and applies the filter.

Cancel button

Closes the dialog box, but does not change filter settings.

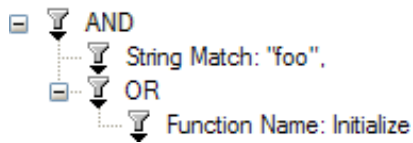
Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

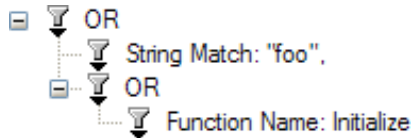
Logical Operations

Logical operations follow the rules of symbolic logic to evaluate expressions or a set of conditions. Log Viewer supports the use of AND / OR operators in filter configurations, so that users can define relationships between filter criteria that determine how the overall result will be evaluated.

Criteria are AND'd by default. But you can easily combine operators. Here is an example that uses both operators.



If you select Swap AND/OR filter, ANDs are converted to ORs and the result will be:



Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

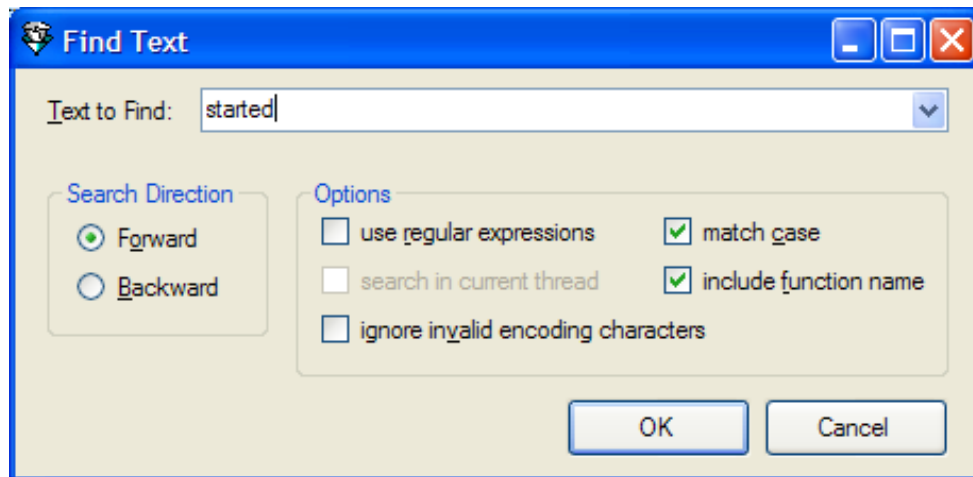
Clipboard Operations

If you right-click a filter in the **Filter Operations** pane, a context menu appears. This menu provides copy and paste commands that allow you to copy and paste filters.

Related Topics

- [Filter Criterion Choices](#)
- [Filter Configuration dialog](#)
- [Set Complex Filters](#)

Find Text dialog



The **Find Text** dialog box allows you to search for strings or patterns of text in the current log file. This dialog appears when you pull down the *Edit* menu and select *Search Forward* or *Search Backward*.

Text to Find drop list

Enter a literal string to find, a regular expression, or drop the list to select a previous entered search string.

Search Direction frame

Forward

Search from the current position in the file towards the end of the file.

Backward

Search from the current position in the file towards the beginning of the file.

Options frame

Use regular expressions check box

Indicates that the search string should be evaluated as a regular expression, rather than as a string literal.

Search in current thread

When checked, restricts the search to the current thread. Threads are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process and more than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled. The thread context includes all of the information the thread needs to seamlessly resume execution, including the thread's set of CPU registers and stack, in the address space of the thread's host process.

Ignore invalid encoding characters

Indicates that the search should ignore characters that do not fully conform to UTF-8. When invalidly encoded characters are ignored, any log message that has an illegal UTF-8 byte sequence is considered to be corrupt and never matches anything. It is good practice not to ignore invalid characters, since trace statements often accidentally contain ASCII strings that are not always legal UTF-8, especially in multi-byte Japanese languages. To match these messages as best as possible, uncheck this option to display text in multi-byte ASCII when illegal UTF-8 sequences are found.

Match case

When checked, performs a case-sensitive search.

Include function name

Indicates that the name of the function should be searched, regardless of whether the function name is toggled on using the [Show Function Names command](#).

OK button

Performs the search and closes the dialog. If the search succeeded, the search result is selected in the message view. Otherwise a beep will sound to indicate an unsuccessful search.

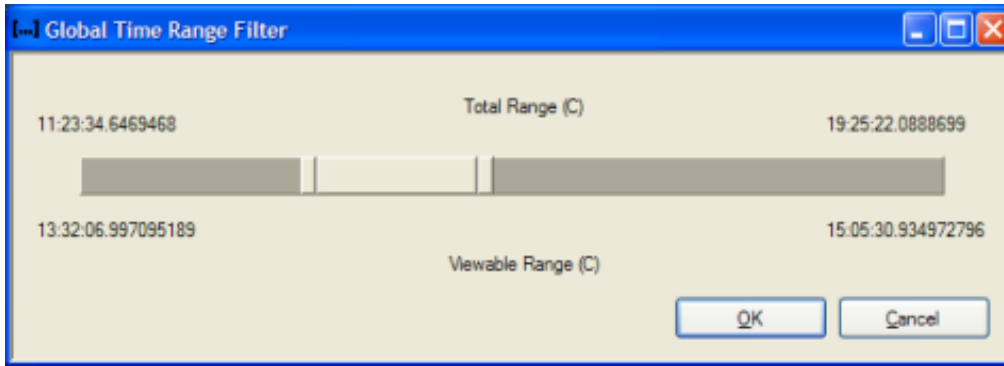
Cancel button

Closes the dialog without performing a search.

Related Topics

- [Find Text](#)

Global Time Range Filter dialog



This dialog box appears when the [Set Global Time Range Filter command](#) is issued. A *global time range* filter excludes all log entries that were logged outside of specified start and end times. Global filters persist until they are manually removed using the [Clear Global Time Range Filter command](#).

start time / end time slide controls

Once you set a global time filter, you can apply other filters to narrow down results. To use this dialog box, click and drag the start time or end time slide controls to new positions. The time values at the top apply show the log's start and end time. The timestamps at the bottom show the range that will be applied to the global filter.

OK button

Applies start and end times to apply a global filter, and closes the dialog. Setting a global filter usually reduces the number of entries in the message list.

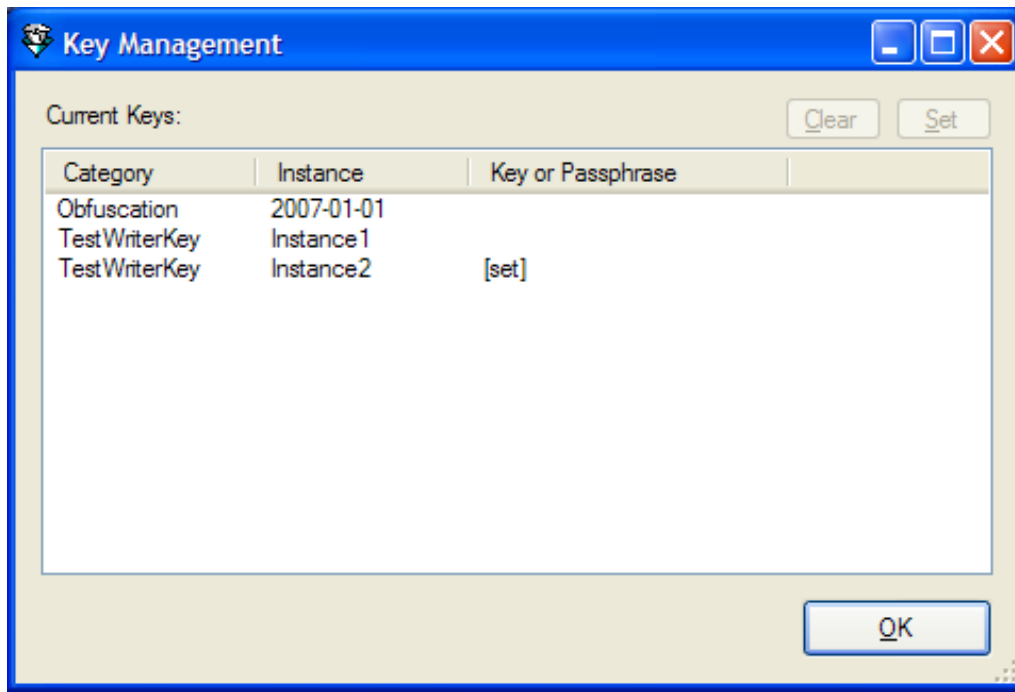
Cancel button

Dismisses the dialog box without changing or setting global filter settings.

Related Topics

- [Set Global Time Range Filter Begin](#)
- [Set Global Time Range Filter End](#)
- [Clear Global Time Range Filter](#)

Key Management dialog



The *Key Management* dialog box lists Category and Instance values that hint at the key or pass phrase needed to decrypt entries in the current log file. This dialog appears when you select **Key Management** from the **Tools** menu. The purpose of this dialog box is to present a list of keys in the current log file, so that you can decode them from a central location, bypassing the need to search the file to locate encrypted messages.

See [Decrypt multiple log messages](#) for procedures about this dialog.

Category column

Category is a general hint from the subsystem developer concerning the key or pass phrase.

Instance column

Instance is a more specific hint from the developer. Category and Instance work together to indicate the key or pass phrase needed to decrypt the key. Here are a few examples:

| Category | Instance |
|--------------|------------------|
| Passwords | UserPassword |
| Passwords | DatabasePassword |
| Passwords | AdminPassword |
| SIP TLS Keys | ServerToPhone |
| SIP TLS Keys | ServerToServer |

Key or passphrase column

This column indicates whether or not the related entry has been decoded.

If the column is blank, you may double-click the row to open the [Message Decryption Key dialog](#), to enter the required key.

If an entry was previously decoded, the word [set] appears in the *Key or Passphrase* column to indicate that the key has already been set.

If you entered a key but have not closed the Key Management dialog, the key or passphrase appears in the column.

Clear button

Clears the **Key** or **Passphrase** field for the selected row.

Set button

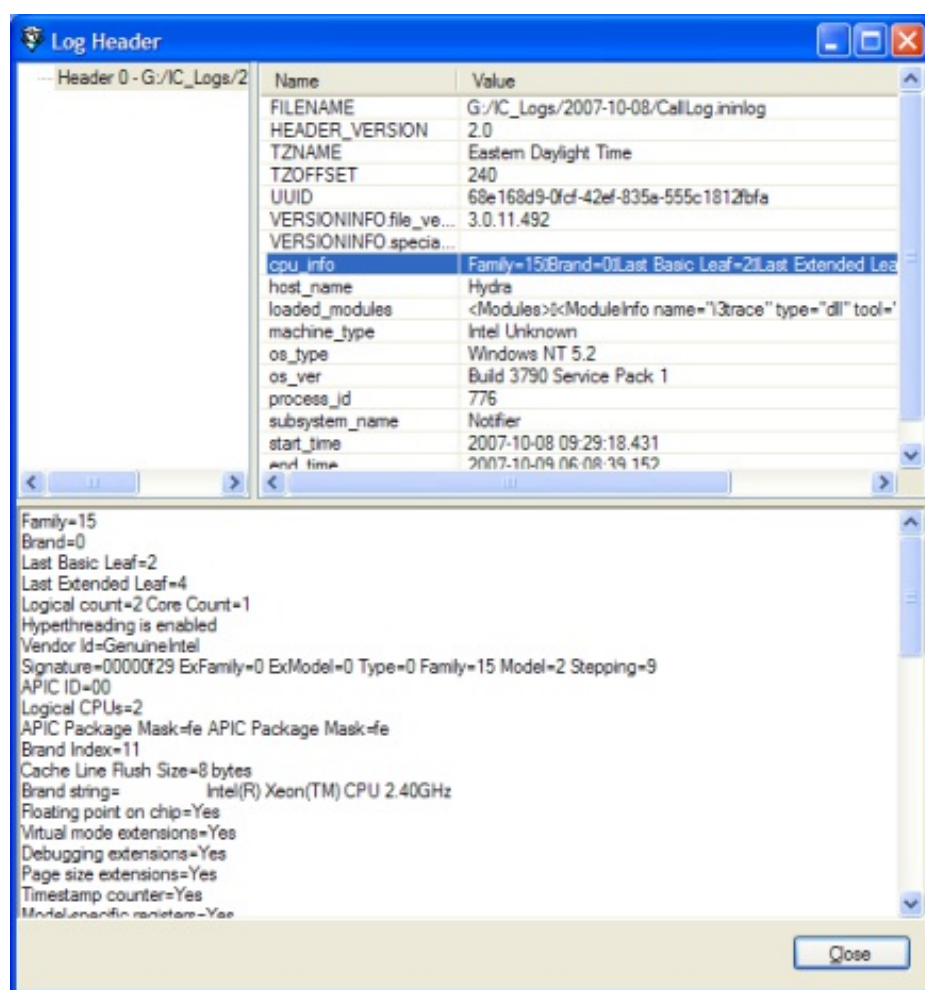
Opens the [Message Decryption Key dialog](#) so that you can enter a key or pass phrase.

No validation is performed to confirm that a key or pass phrase is valid. If you enter an invalid key, the related log message remain encrypted.

Related Topics

- [Decrypt multiple log messages](#)
- [Decrypt a log message](#)

Log Header dialog



The **Log Header** dialog box displays information about the current log file. It uses three panes to display information:

Log pane

The *Log* pane on the left selects a header to examine in the current log. If more than one header is available, you can select one in this list to display details.

List pane

The *List* pane displays a list of items for which information is available, and each item's value.

Detail pane

The *Detail* pane at the bottom displays the complete value of an item in the list pane. This is used to view items with values that are too large to display in the List pane.

When you finish, click **Close** to dismiss the **Log Header** dialog box.

Name/Value pairs in the List pane

FILENAME

The fully qualified path to the log file.

HEADER_VERSION

The version of the log's header section. This number identifies its format.

TZNAME

Time Zone Name

TZOFFSET

Time Zone Offset

UUID

Log's globally unique identifier.

VERSIONINFO.file_version

File version of the subsystem that created this log.

VERSIONINFO.special_build

Text field that the build process injects into binaries to identify the build. For example, "SU2" indicates *Service Update 2*; "ES 450" would identify *Engineering Special #450*.

cpu_info

List of CPU-related descriptors that identify capabilities of the processor on the machine that wrote the log file.

host_name

Name of the CIC server or workstation.

loaded_modules

Information about each .Net module, usually a .dll, used to trace this log.

machine_type

Hardware brand identifier or "Intel Unknown" if the machine type cannot be determined.

os_type

Operating system and its version number. (for example, Windows NT 5.1).

os_ver

Minor version of the operating system, such as Build 2600 Service Pack 2.

process_id

The numeric identifier of the process that logged this file.

subsystem_name

The name of the application or CIC subsystem for which log describes activity.

start_time

Time when this log was created.

end time

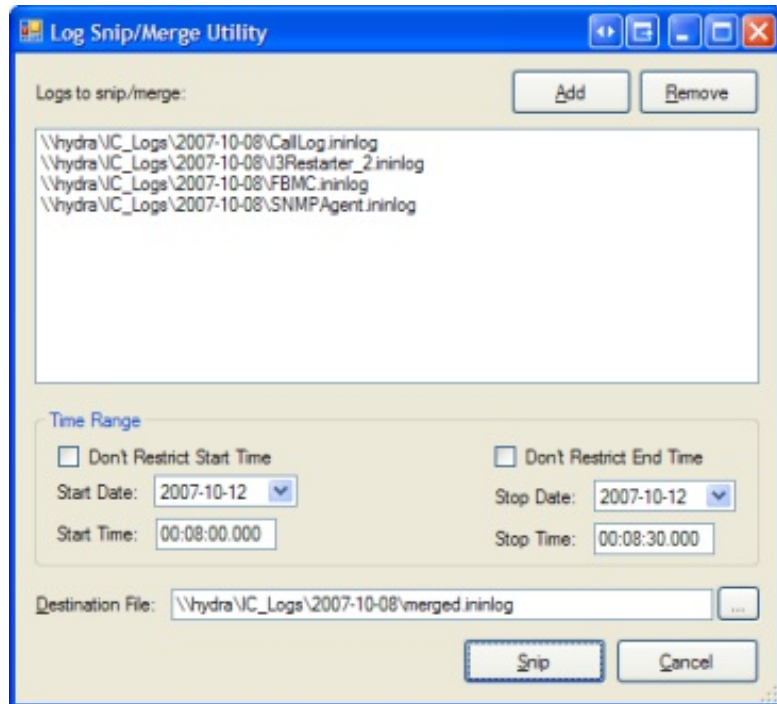
Time when last log entry was written.

Related Topics

- [Display Log Header Information](#)

Log Snip/Merge Utility

The Log Snip/Merge Utility snips (copies) all or part of a log file to a new file. It can merge entries from multiple logs into a new log file.



Add button

Opens the **File Open** dialog box so that you can select logs to snip or merge.

Remove button

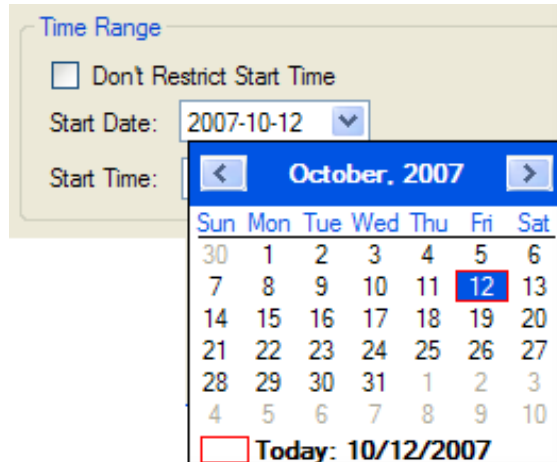
Removes the selected entry from the Logs to snip/merge list.

Don't Restrict Start Time check box

When selected, snips or merges starting with the first record in each log file. When cleared, the snip/merge operation starts at the date and time selected.

Start Date

Opens a calendar control so that you can select a different start date.



Start Time

This field prompts for a start time in *hh:mm:ss:nnnn* format. You do not need to enter times in thousands of a second, but precise selections of this type are supported.

Don't Restrict End Time check box

When selected, allows the snip or merge to end at a particular time in each log file. When cleared, the snip/merge operation ends when end-of-file is reached.

Stop Date

Opens a calendar control so that you can select a different end date.

Stop Time

This field prompts for a stop time in *hh:mm:ss:nnnn* format. You do not need to enter times in thousands of a second, but precise selections of this type are supported.

Destination File

Type the path and name of a new .ininlog file in this field. Pressing the ... button opens a File Save dialog that makes it easier to set the destination folder and filename.

Snip button

Snips or merges the selected files into the new file specified.

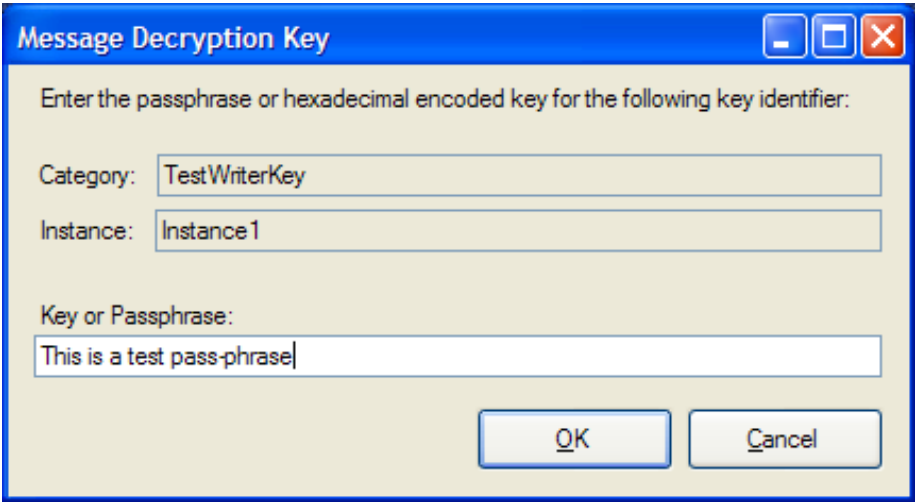
Cancel button

Closes the dialog box without snipping or merging files.

Related Topics

- [Snip/Merge Log Files](#)

Message Decryption Key dialog



This dialog prompts for information needed to decrypt some portion of a message.

Category

Category is a general hint from the subsystem developer concerning the key or passphrase. It classifies the type of information that was encrypted. This can be any string that the developer of the subsystem decided on. This is a read-only field.

Instance

Instance is also an arbitrary string created by the developer that provides a more specific hint. This is also a read-only field. Category and Instance are both displayed in the *Encryption Key Id* column. These fields hint at the key or passphrase that is needed to decrypt the entry.

| Message | Encryption Key Id |
|--|-------------------------|
| main() : Trace out an encrypted message[*** DATA ENCRYPTED - KEY NEEDED! ***]... | TestWriterKey/Instance1 |

Here are several examples of Category/Instance Pairs:

| Category | Instance |
|--------------|------------------|
| Passwords | UserPassword |
| Passwords | DatabasePassword |
| Passwords | AdminPassword |
| SIP TLS Keys | ServerToPhone |
| SIP TLS Keys | ServerToServer |

Key or Passphrase

The string needed to decrypt the message. A passphrase is a series of words or phrases such as "This is a test pass-phrase". A key is not composed of word. For example:

"bafe465169f42df88547bc66e50e811852964214917dd9b7e45523806771863f"

OK button

Decrypts the message if an appropriate Key or Passphrase was supplied, then closes the dialog.

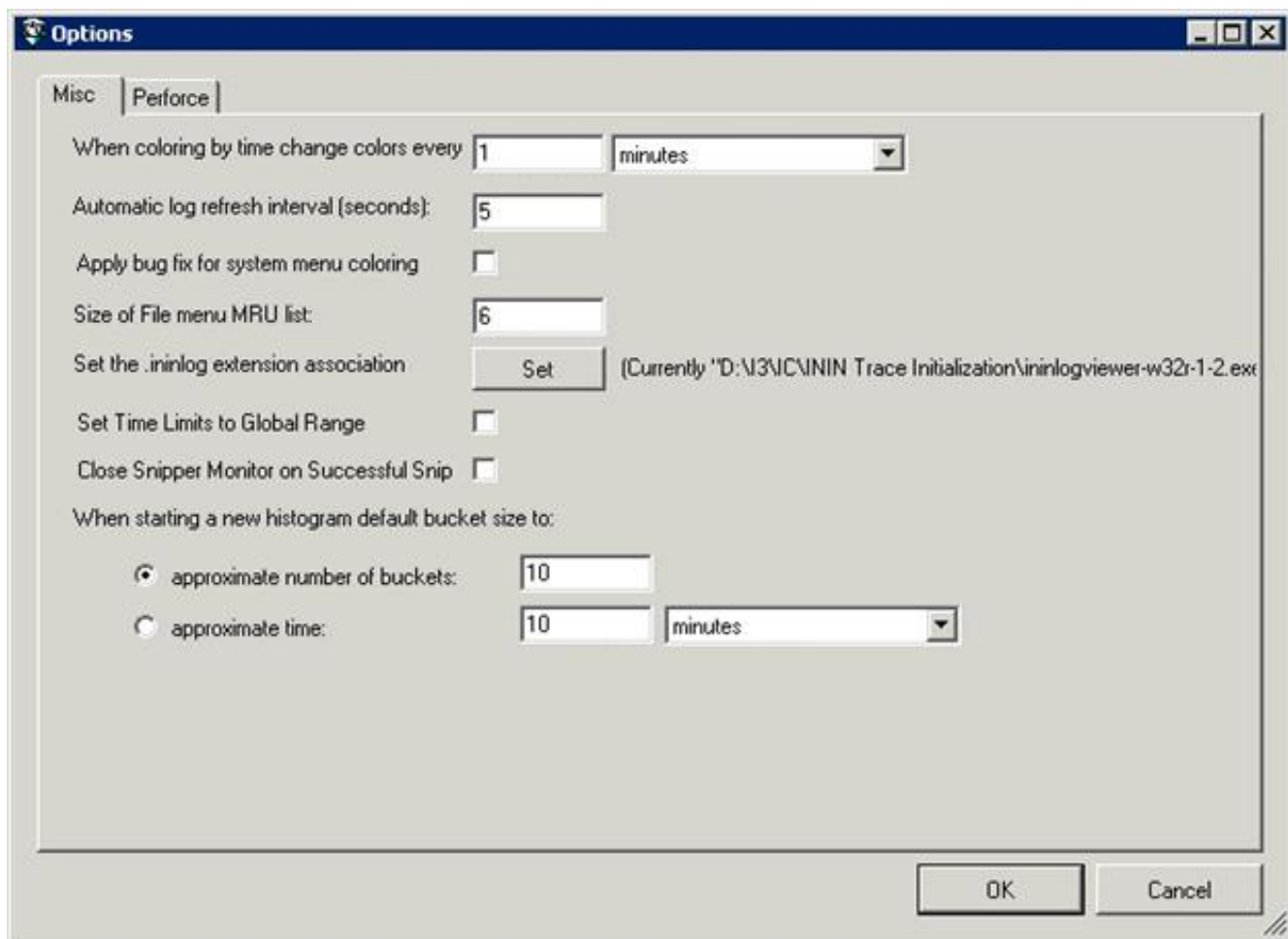
Cancel button

Closes the dialog and cancels the attempt to decrypt.

Related Topics

- [Decrypt a Log Message](#)
- [Manage Columns in the message list](#)

Options dialog – Misc tab



Use this dialog box to set general program preferences.

When coloring by time change colors every

This setting sets the amount of time that will be used to group entries by color when users click a timestamp heading in the message list to categorize by color. Columns are also colorized to group chronologically similar entries when time filters are applied. See [Colorize columns in the message list](#).

Automatic log refresh interval (seconds)

This setting determines the number of seconds that Log Viewer waits before reading the log file to refresh the display.

Apply bug fix for system menu coloring

This check box makes it easier to distinguish menu items when non-standard color schemes are used. Check this box if menus are hard to see on your system due to similarities between foreground and background colors.

Size of File menu MRU list

"MRU" refers to the list of most-recently used files that appears when you choose [Reopen](#) from the **File** menu. This setting sets the number of files that Log Viewer recalls to display in this list.

Set the .ininlog extension association

If you have permission to access the registry key HKEY_CLASSES_ROOT\ininlog, you can click **Set** to change the extension associated with log files. The default extension is .ininlog. Access to this registry key is restricted by default.

Set Time Limits to Global Range

When enabled, keeps global time ranges active at all times so that time ranges are not cleared by the **Clear All Filters** command.

Close Snipper Monitor on Successful Snip

When this option is enabled, the [Snipper/Monitor dialog](#) closes automatically when the process of snipping or merging log files is complete.

When starting a new histogram default bucket size to

Use this option to set the approximate number of buckets or time in minutes.

Related Topic

- [Set Application Options](#)

Options dialog – Perforce tab

The options on this tab of the Options dialog box are for Genesys internal use. This tab configures Log Viewer to display source code for the function that wrote the selected log entry. Lines of code for the function are displayed in the Source View pane. See [Show or hide related Source Code](#).

The **Default Perforce Server** manages code for all non-ION projects. The **Special Perforce Server** is dedicated exclusively to ION development.

Options

Misc **Performance**

Performance Mode: Perforce Client

Special Perforce Server

Semi-colon separated list of 'tiers' that use these perforce settings: core;data;intmgr;media;system;blm;tools;

\$P4PORT perforce:1888

\$P4USER

\$P4CLIENT

Default Perforce Server

\$P4PORT perforce:1666

\$P4USER

\$P4CLIENT

Legacy Search Drives

Semi-colon list of search paths (typically only search drives are necessary):

OK Cancel

Use perforce to find source files check box

This check box determines whether Log Viewer attempts to fetch and display source code from the application that wrote the selected log entry, if the code is not already resident in the referenced folder on the local workstation.

Special Perforce server frame

Semi-colon separated list of 'tiers' that use these performance settings

Semi-colon delimited list of folders to search in Perforce for source code files. Log Viewer will ask Perforce to search these folders and any child folders that they contain.

\$P4PORT

The host and port number of the Perforce server to communicate with. For example:
perforce:1888

\$P4USER

Perforce user name.

\$P4CLIENT

The name of the current client workspace.

Default Perforce server frame

\$P4PORT

The host and port number of the Perforce server to communicate with. For example:
perforce:1666

\$P4USER

Perforce user name.

\$P4CLIENT

The name of current client workspace.

Legacy search drives frame

Semi-colon list of search paths (typically only search drives are necessary)

Semi-colon delimited list of search paths, used to locate files in Perforce's *product root* folder. For example, if you have drive letters assigned for each build product, you can enter drive letters delimited using semicolons. For example:

K;Y;Z

A more often-used technique is to specify paths that point to product root directories. For example:

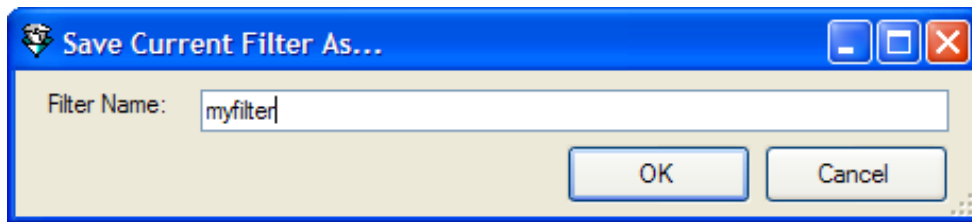
K:\systest\eic\rum

f:\builds\systest\eic\red;f:\builds\systest\eic\rum;f:\builds\systest\eic\yellow

Related Topics

- [Set Application Options](#)
- [Show or hide related Source Code](#)
- <http://www.perforce.com>

Save Current Filter As dialog



This dialog box prompts for the name of a filter to save. It appears when you choose the **Filter > Saved Filters > Save Current Filter As** command. When you save a filter, its name appears in the **Filter** menu under **Saved Filters**.

Filter name

This name can be anything you like. Type a descriptive name for the filter that will help you recall what it does later.

OK button

Saves the filter using the name specified and closes the dialog.

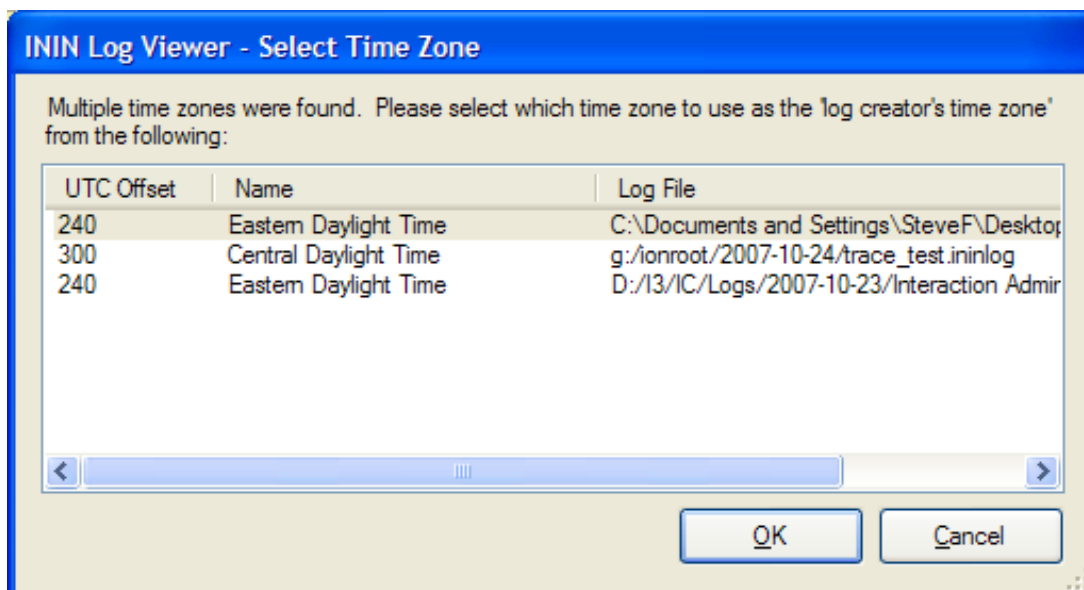
Cancel button

Closes the dialog without saving the current filter.

Related Topics

- [Save the current filter](#)

Select Time Zone dialog

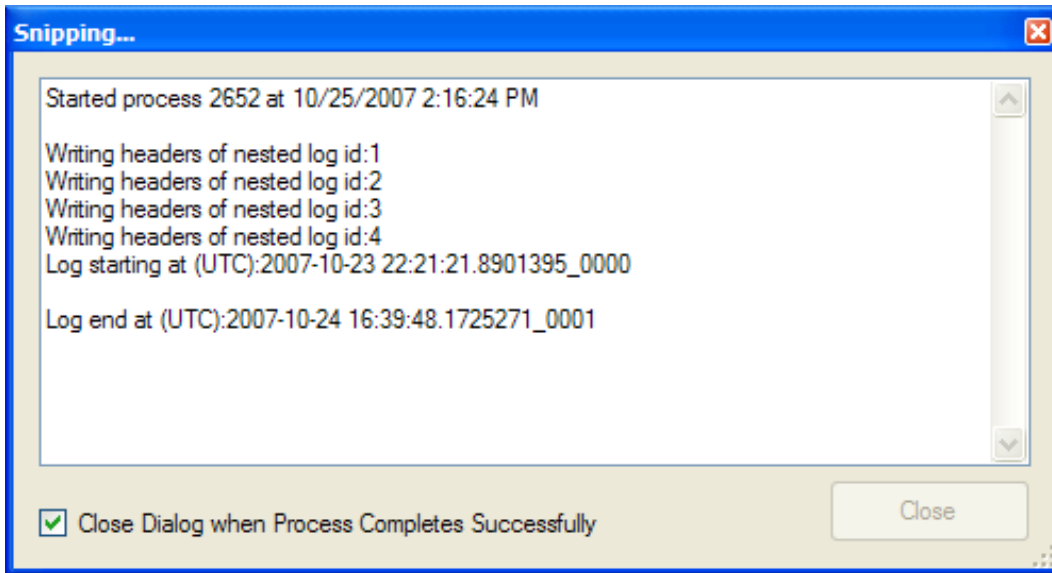


When merging or snipping logs to a new file, you may be asked to specify the log creator's time zone. Time zones from each merged file are normalized to the zone you select. Select a time zone in the list, and then click **OK**. The snip/merge operation then proceeds.

Related Topics

- [Log Snip/Merge Utility](#)
- [Snip/Merge Log Files](#)

Snipper Monitor dialog



The Snipper Monitor dialog box appears when logs are being snipped or merged. It displays status information as work is performed. This is useful when large logs are processed.

Message list

This control displays status messages about the current snip/merge operation.

Close Dialog when Process Completes Successfully

When this check box is selected, the Snipper Monitor dialog box automatically closes itself after this particular snip/merge operation ends. You can configure Log Viewer to always close this dialog box automatically. See [Options dialog – Misc tab](#) for details.

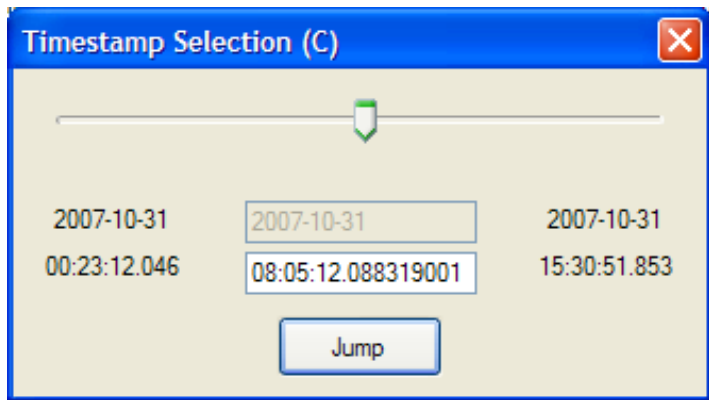
Close button

Manually closes the dialog. This button is disabled when the process is running.

Related Topics

- [Log Snip/Merge Utility](#)
- [Snip/Merge Log Files](#)

Timestamp Selection dialog



Slider bar

Adjusts the value displayed in the Timestamp field.

Date box

If the log spans more than one day, this text box is enabled so that you can specify a date in the format yyyy-mm-dd.

Timestamp field

Prompts for entry of a timestamp in hh:mm:ss:mmmm format.

Related Procedure:

- [Jump to \(or near\) a specific timestamp](#)

Revisions

This topic summarizes changes in Log Viewer.

PureConnect 2018 R3

No changes.

CIC 2016 R1

Updated to reflect new branding and the transition from Interaction Client .NET Edition to Interaction Desktop.

CIC 2015 R1

Updated documentation to reflect changes required in the transition from version 4.0 SU# to CIC 2015 R1, such as updates to product version numbers, system requirements, installation procedures, references to Interactive Intelligence Product Information site URLs, and copyright and trademark information.

IC 4.0 Service Update 5

Note that when tracing levels are modified in Interaction Administrator for specific users, the tracing change is not reflected in Trace Config utility on the user's workstation. This is a display issue only. Opening up the log does reflect the change.

IC 4.0 Service Update 4

No documentation revisions.

IC 4.0 Service Update 3

The StatServer sub-system (StatServerU.exe) was split into two binaries that replaced StatServerU.exe in the \I3\IC\Server\ folder on the IC server. The old log file (StatServer.ininlog) was also deprecated and replaced by new logs:

- StatServerAgent[U|UD].exe handles agent related statistics. Its log file is statserveragent.ininlog
- StatServerWorkgroup[U|UD].exe handles workgroup related statistics. Its log file is statserverworkgroup.ininlog.

The split enhances processing power and allows for statistics gathering in larger environments with higher call rates.

IC 4.0 Service Update 2

A journal file is now created to track log start/stop times. When dealing with a subsystem that produces large log files, it can be difficult to know which logs contain entries for a specific time range. To make this task easier, an additional file is created per subsystem to denote when instances of the subsystem start and stop.

All ininlog files now have a single 'journal' file that is maintained in parallel with the logs. There is only one journal for a log, no matter how many times a subsystem starts and stops, and regardless of whether it runs simultaneously more than once.

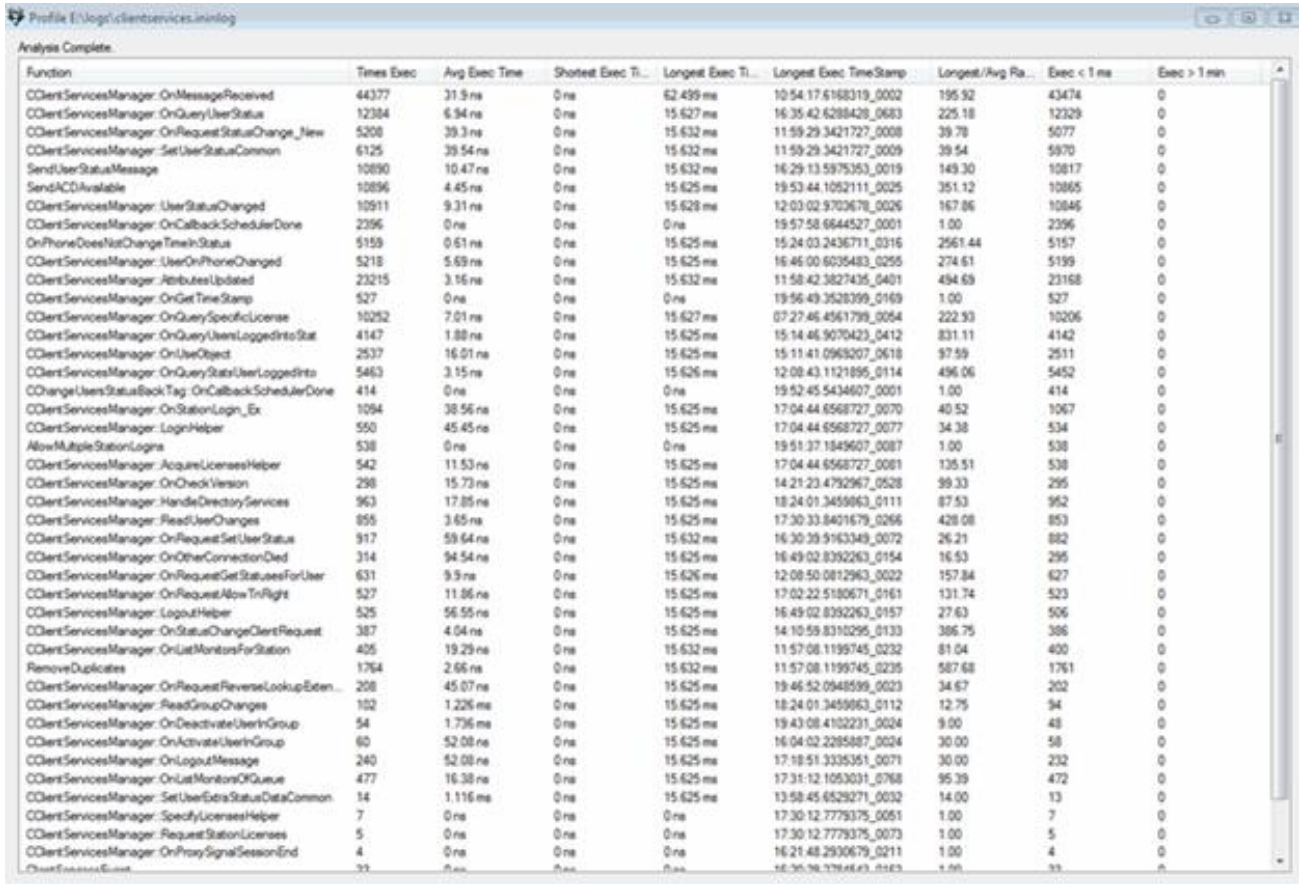
For log files like TSServer.ininlog, TSServer_1, and so on,, the journal file is named TSServer.ininlog_journal. It contains a timestamp for each entry and log when a log file is created and when it is closed. This file can be used to determine which log file contains a particular timestamp range you're interested in.

IC 4.0 Service Update 1

No documentation revisions.

IC 4.0 GA

- The IC User Apps install now adds shortcuts for starting `inintraceconfig` and `ininlogviewer` from the Start Menu > Programs > Interactive Intelligence folder.
- If you're looking at a log and hit "refresh", you may not see new messages immediately, since trace messages are buffered. You can optionally disable buffering by setting the `ININ_TRACE_BUFFERSIZE` environment variable to 0.
- Log Viewer has a new 'profiler' feature, based on enter and exit scope tracing. With a log file open, select **Profile** from the **Tools** menu to get output similar to:



Profile E:\Logs\clientservices.ininlog

Analysis Complete.

| Function | Times Exec | Avg Exec Time | Shortest Exec Ti... | Longest Exec Ti... | Longest Exec TimeStamp | Longest/Avg Ra... | Exec < 1 ms | Exec > 1 min |
|--|------------|---------------|---------------------|--------------------|------------------------|-------------------|-------------|--------------|
| COClientServicesManager: OnMessageReceived | 44377 | 31.9 ns | 0 ns | 62.439 ms | 10:54:17.6168319_0002 | 195.92 | 43474 | 0 |
| COClientServicesManager: OnQueryUserStatus | 12384 | 6.94 ns | 0 ns | 15.627 ms | 16:35:42.6288428_0683 | 225.18 | 12329 | 0 |
| COClientServicesManager: OnRequestStatusChange_New | 5208 | 39.3 ns | 0 ns | 15.632 ms | 11:59:29.3421727_0008 | 39.78 | 5077 | 0 |
| COClientServicesManager: SetUserStatusCommon | 6125 | 39.54 ns | 0 ns | 15.632 ms | 11:59:29.3421727_0009 | 39.54 | 5970 | 0 |
| SendUserStatusMessage | 10890 | 10.47 ns | 0 ns | 15.632 ms | 16:29:13.5975353_0019 | 149.30 | 10817 | 0 |
| SendACDAvailable | 10896 | 4.45 ns | 0 ns | 15.625 ms | 19:53:44.1052111_0025 | 351.12 | 10865 | 0 |
| COClientServicesManager: UserStatusChanged | 10911 | 9.31 ns | 0 ns | 15.628 ms | 12:03:02.9702678_0026 | 167.86 | 10846 | 0 |
| COClientServicesManager: OnCallbackSchedulerDone | 2296 | 0 ns | 0 ns | 0 ns | 19:57:58.6644527_0001 | 1.00 | 2296 | 0 |
| OnPhoneDoesNotChangeTimeInStatus | 5159 | 0.61 ns | 0 ns | 15.625 ms | 15:24:03.2436711_0316 | 2561.44 | 5157 | 0 |
| COClientServicesManager: UserOnPhoneChanged | 5215 | 5.69 ns | 0 ns | 15.625 ms | 16:46:00.6035483_0295 | 274.61 | 5199 | 0 |
| COClientServicesManager: AttributesUpdated | 23215 | 3.16 ns | 0 ns | 15.632 ms | 11:58:42.3827435_0401 | 494.69 | 23168 | 0 |
| COClientServicesManager: OnGetTime Stamp | 527 | 0 ns | 0 ns | 0 ns | 19:56:49.3528399_0169 | 1.00 | 527 | 0 |
| COClientServicesManager: OnQuerySpecificLicense | 10252 | 7.01 ns | 0 ns | 15.627 ms | 07:27:46.4561799_0054 | 222.93 | 10206 | 0 |
| COClientServicesManager: OnQueryUsersLoggedIntoStat | 4147 | 1.88 ns | 0 ns | 15.625 ms | 15:14:46.9070423_0412 | 831.11 | 4142 | 0 |
| COClientServicesManager: OnUseObject | 2537 | 16.01 ns | 0 ns | 15.625 ms | 15:11:41.0968207_0618 | 97.59 | 2511 | 0 |
| COClientServicesManager: OnQueryStatusUserLoggedInto | 5463 | 3.15 ns | 0 ns | 15.626 ms | 12:08:43.1121895_0114 | 486.06 | 5452 | 0 |
| COChangeUsersStatusBack Tag: OnCallbackSchedulerDone | 414 | 0 ns | 0 ns | 0 ns | 19:52:45.5434607_0001 | 1.00 | 414 | 0 |
| COClientServicesManager: OnStationLogin_Exit | 1094 | 38.56 ns | 0 ns | 15.625 ms | 17:04:44.6568727_0070 | 40.52 | 1067 | 0 |
| COClientServicesManager: LoginHelper | 550 | 45.45 ns | 0 ns | 15.625 ms | 17:04:44.6568727_0077 | 34.38 | 534 | 0 |
| AllowMultipleStationLogins | 538 | 0 ns | 0 ns | 0 ns | 19:51:37.1849607_0087 | 1.00 | 538 | 0 |
| COClientServicesManager: AcquireLicensesHelper | 542 | 11.53 ns | 0 ns | 15.625 ms | 17:04:44.6568727_0081 | 135.51 | 538 | 0 |
| COClientServicesManager: OnCheckVersion | 298 | 15.73 ns | 0 ns | 15.625 ms | 14:21:23.4792967_0528 | 99.33 | 295 | 0 |
| COClientServicesManager: HandleDirectoryServices | 963 | 17.85 ns | 0 ns | 15.625 ms | 18:24:01.3459863_0111 | 87.53 | 952 | 0 |
| COClientServicesManager: ReadUserChanges | 855 | 3.65 ns | 0 ns | 15.625 ms | 17:30:33.8401679_0266 | 428.08 | 853 | 0 |
| COClientServicesManager: OnRequestSetUserStatus | 917 | 59.64 ns | 0 ns | 15.632 ms | 16:30:39.5163349_0072 | 26.21 | 882 | 0 |
| COClientServicesManager: OnOtherConnectionDied | 314 | 94.54 ns | 0 ns | 15.625 ms | 16:49:02.8392263_0154 | 16.53 | 295 | 0 |
| COClientServicesManager: OnRequestGetStatusesForUser | 631 | 9.9 ns | 0 ns | 15.626 ms | 12:08:50.0812963_0022 | 157.84 | 627 | 0 |
| COClientServicesManager: OnRequestAllowTrnRight | 527 | 11.86 ns | 0 ns | 15.625 ms | 17:02:22.5180671_0161 | 131.74 | 523 | 0 |
| COClientServicesManager: LogoutHelper | 525 | 56.55 ns | 0 ns | 15.625 ms | 16:49:02.8392263_0157 | 27.63 | 506 | 0 |
| COClientServicesManager: OnStatusChangeClientRequest | 387 | 4.04 ns | 0 ns | 15.625 ms | 14:10:59.8310295_0133 | 386.75 | 386 | 0 |
| COClientServicesManager: OnListMonitorsForStation | 405 | 19.29 ns | 0 ns | 15.632 ms | 11:57:08.1199745_0232 | 81.04 | 400 | 0 |
| RemoveDuplicates | 1764 | 2.66 ns | 0 ns | 15.632 ms | 11:57:08.1199745_0235 | 587.68 | 1761 | 0 |
| COClientServicesManager: OnRequestReverseLookupExtern... | 208 | 45.07 ns | 0 ns | 15.625 ms | 19:46:52.0948599_0023 | 34.67 | 202 | 0 |
| COClientServicesManager: ReadGroupChanges | 102 | 1.225 ms | 0 ns | 15.625 ms | 18:24:01.3459863_0112 | 12.75 | 94 | 0 |
| COClientServicesManager: OnDeactivateUserInGroup | 54 | 1.736 ms | 0 ns | 15.625 ms | 19:43:08.4102231_0024 | 9.00 | 48 | 0 |
| COClientServicesManager: OnActivateUserInGroup | 60 | 52.08 ns | 0 ns | 15.625 ms | 16:04:02.2285887_0024 | 30.00 | 58 | 0 |
| COClientServicesManager: OnLogoutMessage | 240 | 52.08 ns | 0 ns | 15.625 ms | 17:19:51.3335351_0071 | 30.00 | 232 | 0 |
| COClientServicesManager: OnListMonitorsOfQueue | 477 | 16.38 ns | 0 ns | 15.625 ms | 17:31:12.1053031_0768 | 95.39 | 472 | 0 |
| COClientServicesManager: SetUserExtraStatusDataCommon | 14 | 1.116 ms | 0 ns | 15.625 ms | 13:58:45.6529271_0032 | 14.00 | 13 | 0 |
| COClientServicesManager: SpecifyLicensesHelper | 7 | 0 ns | 0 ns | 0 ns | 17:30:12.7779375_0051 | 1.00 | 7 | 0 |
| COClientServicesManager: RequestStationLicenses | 5 | 0 ns | 0 ns | 0 ns | 17:30:12.7779375_0073 | 1.00 | 5 | 0 |
| COClientServicesManager: OnProxySignalSessionEnd | 4 | 0 ns | 0 ns | 0 ns | 16:21:48.2930679_0211 | 1.00 | 4 | 0 |
| ClientServicesEvent | 39 | 0 ns | 0 ns | 0 ns | 16:36:36.1794843_0163 | 1.00 | 39 | 0 |

Each column is sortable. You can optionally right-click an entry to jump to that function's longest execution Scope Entry line in the logfile. One limitation is that you cannot have any filters applied to the logfile when running the profiler. The profile functionality will work with a Global Time Range Filter set, but it will not work with named/adhoc filters.

- Updated the procedure titled [Grant permission to run IC System Manager](#) for user interface changes in Interaction Administrator.
- Updated [Filter Criterion dialog](#) to cover options that apply ad-hoc or named filters.
- Updated explanation of the [Bookmarks dialog](#) to cover new import/export options.
- Removed references to versions of IC prior to 4.0 as distinctions between IC 2.x and IC 3.x no longer apply.
- Updated screen cap of the [About dialog](#) to show Log Viewer's current version number.

Change log

| Date | Changes |
|---------------|---|
| 20-March-2020 | Made it easier to find (with a link from Log Viewer) and understand how to Open a log file . |

Glossary

Admin Services

Admin Services retrieves security and profile information from Directory Services. Directory Services and Admin Services work together to handle connectivity to the Exchange Server. Directory Services handles user configuration and addressing issues, while Admin Services handles security and profiles.

Alert Services

This subsystem allows users and supervisors to define specific circumstances (e.g., average hold time > 10 minutes) under which they are to be alerted and the means by which the alert is to occur (e.g., e-mail, pager, phone call, etc.).

Authentication

Notifier uses challenge/response techniques to authenticate other components and applications to increase the security of products built around the Interaction Center Platform.

Client Services

Client Services is the subsystem of CIC that keeps track of logged-in users, their status, and their rights based on security configurations. Without Client Services there would not be a client interface, such as the CIC clients.

Compression Services

This subsystem compresses audio recordings such as voice mail messages using the TrueSpeech compression algorithm.

Context Attributes

Context Attributes tag message entries to identify a data element of some sort, such as a CallId or a specific user name. Subsystems add context attributes to individual log entries to associate a message with a specific item of information that can be used to group or filter data.

Customer Interaction Center (CIC)

Customer Interaction Center (CIC) is designed for sophisticated contact centers managing inbound, outbound, or blended interactions. CIC provides skills-based routing not only for telephone interactions, but faxes, Emails, text chats, Web call-back requests, and voice over IP calls. CIC can support up to several hundred agents per site, and offers optional pre and post-call routing across multiple locations. And it makes screen popping a breeze, with easy interfaces to products from leading CRM vendors such as Siebel, Pivotal, Onyx, Peoplesoft, and many more.

Data Services

Data Services integrates CIC with relational database management systems such as Microsoft SQL Server, Oracle, Sybase, IBM DB2, etc.

Directory Services

Directory Services manages a repository of CIC configuration information in the Windows NT Registry. When Microsoft Exchange or IBM Notes/Domino support is installed, CIC user information in Directory Services is synchronized with the corresponding entries in the mail server's address book. Directory Services and Admin Services work together to handle connectivity to the Exchange Server. Directory Services handles user configuration and addressing issues, while Admin Services handles security and profiles.

Email Services

Email services integrate CIC with popular e-mail systems such as Microsoft Exchange, IBM Notes, Novell Groupwise, Sun/iPlanet Messaging Server, and other SMTP/IMAP-based systems.

Fax Services

Fax Services is the CIC subsystem that sends and receives faxes.

Handlers

Interaction Processor executes small programs called **handlers** in response to unique events and to specify how the system will behave. When the Interaction Processor recognizes an event that it needs to act upon, it turns to the list of handlers to determine which one should respond to that event. It then runs an instance of that handler and any subroutine handlers that are necessary. Multiple instances of handlers can run at the same time, as those multiple events occur. Once the handler has completed its routine, it deletes itself from the system.

Host Services

Host Services allow CIC to communicate with mainframes and IBM AS/400 systems using the 3270 and 5250 terminal emulation protocols.

IC Server

Customer Interaction Center (CIC) is a client/server software product that transforms a Windows NT server into a comprehensive communications system. The IC server answers and processes calls. The profiles you create in Interaction Attendant are saved to the IC server where they are executed when a call is picked up.

Interaction Attendant

The graphical tool for configuring and maintaining CIC's auto attendant.

Interaction Designer

The CIC graphical application development tool for creating, debugging, editing, and managing handlers and subroutines.

Interaction Processor

Interaction Processor tells the CIC system how to behave based upon any events that occur. An incoming call is just one example of an event that CIC recognizes.

LogSnipper

A command-line utility that saves portions of a log file to a separate disk file. Trace Viewer reads log files and snippets.

Log Snippet

A portion of a subsystem log saved as a separate file.

Logs

Each CIC subsystem writes system messages in the form of logs. A log is a binary file that stores information about an event of some sort, to record normal operation or an abnormal condition. Log entries cannot be modified, but logs can be appended to. Logs maintain a record of processing steps completed, and record the state a CIC subsystem at a specific point in time. Logs entries can be snipped (extacted) using LogSnipper and read using the Trace Viewer utility.

Notifier

The Notifier is a Customer Interaction Center module that acts as a communication center for all other modules. It listens for events generated by other modules and notifies other interested modules that the event has occurred. Notifier makes use of the TCP/IP protocol to communicate with the rest of the Interaction Center Platform. It provides critical services such as Authentication, Request/Response Processing, and Publish/Subscribe Event Processing. Connections between Notifier and other components can be encrypted for maximum security. Notifier passes information between subsystems in real-time. For example, a supervisory application can display the real-time status of every agent in a call center. When an agent finishes a call and hangs up the phone, an icon on the supervisor's screen instantly changes. Similarly, if an administrator changes a user's security rights to disallow access to phone line information, a notebook tab instantly disappears from the user's screen. Notifier's publish/subscribe capabilities reduce overall network traffic by sending event notifications only to components that actually care about them. This allows applications using the Interaction Center Platform to handle much larger numbers of users and interactions.

Object

Everything in CIC is an object, and objects must be stored in lists, or queues. CIC handles several different types of queues, including users, stations, lines, and so on, so we need some way to manage the activity on these queues. For example, you can have call objects, user queue objects, station queue objects, and so on.

OCR Services

Optical Character Recognition services convert faxes to textual documents in specific formats such as Microsoft Word.

Paging Services

CIC uses the Paging Services subsystem to issue digital pages to paging services supporting the TAP protocol.

Process

A process is the execution of a program. It is a collection of virtual memory space, code, data, and system resources. Each process is a distinct entity, able to execute and terminate independently of all other processes. A 32-bit application has at least one process and one thread. A processor executes threads, not processes. Prior to the introduction of multiple threads of execution, applications were all designed to run on a single thread of execution.

Publish/Subscribe Event Processing

The Customer Interaction Center Platform is largely event-driven. Using Notifier, different components can register or "subscribe" for specific events. For example, the Fax Services component might register for all events regarding an outbound call. If that call were suddenly disconnected, Notifier would receive a notification from Telephony Services and then forward the event notification to Fax Services, allowing it to terminate the outgoing fax operation.

Queue

Queues are containers for calls and other types of interactions that can be processed. Each CIC client user has a user queue. Each workgroup, such as marketing or support, has a workgroup queue. Stand-alone phones not connected to PCs and fax machines have station queues.

Queue Manager

Queue Manager is the CIC subsystem that handles queue representations as a logical map of what is occurring within the system at any given time.

Request/Response Processing

Customer Interaction Center Platform components don't communicate directly with each other. Instead, they make requests for services of Notifier and Notifier then forwards the requests to the appropriate components. When Notifier receives a response, it then sends this response to the originating component. For example, the Fax Services component may need to make an outbound call to send a fax. It issues a request for an outbound call to Notifier, which forwards the request to the Telephony Services component. When the outbound call is made, Telephony Services sends a response to Notifier, which then forwards the response to Fax Services. In this way, Fax Services doesn't need to know where (i.e., on which machine) Telephony Services resides.

Speech Recognition Services

Speech Recognition services recognize spoken commands and phrases for applications such as speech-enabled IVR (interactive voice response).

Station Groups

Station groups are groups of phones in break rooms, conference rooms, and other public areas.

Station Queue

A queue where interactions are placed when they are to be processed by a station.

Statistical Services

This subsystem tracks important statistical information for real-time views and historical reporting.

Telephony Services

Telephony Services is the only CIC subsystem that interfaces directly with telephony hardware. This software layer provides a line of demarcation between the rest of Customer Interaction Center and telephony hardware. All voice traffic coming from the Public Switched Network goes to the telephony hardware and it stays below that line. The Telephony Services software processes call data and then communicates to the telephony hardware the information necessary to direct the call to the correct party.

Text-to-Speech (TTS) Services

Convert text such as e-mail messages to audio that can be played over a telephone.

Threads

Threads are the basic unit to which an operating system allocates processor time. A thread is code that is to be serially executed within a process and more than one thread can be executing code inside a process. Each thread maintains exception handlers, a scheduling priority, and a set of structures the system uses to save the thread context until it is scheduled. The thread context includes all of the information the thread needs to seamlessly resume execution, including the thread's set of CPU registers and stack, in the address space of the thread's host process.

Time Slicing

A program can allocate processor time to units in its body. Each unit is then given a portion of the processor time. Even if your computer has only one processor, it can have multiple units that work at the same time. The trick is to slice processor time and give each slice to each processing unit. The smallest unit that can take processor time is called a thread. A program that has multiple threads is referred to as a multithreaded application.

Trace Viewer

A CIC utility program that reads log files and snippets.

Trunk

A trunk is a communications line that connects two switching systems, such as the equipment in a telephone company's central office, and the PBX in a company.

User Queue

A queue where interactions (such as calls and chat sessions) intended for an individual user are routed.

Web Services

Web Services integrate CIC with popular Web servers from vendors including Microsoft, Sun/iPlanet, IBM, Apache, and others to provide services such as text chat, and Web call-back request processing.

Wireless Services

The CIC subsystem that communicates with wireless PDAs such as Blackberry, Palm, and Pocket PC devices.