PureConnect®

2019 R3

Generated:

11-September-2019

Content last updated:

14-June-2019

See Change Log for summary of changes.

GENESYS™

# Log Retrieval Assistant Customer Site

## Technical Reference


### Abstract

This document covers how to install and configure Log Retrieval Assistant (LRA). LRA is a utility that helps customers and support personnel work together more effectively by allowing a support representative to retrieve trace logs and other information from a customer's CIC server.

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

# Table of Contents

# LRA Customer Site

Log Retrieval Assistant (LRA) is a utility that helps customers and support personnel work together more effectively by allowing a support representative to retrieve trace logs and other information from a customer's CIC server. LRA helps a CIC administrator set diagnostic trace levels for various CIC subsystems and to configure Dr. Watson settings on the CIC server.

LRA allows authorized support representatives to request segments of event logs, trace logs, and other data sources (such as the registry) where CIC subsystems have written log data. LRA then routes the information to an off-site support representative via the Internet. LRA sends notification messages to inform the requester and the customer about details of each transaction.

Customers may also push data to a support site, without waiting for a support representative to make a request. See Push transfer logs to a support domain.

## Organization of Material

This introduction explains how the log retrieval process works.

- LRA Configuration explains how to install and configure LRA on an existing CIC server.
- Administration explains how to perform common tasks, such as pushing transfer logs to a support organization.
- Change Log describes new features and changes by release.
- The Glossary defines special terms.

## Related Documentation

When LRA is installed on the CIC server that is used by a support organization, that server is called the Support Site. When LRA is installed on the CIC server that is used by a customer, this server is referred to as the Customer Site. Separate documentation is available for each audience:

- *LRA Customer Site Technical Reference* (this document) is for CIC customers.
- *LRA Support Site Technical Reference* is distributed to support organizations.

These documents can be downloaded from the PureConnect Documentation Library.

# Key features

LRA can set trace levels per topic, and Dr. Watson settings on a remote IC server. LRA retrieves various types of troubleshooting information from a customer's CIC server, including:

- CIC subsystem trace logs.
- Dr. Watson logs.
- Application and system event logs.
- Dump of CIC registry trees, or a portion thereof, including the main CIC tree or just the Directory Service portion.
- Dump of CIC file information, such as filename, time stamp, file size, file version, HotFix version, file attributes, and so on.
- Dump of a CIC server's manifest file, SysInfo for Dialogic and Aculab cards, or portions of a SIPEngine log.
- IC version information.
- Customer's LRA configuration.
- Phone logs.

For more information, see the following:

- LRA is compatible with many editions of CIC
- LRA is designed for busy server environments.
- LRA is highly configurable yet simple to use

## LRA is compatible with many editions of CIC

LRA is compatible with CIC 2016 R1 and some earlier versions, including IC 2.0, 2.2, 2.3, 2.4, 3.0, 4.0, and 2015 R1-R4. Instructions for installing LRA on releases of CIC before IC 2016 R1 are included in the version of this document shipped with those releases. This document is specific to the current release of CIC only. If you need to install LRA on an earlier edition of CIC, refer to the *LRA Customer Site Technical Reference* included with that release of CIC. You will find it in the version of the PureConnect Documentation Library that accompanied that release.

## LRA is designed for busy server environments.

Incoming log requests can be queued for processing at customer-suggested off-peak times. Customers can also set a "slowdown factor" that helps limit the amount of CPU and network bandwidth that LRA consumes. CPU-intensive processes such as snipping, zipping, FTP, etc. sleep intermittently to ensure that LRA does not degrade the overall performance of a busy IC server.

- For example, slowdown factor 1 allows LRA to run at normal speed.
- Slowdown factor 2 runs LRA at half normal speed so that it uses half the resources.
- Slowdown factor 3 runs LRA at one-third speed; slowdown factor 4 runs at one-fourth speed, and so on.

You can assign different slowdown factors to peak- and non-peak hours. For example, you might set the slowdown factor to 2 during business hours, and allow LRA to run at normal speed during non-peak hours.

LRA spawns software processes periodically. To further reduce its overhead on the system, it automatically limits its concurrent process instances to five instances. When a new instance of LRA is started, it looks at other running instances to see if any are malfunctioning and automatically terminates them.

# LRA is highly configurable yet simple to use

LRA provides an HTML-based GUI that is used to submit requests. When a customer configures LRA to allow a support organization to access remote logs, all information is zipped and encrypted prior to transmission across the wire.

LRA automatically maintains a database of customer configurations at each allowed support site. When a customer updates his LRA configuration, LRA mails pertinent configuration information to the support site, which is used to update the customer configuration database. This database makes it easy for support personnel to request logs. To make a request, the support associate only needs to know the name of the customer. LRA retrieves the information needed to generate and send request messages from the database. Support personnel do not have to keep track of these details, and the database is as up-to-date as the last configuration update. LRA does not store sensitive details of the customer's local configuration (such as firewall passwords) in its database.

- **HTML Forms**. Support representatives use an HTML form to select the customer, CIC server, and type of information that LRA should retrieve. LRA initiates requests by sending emails to mailboxes that are monitored by handlers.
- **Email Notifications**. HTML request forms generate a well-formed email message that is sent to the customer's LRA mail account. Handlers create request files from the appropriate emails, kick off server processes that process requests, extract requested data, and FTP data back to the requesting site's FTP server.

  The Customer Site version of LRA utilizes an email client (`Blat.exe`) that does not perform NT authentications. The Customer version uses a handler (`I3LRASendMail.ihd`) to send email messages.

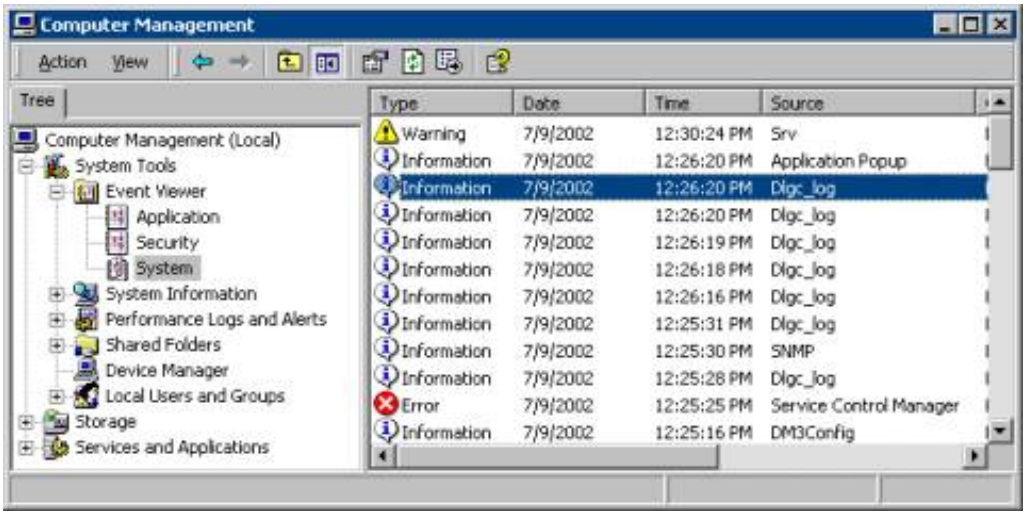
  Status and error emails are sent to the requesting support accounts and optionally to other configured parties. This keeps everyone informed of LRA usage and data that it has made available.
- **File Transfer is built-in**. FTP capability is built-in to LRA. Customers do not need to set up an FTP server. LRA works independently of existing FTP servers. LRA can FTP files from CIC servers that are behind firewalls.

  If a request cannot be processed for some reason, failed requests are retried a configurable number of times before LRA gives up on a transaction. LRA keeps track of each point of failure, and tries again at that point the next time, so that it does not repeat steps unnecessarily. For example, if the system goes down after LRA has zipped a file, but before it could FTP, it resumes at the FTP step.
- **Flexible Architecture**. LRA supports multiple requesting sites. A customer can optionally configure LRA to allow support representatives at reseller sites to make requests. By default, Genesys is the only organization that is authorized to submit LRA requests.

# Overview of CIC logging mechanisms

CIC uses two logging mechanisms:

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




   NT Event Logs are viewed using Microsoft Management Console.

2. Trace logs document the operation of various IC subsystems. This type of logging is more verbose. Most IC subsystems have a dedicated trace log. These logs contain information about error conditions, warnings, and data that helps indicate 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 IC subsystem.

   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.

   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.

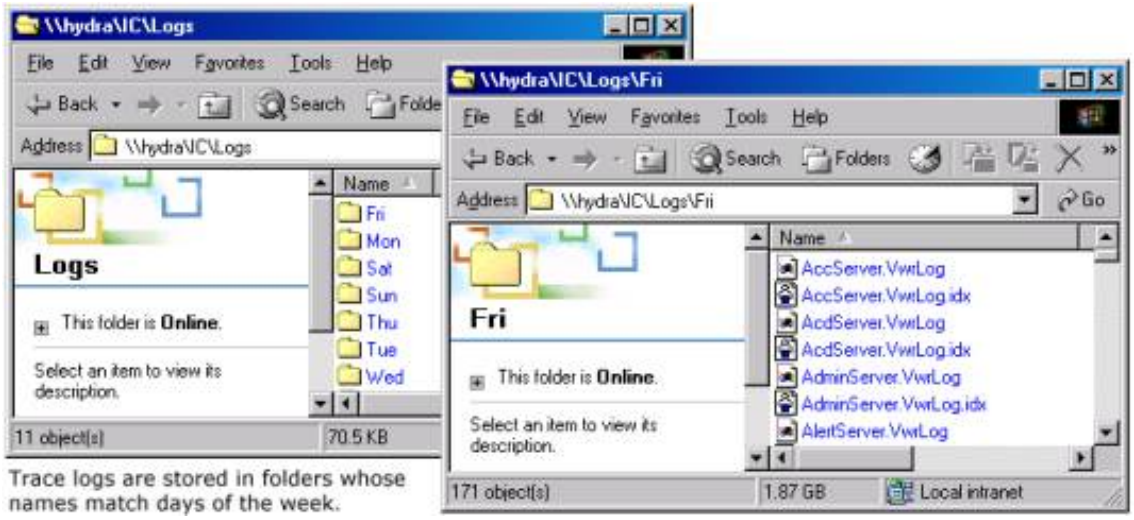
# Location of CIC Trace log files

In IC 2.x and later, trace log files are stored by default in `\i3\ic\logs`.

**Trace Log Folder and Filename Conventions**

The default location of the trace logs folder is configurable. You can change the trace log path using the IC System Manager utility. If a daily log file exceeds its size threshold, it is broken into separate log files within the folder for that day.

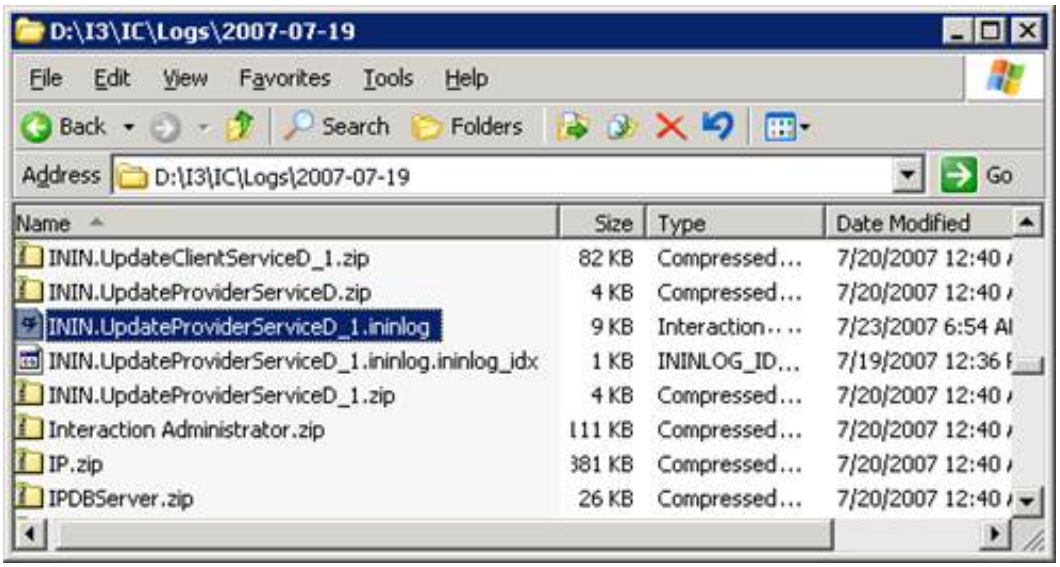
In releases prior to IC 3.0, trace logs were stored on the CIC server in folders named after days of the week, and log files are identified by a `.VwrLog` extension. Trace messages for each logged subsystem are stored in folders for a specific day of the week.




For example, on an IC 2.x system, Fax Server log messages on Friday might be written to:

`I3\IC\Logs\Fri\FaxServer.VwrLog`

In IC 3.0 and later, trace logs are not stored in folders named after the day of the week. Instead, log folders are named using the current date, in the form `YYYY-MM-DD`. LRA is able to navigate these directories to find the target files for snipping and zipping.



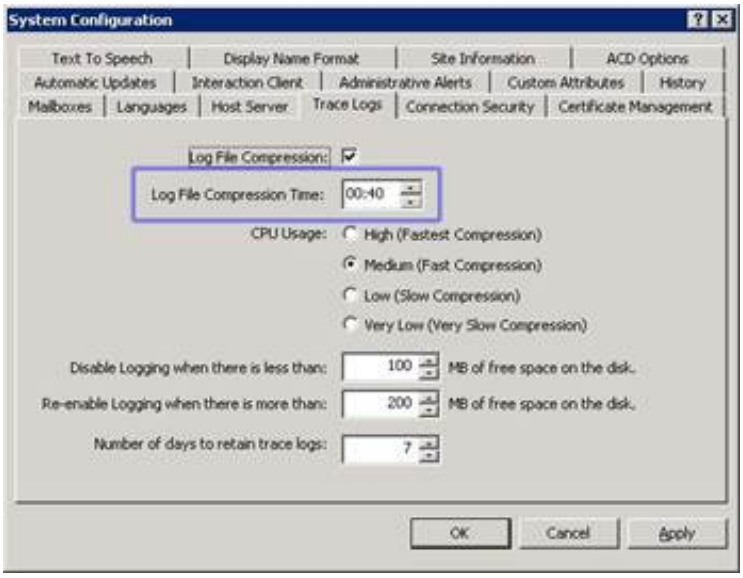

In the example above, Windows Explorer is displaying a list of log files in a log folder named 2007-07-19. File extensions for IC 3.0 and later include the following:

- The `.ininlog` extension identifies a trace log file.
- The `.ininlog.ininlog_idx` identifies the index file of a trace log.
- Log files are automatically compressed into zip archives. LRA automatically unzips compressed files when it needs to access log files in an archive.
- IC trace logs are stored in the Logs share on the server. The physical path is `i3ICLogs`.
- Phone logs are named using the phone's MAC Address. Logs are created when a phone is rebooted.

# Automatic Log File Compression

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, do the following:

1. Open Interaction Administrator and select the **System Configuration** container.
2. Double-click the **Configuration** entry.
3. When the **System Configuration dialog** appears, click the **Trace Logs** tab.
4. Change the **Log File Compression Time**.
5. Click **OK**.

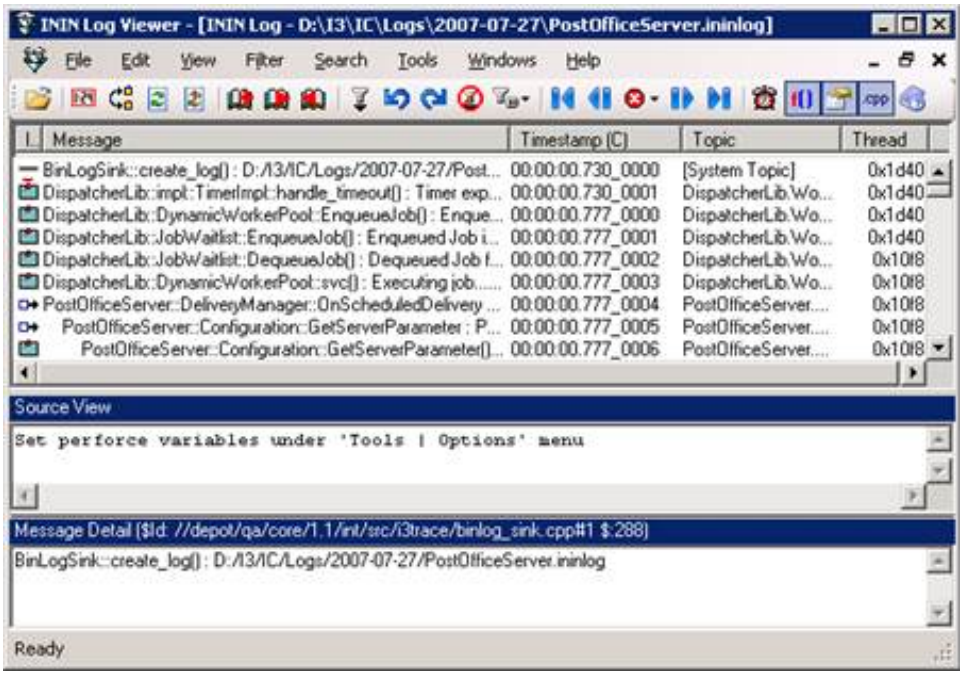


# Log Viewers

CIC provides two utilities that help manage trace files: Log Viewer and Trace Config. The first utility displays selected portions of log files. The second controls the degree of detail logged by each CIC subsystem.

You can start the Log Viewer and Trace Config utilities by navigating to the Genesys programs folder at **Start** > **All Programs** > **Genesys**.

Log Viewer reads trace logs and log snips. This powerful tool searches for literal strings in log files, finds log entries that occurred at a specific time, locates specific types of log entries, manages bookmarks, color codes entries, and filters logs to include only entries of interest. It also allows an administrator to view multiple logs and synchronize log entries. To use LRA, you do not need to use Log Viewer or Trace Viewer, but these are valuable system tools.



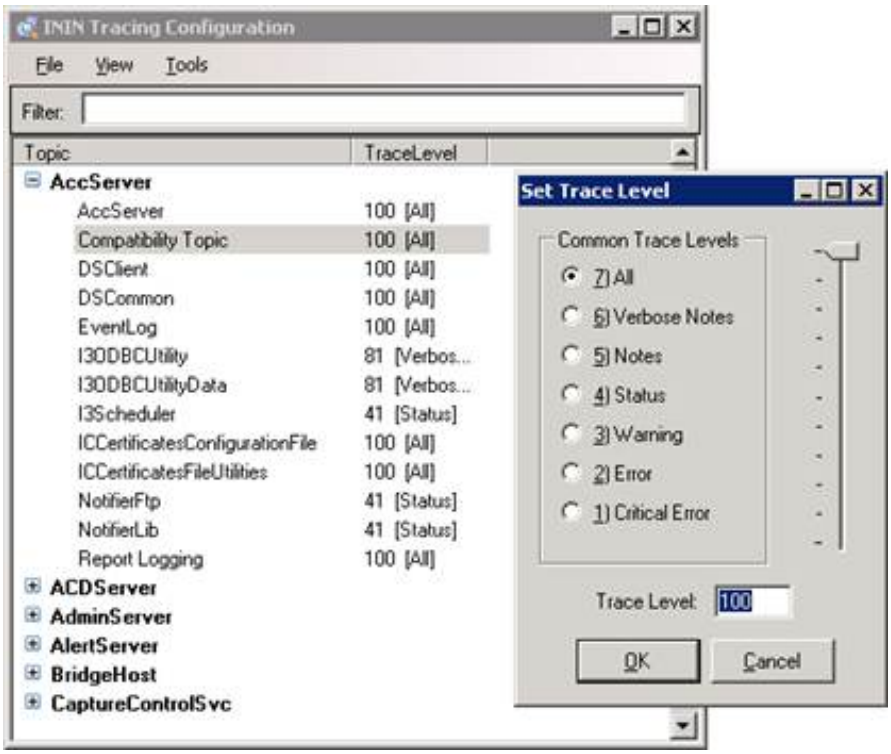

For more information, see the following:

- The Trace Configuration Utility
- Other Utilities: IC Trace and LogSnipper

## The Trace Configuration Utility

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

The Trace Configuration Utility:

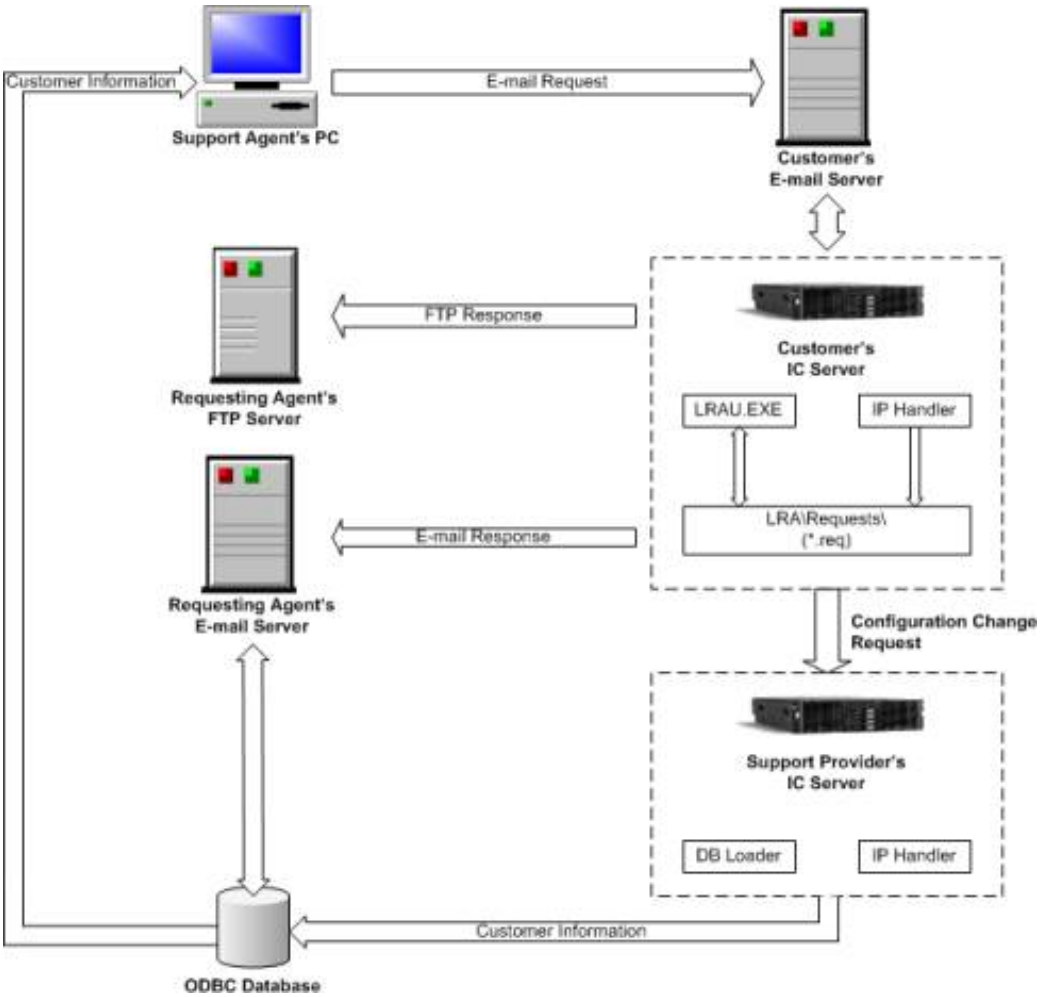



## Other Utilities: IC Trace and LogSnipper

Two other utilities deserve brief mention. IC Trace (`ICTraceA.exe`) is a command-line version of the Trace Configuration utility. Log Snipper is a command-line utility that can be used to snip segments of log files. However, LRA eliminates the need to manually snip segments of log files. The executable name of the Log Snipper utility varies between releases of CIC:

| IC Version | File Name |
|---|---|
| IC 3.0 and later | This utility is provided in two forms:<br>1. `logsnip.exe` is always the most current version.<br>2. An executable whose name contains version information. For example: `\I3\IC\ININ Trace Initialization\logsnip-w32r-1-1.exe`. |

# How the LRA process works




1. Customer fills out and submits an LRA Configuration form. Information about the customer is added to or updated in the database. To accomplish this, a handler named `I3LRAAdminIncomingMailMessage` on the support provider's IC server monitors the LRA monitored mailbox. When an incoming update request message is received, it invokes a process named `I3LRADBLoaderU.exe` to update database tables that store information about LRA customers and configurations.
2. A support associate or customer fills out a HTML-based LRA request form. When the form is submitted, client-side code in the HTML page composes a formatted email message.
3. The next step depends upon the version of CIC used. In releases before IC 2.3, a script in the HTML page calls a COM DLL named `I3LRAMgrU.DLL` to send the email message to the customer's Monitored Mailbox 0. This is the Email account associated with the CIC administrator. In IC 2.3 and later, monitored mailbox 0 can be associated with any email account using the LRA plug-in for Interaction Administrator. However, customers are strongly encouraged to dedicate this mailbox for LRA's exclusive use.
4. When the message arrives at the customer's CIC server, a handler named `I3LRAMonitorMailbox` fires.
5. If a server parameter named `LRADomains` exists, the handler checks to see if the Email originated from a domain listed in `LRADomains`. If the Email message did not originate from a known domain, the handler terminates. If `LRADomains` does not exist, no domain checking is performed.
6. Next, the handler looks at the subject of the email message to ensure that it is formatted as follows:

   `I3LRARequest|[`*`IC_Servername`*`]|[now|deferred]`

   The subject must begin with `I3LRARequest` to indicate that it is an LRA request message. If the subject of the message is invalid, the handler terminates.

   *`IC_Servername`* is the name of the server that the handler is executing on. The third parameter controls whether the request is processed immediate or is deferred:

   - `now` indicates that the request should be processed immediately.
   - `deferred` indicates that the request should be processed at a later time, specified in LRA's configuration.

   The only messages that LRA deletes from the customer's mailbox are request messages that LRA has recognized and processed. LRA does not delete messages that it does not recognize.

7. Once the message has been validated, the `I3LRAMonitorMailbox` handler creates an LRA request message in the `I3ICServerLRARequests` folder. If the message is marked for immediate action, the handler runs `I3LRAU.exe` to process the request. The filename of the request message is `I3LRARequest_YYYYMMDDHHMMSS.REQ`. The request name is unique, since it is based upon the current date and time.
8. Every 15 minutes, a handler named `I3LRATimerInitiator` starts a server process named `I3LRAU.EXE` to process pending request files.
9. At startup, `I3LRAU` looks in the requests directory for unprocessed requests. It also checks for other running instances of itself (up to 5) to see if any of them have been active for more than 20 minutes. If an instance is not making progress, and has persisted for more than 20 minutes, it is terminated.
10. If request files are present, `I3LRAU` reads each file to find out what data it should extract. It retrieves the requested data and stages it in the *working directory* inside one or more encrypted `.zip` files. If the Autosend configuration parameter is checked, `I3LRAU` initiates an FTP file transfer to transmit files to the requester's FTP directory.
11. `I3LRAU` sends an email message to the requestor to notify that it is processing the request, or that it cannot process the request due to server down condition, invalid FTP configuration, FTP file transfer error, etc.
12. If the request was for an installation, configuration, trace level, or Dr. Watson-related change, LRA sends an update request email message to the requester's CIC server.
13. When all FTP transfers for a request are complete, `I3LRAU` sends an email notification to the requestor. This message indicates that the file transfer is complete and also specifies the directory where files were uploaded.
14. `I3LRAU` deletes the processed request from the requests directory, and deletes processed `.zip` files from the working directory. It then repeats steps 9-11 until it has processed all remaining request files. `I3LRAU` terminates when there are no additional files left to process.

## Format of a Log Request E-mail

The payload of log request emails is plain text that summarizes the value of fields on the Log Request form. Requests are normally deleted as they are processed by the server. Customers don't need to worry about the format of these messages, but here is an example:

```
From: Tippecanoe_user
Sent: Monday, July 23, 2017 6:10 PM
To: Doe, John
Subject: LRA Status (I3LRARequest_20070723180943.P6100)
Processing request:
--------------------
ObjType: Request
DeferTime: Now
RegistryDS: False
EndTime: 5:00 PM
Server: TIPPECANOE
ErrorEmail: john.doe@inin.com
ICFiles: True
DestDir: \upload
LogFile: AlertServer
StatusEmail: john.doe@inin.com
RegistryPT: False
InstallLogs: False
YearMonthDay: 2017-07-23
Requestor: john.doe@inin.com
EventLogs: False
Customer: Tippecanoe
DrWatson: False
Retries: 3
VersionInfo: False
Weekday:
Slowdown: 3
PhoneFiles: ALL
PackIndiv: False
RegistryIC: False
Defer: False
DestSite: I3
ReqDate: 20170723180943
BeginTime: 8:00 AM
```

# Format of Configuration Request E-mail

Here is a sample of the email that would be sent to the support server when the customer server would have its LRA configuration changed.

```
From: Tippecanoe_user
Sent: Monday, July 23, 2017 6:06 PM
To: Doe, John
Subject: LRA Update (I3LRARequest_20170723180053.P1672)
Customer: Tippecanoe
Server: TIPPECANOE
LRAVersion: 2.0
ProductVersion: 3.0.0
--------------------
Trace settings:
--------------------
Trace settings are now retrieved with log requests...
--------------------
Dr. Watson settings:
--------------------
ObjType: Watson
DumpAllThreads: True
Server: TIPPECANOE
LogFilePath: D:\I3\IC\Logs\DrWatson\
SoundNotification: False
Instructions: 20
VisualNotification: False
AppendToLogFile: True
CrashDumpFile: D:\I3\IC\Logs\DrWatson\user.dmp
CreateCrashDump: True
MaximumCrashes: 10
ReqDate: 20170723180554
DumpSymbols: True
--------------------
LRA Configuration:
--------------------
ObjType: Config
CustName: Tippecanoe
WorkDir: D:\I3\IC\Logs
OPBegin: 23:00
OPEnd: 05:00
StdSlowdown: 3
OPSlowdown: 1
MonitoredEmail: tippecanoe_user@dev2000.com
PassiveMode: True
Autosend: False
Defer: False
DestSite: I3
FTPServer: ftp.inin.com
LRAClientMailbox: john.doe@inin.com
Autoupdate: true
```

# Security considerations

Security should always be considered when data is transmitted to another organization.

## Sensitive data in log files

Log files can contain sensitive data. For example, an IP log might contain PIN numbers or account information. Care should be taken by all parties to protect the confidentiality of log information. At this time, LRA cannot be configured to restrict remote access to particular logs. This may be added in a future release. However, the support personnel who examine logs have your company's best interests at heart. LRA merely automates sharing of information that is routinely exchanged between customers and support groups.

## LRA can be configured to process requests only from known domains

By default, LRA processes Email requests that it receives from any domain. LRA can be configured to process only those email requests that it receives from specific domains, such as ININ.com or the domain of a trusted reseller. To restrict processing to specific domains, create a server parameter named LRADomains whose value is a semicolon-separated list of domains that that LRA should process. Here's how to do it:

1. Run Interaction Administrator.
2. Create a server parameter called `LRADomains`.
3. For its value, enter a semicolon-separated list of domains that are eligible to request logs through LRA. LRA will process requests only from domains in this list. For example, to restrict processing to requests from Genesys and reseller whose domain is acme.com, the value of the `LRADomains` parameter would be: genesys.com;acme.com.

If you delete the `LRADomains` server parameter, LRA will process requests from all domains. If you un-manage the handler that LRA uses to process requests (`I3LRAMonitorMailbox`), LRA will not process requests from any domain. However, you can explicitly push data to a specific domain. See Push transfer logs to a support domain.

## Sensitive information in the configuration file

LRA saves the UserId and Password used by its FTP process to navigate a firewall in the local configuration file. This information is stored as clear text, to be used locally by the `I3LRAU` process.

Password information never leaves the customer's server and it is not stored in the master configuration database. However, the possibility exists that a CIC user might navigate to the `i3icserverLRA` directory to read sensitive information from the configuration file.

Your network administrator can eliminate this vulnerability by restricting access to the LRA directory to master administrator account used by the CIC server and its processes.

## Log data is encrypted prior to transmittal over the wire

LRA compresses and encrypts log files to create `.zip` files. If a third party somehow intercepts a file, the illicit party could view the names of log files in the archive, but could not access its contents, since the file is password-protected.

## SMTP/Email considerations

If the SMTP address of the account associated with monitored mailbox 0 is not visible to the outside world, LRA will not function properly. Customers must take steps to obtain a visible SMTP address (e.g. by creating a contact that forwards LRA Emails, or by setting up a sub-domain that is visible outside of the local network). It is the customer's responsibility to resolve this rare situation.

# LRA Configuration

The method used to configure LRA on a customer site depends upon the version of CIC. In IC 2.3 and later, LRA is installed as part of the **IC Server install** and it is configured using **Setup Assistant** and **Interaction Administrator**. In earlier releases of CIC, a hot fix installed LRA components, and LRA was configured using HTML forms.

The procedures in this document apply to CIC 2015 R1 and up platforms. LRA components are installed automatically by the IC Server install.

> LRA must also be configured on the CIC server used by the support organization, but that is the responsibility of the support organization.

To put LRA into operation, complete these tasks:

- Optionally configure LRA Mailbox settings in Setup Assistant
- Configure LRA containers in Interaction Administrator

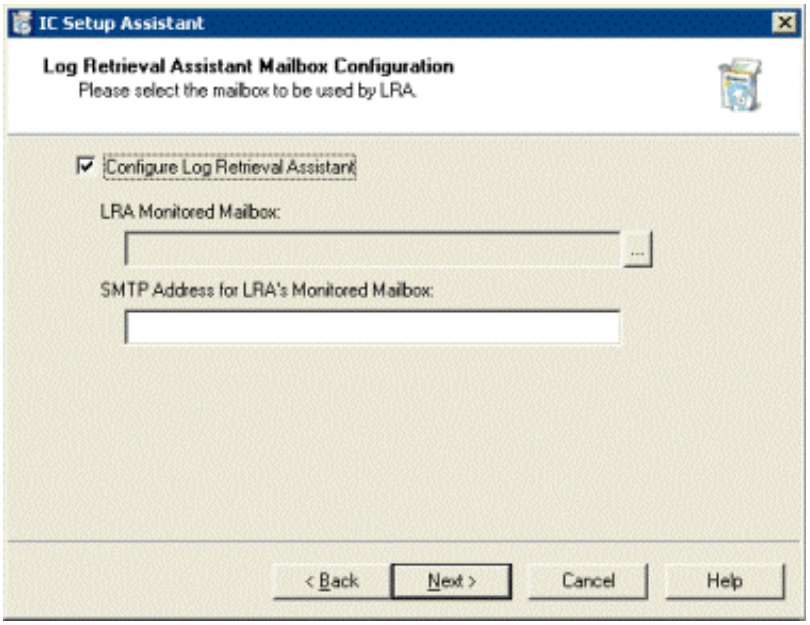
# Optionally configure LRA Mailbox settings in Setup Assistant

To put LRA into operation quickly, an Administrator can optionally configure LRA Mailbox settings in **Setup Assistant** to identify the mailbox that LRA will monitor to pick up requests. Once mailbox settings are defined, LRA will run "out of the box" using default parameters. However, the Administrator must activate LRA by opening the LRA container once in Interaction Administrator, and selecting the **OK** button to send an update request.

The procedure below explains how to perform these tasks in **Setup Assistant**. If mail-related settings are not configured in Setup Assistant, you can configure LRA later in Interaction Administrator. See Configure LRA containers in Interaction Administrator.

To configure LRA Mailbox settings in Setup Assistant:

1. Start **Setup Assistant**. A page in Setup Assistant named **Log Retrieval Assistant Mailbox Configuration** prompts for information about the mailbox that LRA will monitor to pick up requests.
2. In Setup Assistant, navigate to the **Log Retrieval Assistant Mailbox Configuration** page. Place a checkmark next to **Configure Log Retrieval Assistant**. This option allows an administrator to configure mailbox settings so that LRA can operate in accordance with default options.




   If settings on this dialog were preconfigured by the IC Survey file, those settings will appear as default values when this dialog is opened. You can review the contents of an IC Survey file by selecting **View Survey** in the **Load IC Survey File** dialog or opening it in a Pre-Install survey in the IC Survey system.
3. The **LRA Monitored Mailbox** field prompts for the mailbox that will be used as the LRA Monitored Mailbox. This is the Email account on the customer site that Log Retrieval Assistant should monitor to pick up requests.
4. Click the button on the right (**...**) to open the **Mailbox Selection dialog**. Depending on the mailbox option (for example, mail server directory or Voice Mail only), you may need to provide the **Name**, **Display Name**, **Address**, **Directory**, **Message Store**, and/or other information. Refer to *Interaction Administrator Help* for help with the Mailbox Selection dialog. Customers are strongly encouraged to dedicate this mailbox for LRA's exclusive use.
5. Type the SMTP address of LRA's monitored mailbox in the **SMTP Address** field. For example, you might enter `someplace@somewhere.com`.
6. Select **Next** to configure other Setup Assistant pages. When Setup Assistant ends, you can begin using LRA after activating it in the next step.
7. But first you must activate LRA by opening the **LRA** container once in *Interaction Administrator*. Then select ***OK*** to send an update request.

# Configure LRA containers in Interaction Administrator

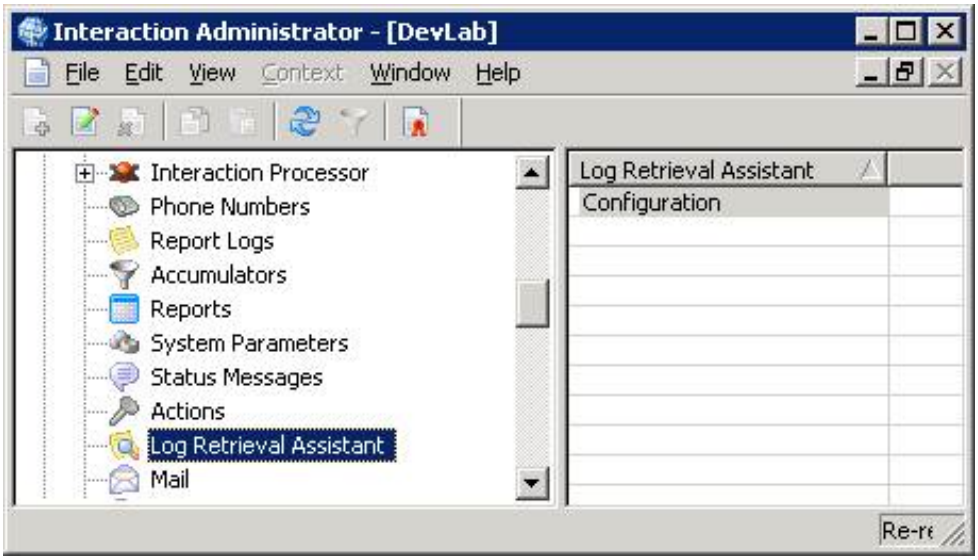
This procedure explains how to configure LRA so that a support representative can request or retrieve information from your CIC customer site. LRA must also be configured on the CIC server used by the support organization. However, you do not need to configure the support site server. That is the responsibility of the support site.

The process of configuring LRA publishes information about your CIC server to an LRA database at your support organization. This database stores information needed to perform file transfers and send email messages. It does not store passwords or other potentially sensitive information.

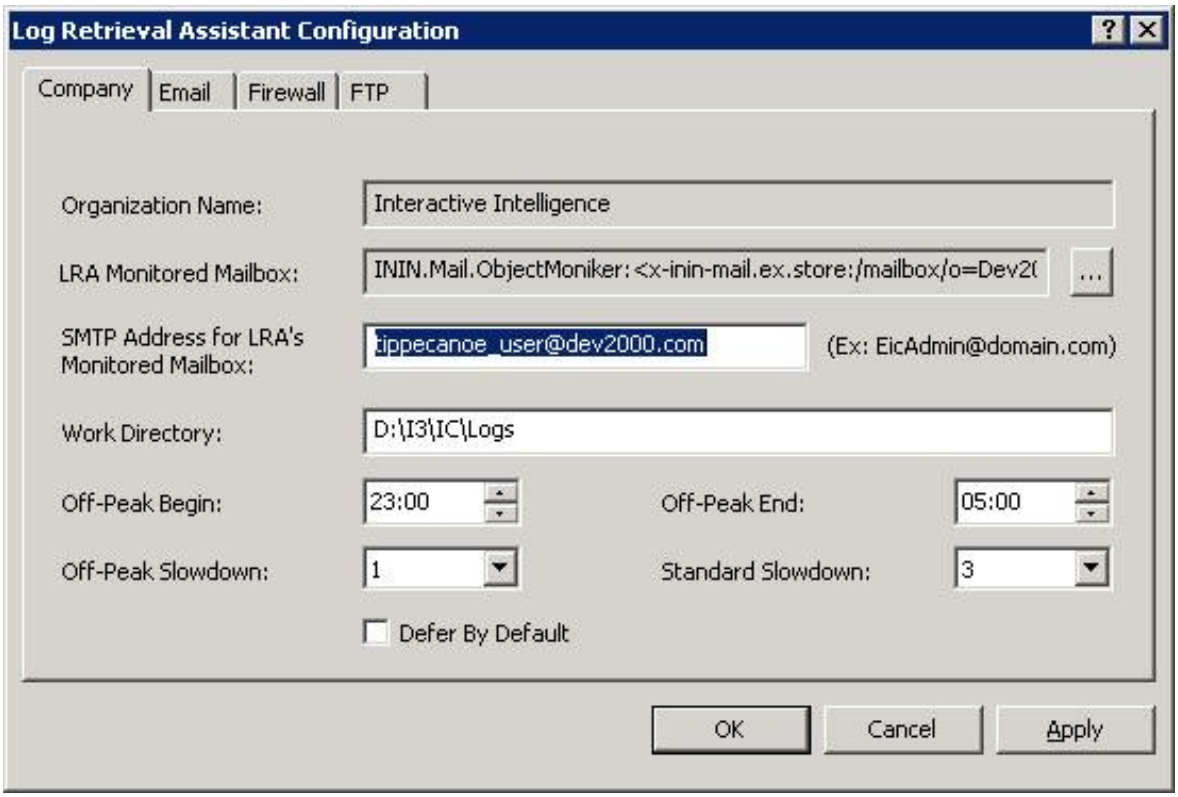
You need only configure LRA once, unless some aspect of your site configuration needs to be changed. For example, you might wish to change the email account used to receive status messages.

LRA is configured using a **Log Retrieval Assistant container** in Interaction Administrator. This container is a child of the **System Configuration** container. It manages company, mailbox, Email, firewall, and FTP settings. It mimics the HTML-based **Customer Configuration** form used to configure previous releases of LRA. You can optionally use the HTML page to configure these settings.

1. Start Interaction Administrator and expand the **System Configuration** container.
2. Select the **Log Retrieval Assistant** container.




3. Double-click the **Configuration** entry to open the **Log Retrieval Assistant Configuration** property page. Set options on the **Company** tab as follows:

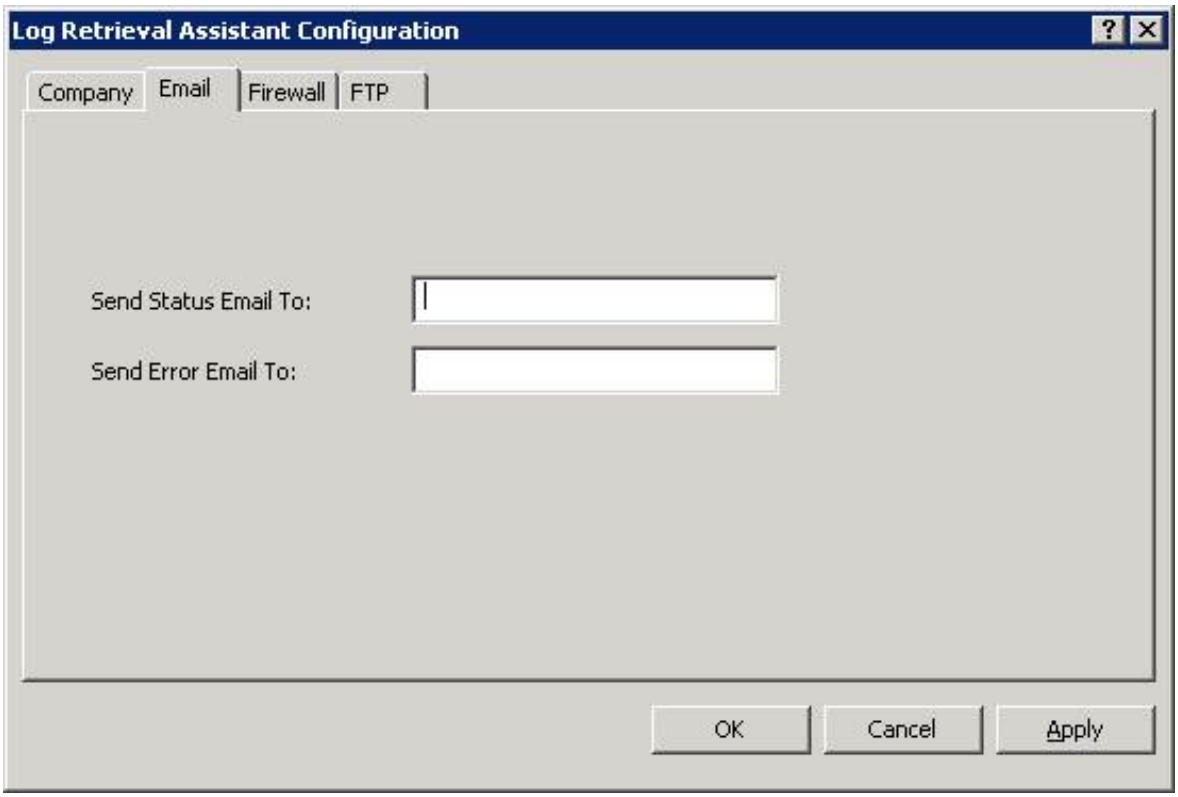



4. The **Organization Name** field is read-only. This name identifies your organization in the master database and in Emails sent by LRA at your site. The name displayed in this field is the value found in the configuration of the **System Configuration** node, under the **Site Information** tab.
5. **LRA Monitored Mailbox** identifies the Email account on the customer site that LRA will monitor to pick up requests. Use the browse button (**...**) to select an account. Support representatives mail log requests to this account for processing by LRA. A dedicated mailbox is strongly recommended. This field sets monitored mailbox 0 (used by the post office and handler initiator) to the value you select.

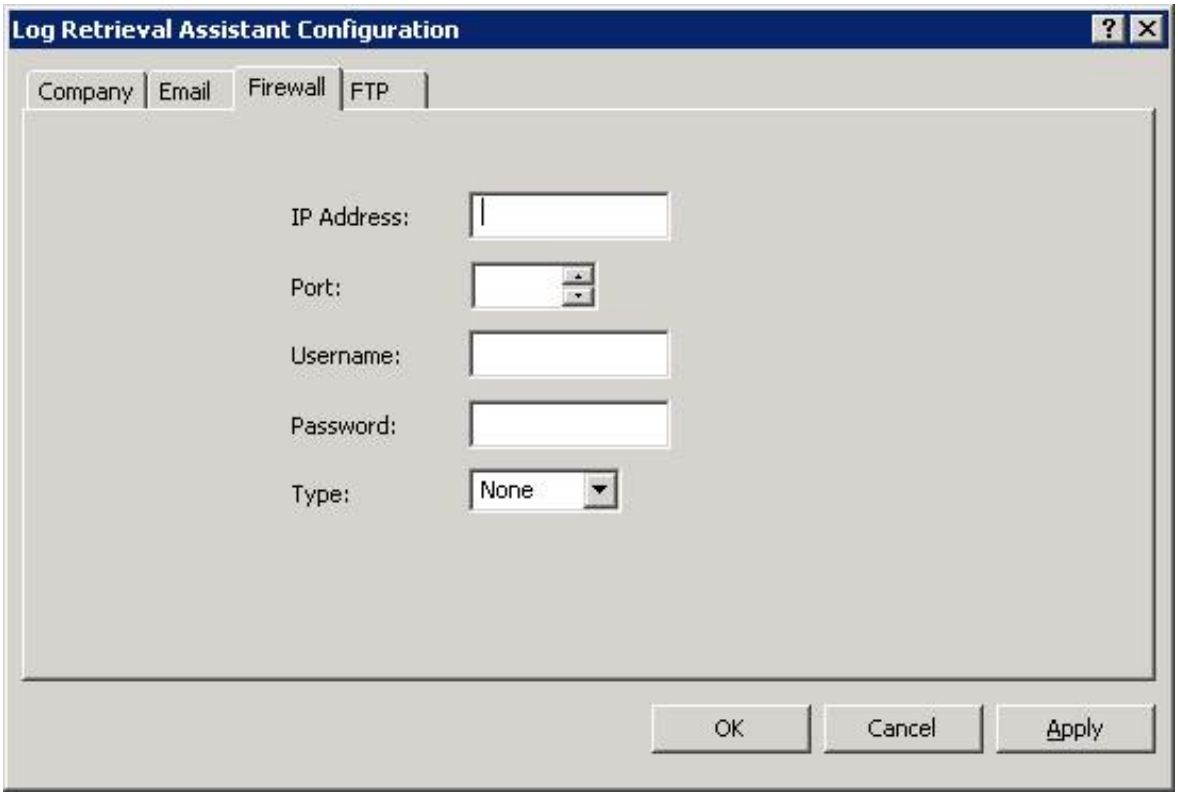
6. Type the SMTP address of the LRA Monitored mailbox in the SMTP Address for LRA's Monitored Mailbox field (e.g. `account@domain.com`). The is the address where configuration updates will be sent.
7. Complete the **Work Directory** field by typing the fully qualified path to a working directory where log files are compressed (zipped) prior to FTP transfer. If for some reason the FTP process fails, log files will persist in this location until a subsequent FTP attempt is successful (or until files are manually deleted). The I3 logs directory is used by default.
8. Use the spin controls to specify **Off-Peak Begin** and **End** times in 24-hour format. These fields indicate a block of time when the customers IC server is not at peak utilization. Deferred log retrieval requests are executed during this period to minimize impact on the server.
9. Use the **Off-Peak** and **Standard Slowdown** list boxes to select a value between 1 and 20. These *slowdown factors* limit the amount of CPU and network bandwidth that LRA can consume. Higher values force CPU-intensive processes such as snipping, zipping, FTP, etc. to sleep intermittently so that LRA does not degrade the overall performance of the CIC system.

   LRA runs at normal speed when the slowdown factor is 1. It runs at half speed (and consumes half the resources) when the slowdown factor is 2. A factor of 4 means LRA is operating at one-quarter speed with a corresponding decrease in system resources used. This factor applies to requests processed during normal hours and must be between 1 and 100.

   Different slowdown factors can be set for peak-time and non-peak times. For example, you might set the slowdown factor to 2 during business hours, and allow LRA to run at normal speed during non-peak hours.
10. To defer processing of all LRA requests until off-peak hours, check **Defer By Default**. In an emergency, support personnel can override this setting on a per-request basis, meaning that they can flag a request to be processed immediately.
11. Click on the **Email** tab. This page configures email settings for LRA.




12. Complete the **Send Status Email To** field by entering an Email address.LRA optionally sends status emails to the email addresses in this field when jobs start and finish. Leave this field blank if you do not want to receive status emails.
13. Complete the **Send Error Email To** field by entering an email address. In the event that an unrecoverable error occurs, LRA will send an error notification message to the email account identified in this field. Leave this field blank if you do not want to receive error notification emails.
14. Contact your local network administrator to find out if your CIC server is behind a firewall. If it is, you must specify additional information that allows outbound payloads and data to pass through the firewall. Click the **Firewall** tab.




15. To complete the fields on this page, you may need to obtain help from your local network administrator.

**IP Address**

**IP Address** is the host name (or IP address) of the firewall.

**Port**

This number identifies the port used by FTP to pass data through firewalls. Contact your local network administrator to find out which port on the firewall is opened to FTP traffic.

**Username**

This field stores the User Id needed to pass data through the firewall. It is likely that you will need to contact your local network administrator to obtain this information.

**Password**

This field stores the password for the **Username** specified above.

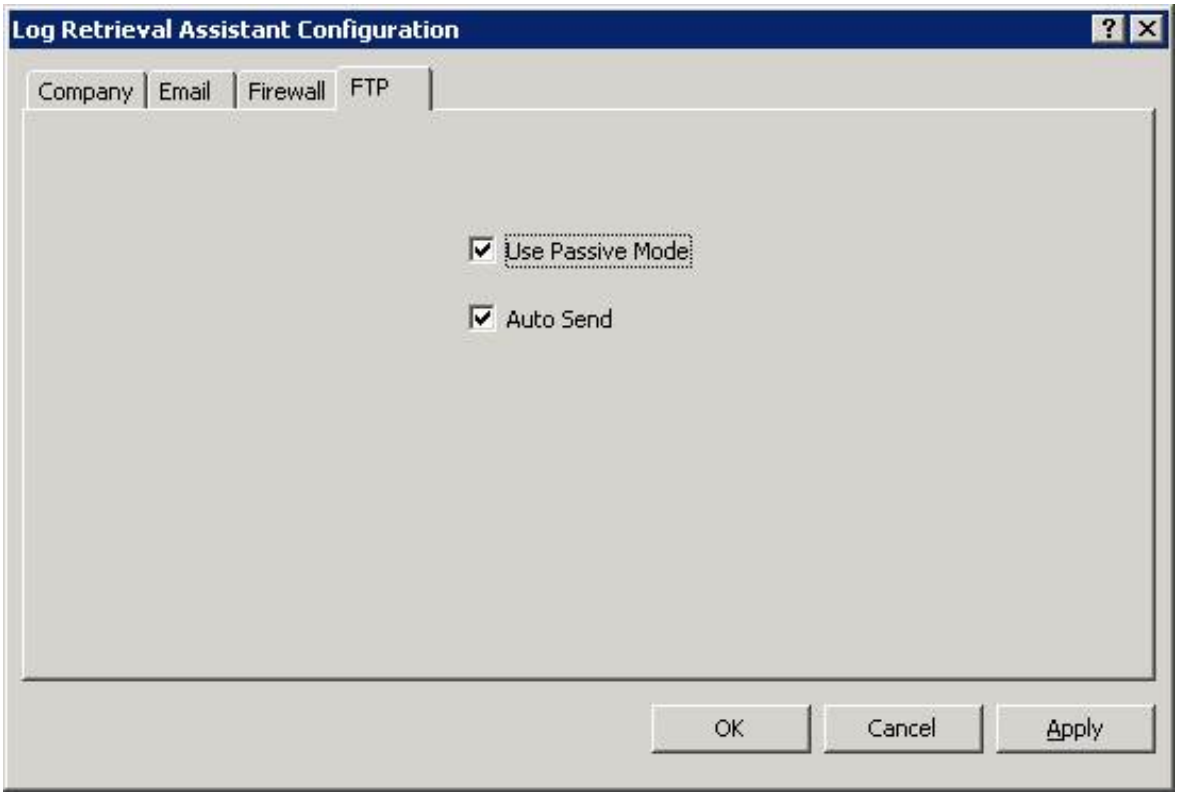
**Type**

This field identifies the type of firewall used. The choices are **None**, **Socks4** or **Socks5**. **Socks4** is a protocol that relays TCP sessions at a firewall host to allow application users transparent access across the firewall.

**Socks5** does the same thing, except that it also resolves issues that **Socks4** does not fully address or omitted. **Socks5** provides strong authentication, authentication method negotiation, address resolution proxy, and other features.

Sensitive information about your firewall, such as ID and password information, is never transmitted to a remote server or passed to a remote database. LRA uses firewall configuration information to transmit outbound data through the firewall. The firewall Id and password is stored locally in a configuration (`.cfg`) file in the `serverLRA` directory so that LRA can retrieve it. If this poses an unacceptable security risk, you should deny user access to the `serverLRA` folder.

16. To enable or disable FTP configuration settings used by LRA, click on the FTP tab:




**Use Passive Mode**

This checkbox determines whether FTP operations will be performed in passive or active FTP mode. Passive mode allows FTP operations to pass data through certain types of firewalls that would not otherwise allow the flow of data.

This option should be checked unless a PureConnect Customer Care representative requests otherwise. It affects the way the data connection (the socket on which the files and folder listings are transferred) is initiated.

When this option is checked (default), the LRA process (`I3LRAU.exe`) will initiate the data connection to the FTP server. This behavior is more firewall-friendly and has a greater chance of succeeding.

When this option is not checked, the LRA process (`I3LRAU.exe`) will listen for a data connection from the FTP server. Most firewalls do NOT allow connections to be initiated from the outside, and therefore may cause the FTP operation to fail.

**Auto Send**

This check box determines whether requested data is automatically FTP'd from the customer site to the requestor's FTP site. When checked, the I3LRAU server process FTP's `.zip` files as soon as it finishes staging them in the working directory. When this option is unchecked, `.zip` files remain in the working directory until they are manually FTP'd to the requestor by the customer. As a rule of thumb, you should leave this option checked unless you wish to inhibit all LRA-related file transfers for some reason.

When **Auto Send** is unchecked, LRA extracts logs and zips them, but does not do anything else. Customers must use an Internet FTP utility (e.g. WSFTP or equivalent) to manually transfer `.zip` files to the support site.

17. Click **OK** to apply changes and close the dialog. LRA is now configured and is ready to use.

**Related Topics**

Optionally configure LRA Mailbox settings in Setup Assistant

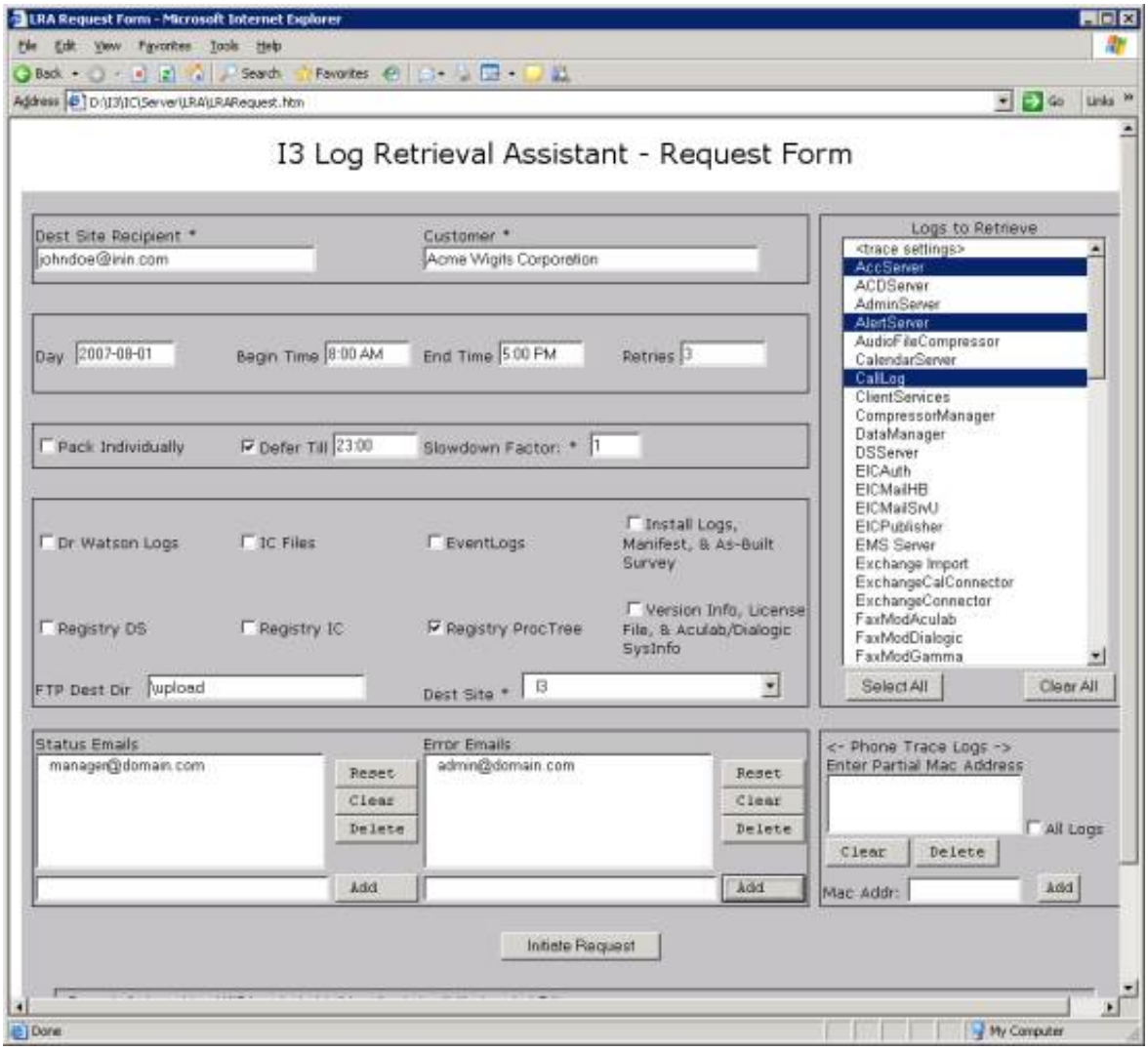
# Administration

If the CIC server goes down, LRA can still be used to provide information to a support organization. Customers must manually initiate requests to push log data to the support domain, using the `LRARequest.htm` form. (See Push transfer logs to a support domain.) Trace levels cannot be adjusted when the CIC server is down, and no email processing will occur. The related topics are:

- Push transfer logs to a support domain
- Fields on the Customer Request Form
- How to change the E-mail address of the support site

## Push transfer logs to a support domain

This procedure explains how to push a log file to a support agent if CIC is down, or without waiting for an agent to make a request. Customers may push logs to a support representative by selecting Transfer Logs from LRA's main menu. This opens `LRARequest.htm`—the **Log Retrieval Assistant Request Form**. Use this form to transfer data to a support representative, without waiting for the representative to make an LRA request. This technique is also useful when the CIC server is down (and is consequently not processing log request emails).




The **Log Retrieval Assistant Request Form** appears when **Transfer Logs** is selected from the main menu.

Follow these steps to submit a manual support request:

1. If you have not done so already, open the request form by selecting **Transfer Logs** from the **Main Menu**.
2. Fill in form fields as needed. The **Dest Site Recipient** and **Dest Site** fields must contain values when the form is submitted. Otherwise an error will occur. See Fields on the Customer Request Form for information about fields on this screen.
3. Review your selections before submitting the form. In particular, you should check the contents of the **FTP Dest Dir** field, to ensure that it contains the name of a valid destination directory. Your support representative can supply this information. Also

check to make sure that the appropriate log files are selected.

4. Select **Submit** to initiate the request. When the request is processed, `I3LRAU.exe` will zip and FTP files to the remote directory. An alert box appears to tell you that the request is being processed.


5. Select **OK** to dismiss this dialog. Control will return to the main menu (`LRAMain.htm`).

## Fields on the Customer Request Form

The **Customer Request form** (`LRARequest.htm`) contains the fields listed below. An asterisk identifies required fields.

**Requester**

This field prompts for the name of the log recipient.

**Customer *[server]** list box**

This read-only field is automatically populated with **Company Name** data, read from the customer's local configuration file.

**Day**

Allows entry of a day of the week for which data should be retrieved. In IC 3.0 and later, the date format is `yyyy-mm-dd`. In releases of IC before 3.0, the day of the week is specified (Monday, Tuesday, etc.)

**Begin Time**

This field sets the start time of log data selected. Time can be entered using 24-hour notation, or has `hh:mm:ss AM|PM`. For example, 1:30 pm could be entered as 13:30, or as 1:30 PM.

**End Time**

This field sets the end time of log data retrieved.

**Retries**

This field sets the total number of attempts that the system will make to recover from an error. This applies to all LRA operations, including zipping and file transfer.

**Pack Individually**

Check this option to package each file into a separate zip file. LRA may decide to pack and send files individually if the system is low on disk space.

**Defer Till**

When this field is checked, the request will be deferred until the **Off-Peak Begin Time** (defined in the customer's configuration). If this field is not checked, the request is processed immediately.

**Slowdown Factor***

This value displays the throttling factor associated with the current time, or the deferred time. When **Defer Till** is checked, the showdown factor for non-peak times is displayed. When **Defer Till** is unchecked, the field displays the slowdown factor for peak times, as is defined in the customer's configuration record.

**Dr Watson Logs**

This checkbox indicates whether the request will retrieve a Dr. Watson Log and a crash dump file if one exists.

**IC Files**

This checkbox indicates whether a dump of CIC file information should be retrieved. This provides information about critical CIC files, such as file name, time stamp, file size, CRC, etc. This option can take significant time to complete, especially if a slowdown is in effect.

**EventLogs**

Indicates whether application and system Event Logs are selected by the request.

**Install Logs, Manifest, & As-Built Survey**

This option provides the CIC server manifest, installation logs, and survey log.

**Registry DS**

Indicates whether the request should select the Directory Services tree from the registry.

**Registry IC**

Indicates whether the request should select the entire CIC tree from the registry.

**Registry ProcTree**

Indicates whether the request should select the Process Tree from the registry.

**Version Info, License File, & Aculab/Dialog Sys Info**

Indicates whether the request should retrieve a text file that contains information about all Hot Fixes applied to the CIC server, licenses, and telephony firmware SysInfo reports.

**FTP Dest Dir**

Enter the name of the destination FTP directory at the support site. The default directory is `upload`, but you should change this to the name of an actual directory that a support representative has given you.

**Status Emails**

This field is pre-populated with Email accounts read from the customer's configuration file. Status messages are sent to recipients listed in this field.

**Error Emails**

This field is pre-populated with Email accounts read from the customer's configuration file. Error messages are sent to recipients listed in this field.

**Phone Trace Logs**

The options in this section of the form retrieve telephone logs. The log for a particular phone is identified by its MAC address.

> A Media Access Control address (MAC address) is a unique identification code assigned to a hardware device, such as an IP phone.

**Mac Addr**

This field accepts full or partial entry of a phone's Mac address, to retrieve corresponding phone logs. After typing an address in this field, select the **Add** button. If you do not know the Mac addresses of phone devices, check the **All Logs** checkbox to retrieve all phone logs.

**All Logs**

Retrieves all available phone logs, without the need to specify Mac addresses.

**Clear**

Removes all Mac Address entries from the list.

**Delete**

Deletes the selected Mac address from the list.

**Reset**

Refreshes the contents of a **Status Emails** or **Error Emails** field, using data read from the local configuration file.

**Clear**

Clears the entire contents of a **Status Emails** or **Error Emails** field.

**Delete**

Removes selected recipients from a **Status Emails** or **Error Emails** field.

**Add**

Adds user-supplied Email recipients to the **Status Emails** or **Error Emails** field. This information is not saved in the configuration file.

**Select All (Logs to Retrieve)**

Selects all entries in the **Logs to Retrieve** list. When you press this button, all subsystem logs are flagged for retrieval. Use this feature sparingly or not at all, since it can cause a huge amount of data to be processed by the request. Most problems can be resolved without examining every system log.

**Clear All (Logs to Retrieve)**

Deselects all entries in the Logs to Retrieve list so that no subsystem logs are flagged for retrieval. (To make individual selections or deselections, simply click on items in the list.)

**Intiate Request**

Routes a new request for processing by LRA.

# How to change the email address of the support site

As mentioned earlier, LRA configuration settings are stored in a local configuration file named `i3lra.cfg`. To send email to a partner's support organization instead of Genesys, edit the file as follows:

1. Use a text editor to edit `i3lra.cfg`.
2. Change the value for `LRAClientMailbox` from `SupportLRA@inin.com` to the partner's email address.
3. Change FTP server settings as follows:
   a. Change `DestSite` to the descriptive name of the support organization.
   b. Change `FTPServer` from `ftp.inin.com` to the ftp address of the support organization.
   c. Change `FTPport` to the port number used at the support site for FTP traffic.
   d. Change `FTPUid` to the user id required to access the support organization's FTP site, where applicable.
   e. Change `FTPpwd` to the password required to access the support organization's FTP site, where applicable.
4. **Save** the file.

This procedure is only required if a partner is taking on support. The `LRAClientMailbox` parameter cannot be changed using the HTML GUI. You must manually edit the file.

# Glossary

**Customer Site**

When LRA is installed on the CIC server that is used by a customer, this server is referred to as the customer site. Separate documentation is available for each audience.

**Email Notifications**

When a support representative requests log information, a well-formed email message is sent to the customer's LRA mail account. LRA monitors this account to find work.

**Event Logs**

Event logs store high-priority messages that require the immediate attention of a system administrator.

**Log Retrieval Assistant (LRA)**

LRA is a CIC utility that helps customers and support personnel work together more effectively by allowing an authorized support representative to retrieve trace logs and other information from a customer's CIC server. LRA helps a CIC Administrator set diagnostic trace levels for various CIC subsystems and to configure Dr. Watson settings on the CIC server. LRA allows authorized support representatives to request segments of event logs, trace logs, and other data written by CIC subsystems. LRA then routes the information to an off-site support representative via the Internet. LRA sends notification messages to inform the requester and the customer about details of each transaction.

**LRA Monitored Mailbox**

LRA Monitored Mailbox is a specified email account on the customer site that Log Retrieval Assistant will monitor to pick up requests. Log requests are mailed to this account for Log Retrieval Assistant to process.

**Monitored Mailbox #0**

The email account associated with a CIC administrator.

**Slowdown Factor**

To ensure that LRA does not degrade the overall performance of a busy CIC server, customers can set a slowdown factor that helps limit the amount of CPU and network bandwidth that LRA consumes. This causes CPU-intensive processes such as snipping, zipping, FTP, etc. to sleep intermittently.

**Support Site**

When LRA is installed on the CIC server that is used by a support organization (e.g. Genesys) that server is called the support site.

**Trace Logs**

Trace logs document the operation of various CIC subsystems.

# Change Log

The following table lists the changes to the *Log Retrieval Assistant Customer Site Technical Reference* since its initial release.

| Date | Changes |
|---|---|
| IC 4.0 GA | • The filename of this publication is `LRA_Customer_Site_TR.pdf` which reflects its new title: LRA Customer Site Technical Reference. It was previously classified as an installation guide.<br>• No other revisions, except for copyright and trademark updates. |
| 01-August-2014 | 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. |
| 12-June-2015 | • Updated cover page to reflect new color scheme and logo.<br>• Updated copyright and trademark information. |
| 09-October-2015 | Updated documentation to reflect 2016 R1 release. |
| 04-February-2016 | • Changed all the references and links to the new CIC Documentation Library at help.inin.com.<br>• Updated documentation to reflect 2016 R2 Release. |
| 19-April-2018 | Rebranded from Interaction Intelligence to Genesys. |
| 14-June-2019 | Reorganized the content only, which included combining some topics and deleting others that just had an introductory sentence such as, "In this section...". |