

Cryoserver GroupWise Configuration (GCIDaemon)

December 2007

Contents

INTRODUCTION	3
EMAIL EXTRACTION DETAILS	4
INITIALIZATION PHASE	4
LEGACY IMPORT MODE.....	4
NORMAL MODE	5
RETENTION DATES	6
BCC (BLIND CARBON COPY) RECIPIENTS.....	6
COMPLETENESS OF DATA EXTRACTION.....	6
LDAP (EDIRECTORY).....	7
DEDUPLICATION	7
GROUPWISE IMAP	8
PERFORMANCE.....	10
INSTALLATION AND CONFIGURATION	11
TRUSTED APPLICATION REGISTRATION	11
ENABLING MESSAGE RETENTION	12
LDAP CONFIGURATION	13
CRYOSERVER CONFIGURATION	14
CRYOSERVER CONFIGURATION FOR SSL/TLS LOGIN SUPPORT.....	15
GCIDAEEMON CONFIGURATION	15
STARTING AND STOPPING GCIDAEEMON.....	20
GROUPWISE MANUAL IMAP OPERATION	22
TROUBLESHOOTING.....	24

Introduction

This document details how to install and configure GroupWise for Cryoserver (*GCIDaemon*).

GCIDaemon is an application that journals messages from GroupWise to Cryoserver. It does this by creating one thread for each GroupWise post office. Each thread logs into the GroupWise IMAP server for its post office, authenticating itself by using a trusted application key. This mode of authentication allows it to obtain a list of users on the post office and log in as each one in turn without needing to provide further authentication.

Once logged in as a user, it can obtain a list of folders then visit each folder in turn and search for new messages. Each new message is extracted, recipient lists expanded using an LDAP connection to e-Directory, and sent or stored as an internet mail in an 'enveloped' format.

Before leaving the user's mailbox the retention date is set so that journaled messages are removed from the trash folder. New messages cannot be deleted until after the next visit.

Requirements

- **GroupWise** v6.5 with Service Pack 4, or 5, or GroupWise v7. The Internet Addressing feature of GroupWise should be used.
- **IMAP** – an industry standard method to access (read) mail in user mailboxes. IMAP must be enabled for each Post Office, and two settings added to the start-up configuration scripts.
- **LDAP** (eDirectory) – an industry standard for accessing directory data (for example, users and email addresses & distribution lists). The older *NDS* may be used, but it does not hold Distribution Group information.

Terminology

- **Cryoserver** - a system for storing formatted email in a searchable, audited and secure way.
- **Daemon** - a process that works in the background.
- **Trusted Application** – a method for a remote process to authenticate with GroupWise and get special privileges. In this case, to read all mailboxes in a PostOffice.
- **Retention Date** – a feature of the GroupWise Trusted Application facility that prevent users from deleting email until it has been processed and the retention is updated.

References

Groupwise extensions to IMAP can be found at:

<http://developer.novell.com/ndk/doc/gwimap/index.html?page=/ndk/doc/gwimap/gwimpe/nu/data/al7te9j.html>

Email Extraction Details

GCIDaemon polls each GroupWise post office for messages via IMAP. It gains access to individual user mailboxes without requiring their login details because of the Trusted Application status.

The range of email extracted from a user's mailbox is determined by the GCIDaemon mode.

The mode is selected through command-line parameters and may be one of the following:

- **Legacy Import Mode.** Processes all/selected messages (up to the date of GWDaemon initialization) then exits.
- **Normal Mode.** Processes new messages by polling each mailbox in turn, and repeating indefinitely. The user mailbox retention date may be set, if required.

A database of extracted email IDs is stored so that the same message is not processed twice (deduplication). The database persists so that the application can be restarted any number of times and duplicate email will continue to be detected.

These modes are described in more detail below.

Initialization Phase

Initialization is an automated process and establishes a date and time from which a forensic email record will be created. Messages with dates prior to initialization may be imported using *Legacy Import Mode*.

Initialization involves:

- Opening an IMAP connection
- Logging in as a trusted application
- Obtaining the user list
- Setting each users retention date to the current date.

When a new post office is added to the configuration file, and the daemon is restarted in Normal or Legacy Import Mode, then the post office will be initialized.

During normal post office processing, the daemon rechecks the post office user list. If new users are added to the post office, then they are initialized into the daemon and set with the initial retention date.

Legacy Import Mode

Legacy Import Mode collects messages created prior to initialization from each post office. These messages are marked as imported in Cryoserver, indicating that they are not

identical to the original email as delivered to the user. Legacy Import Mode is a slight variation of Normal Mode, the differences being:

- When searching a folder, messages are selected by date range provided in the configuration file, or all messages up to the date of initialization.
- Retention dates are not used for searching and are not set by the application.
- After processing each mailbox, a summary is written to an import log file.
- After a post office has had all users fully extracted, an email is sent with the completion status.
- After all post offices have been processed, the daemon exits.
- The daemon can be stopped and restarted at any time. It will continue from the point that it was last stopped.

Import and Normal Mode message objects persist in the same database to ensure duplicates are detected consistently.

Due to IMAP and LDAP issues, it is possible that a single post office pass is insufficient to extract all email. Consequently, the application rescans five times, selecting any mail that was not processed on earlier runs.

Note: Distribution Groups will be expanded to show **today's** recipients – which may not be true as at the time that the mail was originally sent.

Normal Mode

In Normal Mode, each mailbox is visited in turn and any new messages are extracted. This process is repeated indefinitely until the application is shut down.

Normal Mode carries out the following:

1. Opens an LDAP connection.
2. Opens an IMAP connection.
3. Logs in as a trusted application.
4. Obtains the user list.
5. Visits the next mailbox.
6. Obtains the folder list.
7. Visits the next folder.
8. Searches for message dates since the last retention date and with UID greater than the last one processed. For each message found, it:
 - Fetches and expands the recipient headers using LDAP
 - Fetches the message content
 - Stores the message in the store directory for the post office. The file stored consists of the message object (serialized as a set of properties) followed by

the RFC822 representation of the message. This file will later be picked up by the *Message Store Handler* and converted to RFC3462 format and passed to Cryoserver.

Due to the nature of IMAP and LDAP, if the system detects problems, it will disconnect from IMAP and LDAP and then reconnect. Processing will then continue from where it left off. This may occur several times if GroupWise is taken off-line.

Retention Dates

A feature of GroupWise is to prevent email to be deleted until its date/time is older than the retention date set for that user's mailbox. A Trusted Application can be allowed to update the user's mailbox retention date.

The retention date setting in GroupWise can be applied to individual mailboxes, post offices or the entire server.

Note: Retention also applies to the *Draft/Work-in-Progress* folder. This means that when a user updates a draft copy of an email prior to sending it, GroupWise will store a separate copy of each draft version of an email (until the retention has been updated). This is a known bug with GroupWise that will not be fixed in version 6.5.

BCC (Blind Carbon Copy) Recipients

Due to the nature of BCC information, **only** the sender actually knows the full BCC recipient list. This information is not available in received mail after delivery to each mailbox. Consequently, BCC information (final recipient vs. intended recipient) is not available to the GCIDaemon.

For this reason, most other email systems (Notes/Exchange/Teamware) support archive journaling during the transport phase of new mail – where the true *final* recipient information becomes available. In Exchange and Teamware, a special 'envelope' format of journal email is produced, where this final recipient list is added to the email data within the envelope part of the email.

GCIDaemon generates mail in an 'envelope' format – one that holds the full original email plus an extra part that lists the recipients of the email.

Completeness of Data Extraction

Because IMAP is used to extract email, only those folders and items that are made available to IMAP are extracted. In practice, this means that the following **are** included:

- The Inbox and any subfolders
- Any standard user-created email folders
- Sent Items
- Draft mail (though the Daemon will skip these)
- Deleted Items

But the following are NOT included:

- Diary appointments
- Shared folder contents
- Non-email items (documents, and other general file data)
- Notes
- Contacts/Address Book data
- Instant Messaging.

Note: Cryoserver only stores data in Internet Mail format. Consequently items like Notes and Appointments will not work in Cryoserver, unless they are part of an email.

LDAP (eDirectory)

GCIDaemon uses LDAP (usually e-Directory – but it could be another system) in order to:

- Convert lists of GroupWise formatted recipient addresses [user name/postoffice/server] into lists of RFC822 (internet) addresses [name@domain.com].
- Expand distribution groups – to obtain the list of internet email addresses for each member of the group (and groups-within-groups).

LDAP is only used to convert email addresses for the set of domain names specified in the configuration file. For example, it will attempt to look-up the address *fred/MYPO/NY1@abcdomain.co.uk*, but not *fred@msn.com*, where *abcdomain.co.uk* is configured in GCIDaemon as a company's domain.

LDAP data is cached within the memory of the GCIDaemon process. Therefore, LDAP is not accessed where the same email address occurs several times. However, to prevent any data entry from becoming stale (where a user's email address changes) it is refreshed from LDAP after the configured timeout period.

TLS / SSL Access to LDAP

It is possible to use TLS (preferred) or SSL as encryption techniques to eDirectory/LDAP. To do this a certificate needs to be created (TLS) or exported (SSL).

For TLS, a separate utility can be used to access and create a TLS certificate. The utility can be found on the Novell website. We supply an enhanced utility that includes a system to test the LDAP connection parameters with some email addresses.

Deduplication

Each single mail in GroupWise is allocated a unique ID, regardless of the number of recipients. Therefore, when an email is sent to five users, GCIDaemon will find this same

email five or six times (once for the sender, if an internal mail). However, they will **all** have the **same** ID code. GCIDaemon keeps a database of the extracted IDs.

IMAP can return just the mail headers, prior to reading the whole mail from the server – and so the GCIDaemon is able to only download the first copy of these emails.

If multiple GCIDaemon systems are used, then duplicate items will be created, unless they can share the same database. Consequently, this is not recommended.

Cryoserver does not currently deduplicate received emails.

GroupWise IMAP

GCIDaemon uses IMAP to extract email, as this guarantees that every GroupWise email is converted into the Internet mail format (MIME / RFC822) in a standard, fast and consistent way. Furthermore, mail extraction (GCIDaemon) can be hosted on any server (for example, Linux or even a mainframe).

If the GroupWise Mail API is used, then all GroupWise internal mail body-text (and some attachment data) would need to be converted into equivalent MIME formats (plain text/html) – which may not produce very good fidelity with the original item. Furthermore, it requires a Windows computer to be used for the extraction process.

IMAP Read and Size Limit Settings

GroupWise IMAP has some limitations, the key one is that it caps the total number of emails allowed to be listed/extracted from any single folder or sub-folder. By default this is set to (just under) 5000. If a folder is opened with more than this limit, IMAP will raise a warning message. The */imapreadlimit* parameter in the Postoffice start-up configuration file allows this limit to be raised – but it then uses more GW memory where a very large folder is opened. A good start setting value is 10 (= 10,000 mail limit), though 30 could be allowed (server memory use should be monitored).

Another setting is the */imapsizelimit* that determines the maximum size (in MB) of a mail that is read into the server memory. Over this limit size, the data is read directly from disk. By **not** setting this, or setting it to a large value, some GroupWise systems will AbEnd (Abnormally End). We recommend using a value of between 5 and 8. Again, use GroupWise monitoring tools to ensure that the memory use does not rise too much.

An example start-up section in a postoffice.poa configuration file:

```
; INTERNET AGENT SWITCHES

/imapreadlimit 10

/imapsizelimit 5

;/imap Enabled

; IMAP Port, The default is 143, but alter for MTAs' imap or other post
offices on same server

;/imapport 144
```

Note: The formatting of these switches is different on Netware, Linux and Windows:

	NetWare POA	Linux POA	Windows POA
Syntax	<code>/imapreadlimit-number</code>	<code>--imapreadlimit number</code>	<code>/imapreadlimit-number</code>
Example	<code>/imapreadlimit-10</code>	<code>--imapreadlimit 20</code>	<code>/imapreadlimit-50</code>

For further examples see:

http://www.novell.com/documentation/gw65/index.html?page=/documentation/gw65/gw65_admin/data/a84jmbe.html

IMAP Error Handling

Novell's implementation of IMAP in GroupWise has a few inconsistencies – though GroupWise 6.5 Service Packs 4 and 5 are improvements. Consequently, there is a fairly robust error handling strategy as follows:

- If an exception is thrown during message processing a *FailedMessage* instance is created for it and saved in the database.
- After each folder has been processed in the normal way the failed messages for the folder are retried.
- Each time a retry fails, the message retry count is incremented. When the retry count reaches the retry limit (currently hard-coded at 3) the failed message record is deleted and an alert email is sent.

If, on completion of a mailbox, there are outstanding failed messages, the retention date for the mailbox is set to the date of the earliest failed message instead of the latest successful message as normal.

IMAP Performance

IMAP is a fairly efficient method for mail extraction. GCIDaemon tries to only access new email in a folder, or ones within a specific range. It keeps a list of all GroupWise internal message ID's that have been extracted – so it only reads the whole mail body for items not yet extracted.

The rules of IMAP determine that the following processing will be observed:

- A sequential item number system will ensure that every item in a folder can be referenced uniquely by IMAP. [This is **not** the same as the GroupWise internal mail ID].
- When an email is changed, deleted or merged, the sequential number may need to be recomputed.
- An IMAP flag tells clients when these sequential numbers have been reset – in which case all mail in the folder is reexamined.
- IMAP can retrieve mail lists via a query – for example, limiting mail to a date or number range.
- IMAP performs any conversion from proprietary GroupWise mail formatting into Internet Mail format.

Therefore, IMAP is most efficient when:

- Only new mail is being added. Changes to folder content may result in extra processing for IMAP.
- Internal GroupWise format mail is kept to a minimum.
- Mail is not allowed to get too large (large = 20MB+, very large = 100MB+).
- Folders are not allowed to have too many items (large = 5000+).

Performance

In **any** system, mail journaling will cause about 35% extra workload on the server. For legacy email extraction with multiple mailbox reader threads, this may be much greater.

GCIDaemon saves the current position in every folder of every mailbox and it keeps a list of every email ID that was extracted. This helps prevent rereading existing data, or accessing mail that was previously extracted.

However, if GCIDaemon is seen as affecting the GroupWise performance, a delay can be configured to pause between each:

- Connection
- Mailbox
- Folder
- Mail item.

The downside of mail-item and folder delays is that it takes longer to traverse a post office.

LDAP lookups are cached, thus reducing the number of lookups for the same information. The cache size and timeout are configurable, so that more LDAP data can be held in memory for longer (as reasonable).

Installation and Configuration

The following sections describe the procedures needed to install or configure each component that supports GCIDaemon.

Trusted Application Registration

The application used to register GCIDaemon as a trusted application needs to be run on a Windows-based computer with the *GroupWise NetWin32 Dynamic Link Library* registered. This DLL is registered automatically when *ConsoleOne*, GroupWise snap-ins or the GroupWise client is installed.

Note: The trusted application will only need to be installed **once per domain**.

1. Run **GWTA_Install.bat** specifying the path to the GroupWise domain database.

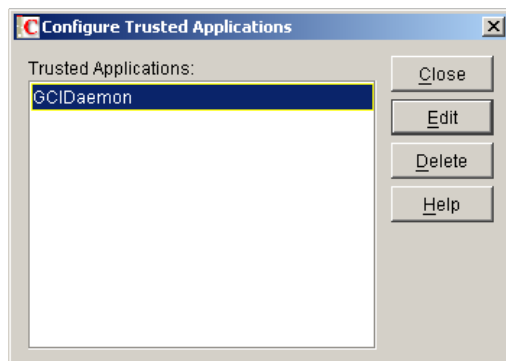
For example, GWTA_Install.bat \\hostname\public\grpwise\domain\domainname

You see a message stating the application has been registered and you see two new files in the directory:

- *gwa_GCIDaemon.ini* which contains the trusted application key used by GCIDaemon to access the GroupWise Post Office.
 - *Gwa_GCIDaemon_remove.bat* which is used to remove the trusted application from the GroupWise domain.
2. To check that the trusted application has been installed correctly start **ConsoleOne**, and click the GroupWise System icon in the folder-tree.

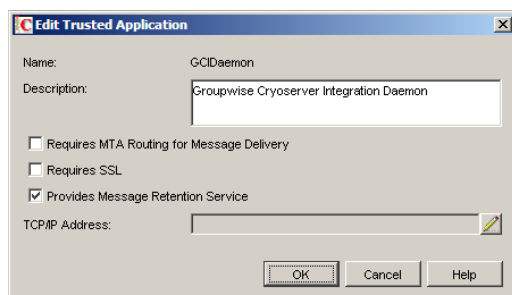
Then on the Client menu bar click, **Tools > GroupWise System Operations > Trusted Applications**.

You see the following:



3. Select GCIDaemon and click **Edit**.

You see the following:



4. Select **Provides Message Retention Service**.

The retention date is **not** enforced within GroupWise **until** the post offices have been adjusted to perform retention checking. When set, the user's mail cannot be deleted if it is dated **after** the current retention date for the user.

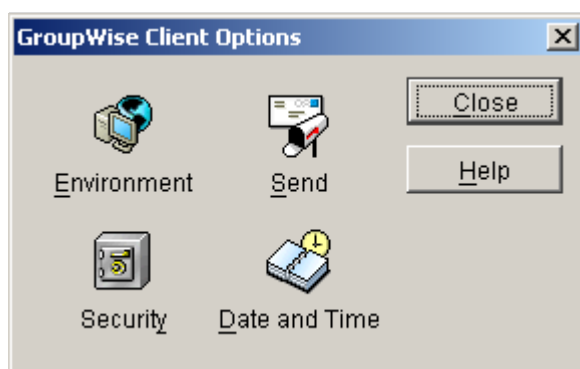
In Normal Mode, after a user's mailbox has been visited and all recent emails extracted, the user's retention date is reset to the current date. Thus the contents of the user's trash folder will be released and emptied.

Enabling Message Retention

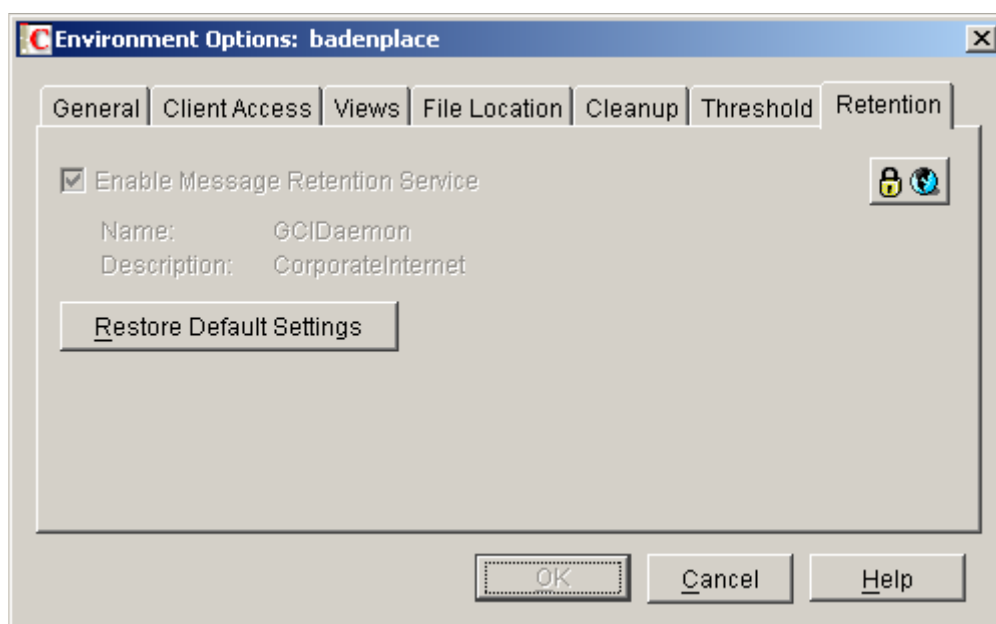
After installing GCIDaemon, the Groupwise Message Retention Service needs to be enabled. This can be specified at the domain, post office or individual user level. After this retention has been enabled, all messages within the relevant mailboxes will be retained by GroupWise until CIDaemon extracts them and updates the retention date timestamp.

To enable retention

1. From **ConsoleOne**, right-click the domain, post office or user where message retention is to be enabled.
2. Click **GroupWise Utilities, Client Options** to display the GroupWise Client Options dialog box:



3. Click **Environment** to display *Environment Options* and then click the **Retention** tab.



4. Select **Enable Message Retention Service**.

Note: If you have chosen a post office or domain for the message retention service you must click the padlock icon on the right to disable the ability to toggle the message retention service at lower levels.

Now all users within the scope of the retention service will be unable to delete or edit sent and received mail.

You must set GCIDaemon configuration option to match the GroupWise retention setting:

```
gcidaemon.retention=true or, <postoffice>.retention=true
```

GCIDaemon will set the users retention date in GroupWise if this flag is set to *True*. Otherwise, it will hold the date in its internal database.

Note: If a user tries to delete a message it will be moved to the trash folder. The trash folder is only emptied after GCIDaemon has successfully processed all messages in the mailbox and updated the retention timestamp.

LDAP Configuration

Both GCIDaemon and Cryoserver require access to the LDAP system (e-Directory) that allows directory search permissions. Search permission is required to support distribution list expansion.

Note: Cryoserver currently only supports plain-text login.

GCIDaemon also supports LDAP login using SSL, TLS, DIGEST-MD5 (a SASL method). The default is plain text.

Use Console One to add a new user named **CryoserverLDAP** to the organisation with rights to read the directory of each post office. The password will be added to the GCIDaemon configuration file, and must be added to Cryoserver, via the Super User configuration, for the company.

For Cryoserver to support end user login via LDAP, you must select the 'Allow plain text password' option in the LDAP Server node using Console One. Furthermore, you must allow non SSL/TLS access. Otherwise, Cryoserver will require local basic user accounts to be manually added to Cryoserver via an Admin user.

Cryoserver Configuration

Log into Cryoserver as a super-user.

In the **Company Details** section enter the following custom information:

LDAP directory user	cn=CryoserverLDAP,ou=<organisational unit>,o=<organisation>
LDAP directory password	(as set in LDAP/eDirectory)
LDAP user dn	#
LDAP base dn & search dn	o=<organisation>
LDAP primary field name	mail
LDAP primary field pattern	(.*)
All other LDAP primary/secondary fields must be left blank.*	
LDAP type	custom
LDAP translate users	Yes
LDAP translation key	cn
LDAP SSL	No
LDAP cache size/timeout	300 *
Spool mode	RFC3462 **

* Note: As GCIDaemon automatically expands distribution lists, do not enter any other LDAP information in the fields as this may cause Cryoserver to work slowly or put messages in the error directory. This also means that the LDAP Cache is not used.

** Note: As GCIDaemon uses an envelope wrapper for messages containing the original recipients Cryoserver needs to be configured to use the RFC3462 format so that it knows to extract the message from the envelope before indexing and archiving.

Cryoserver Configuration for SSL/TLS Login Support

Cryoserver Version 1.3.4i now supports end-user login validation via SSL/TLS access to eDirectory (and Active Directory too).

To support TLS, a TLS certificate needs to be created by running the Novell TLS certificate utility.

Cryoserver have an extended version of this utility that can also test the LDAP connection and its ability to convert/expand email addresses.

- Expand (unzip) the LDAPtest_install.jar to /opt/ldaptest
- Edit the bin/tls_cert_create so that the directory paths and parameters are correct - you will need to enter a user's LDAP FQDN and password, and path to the output file
- Run the /opt/ldaptest/bin/tls_cert_create.sh script

Put the path to the TLS certificate file created above into the gcidaemon.conf configuration file, and enter it into the Company Edit web page in the Cryoserver Super User web.

GCIDaemon Configuration

1. Obtain the IP address and IMAP port number of each of the post offices then place them in the configuration file along with the trusted application key.
2. Edit the configuration file:

```
vi /opt/gcidaemon/conf/gcidaemon.conf
```

Sample Configuration File

```
# general configuration

gcidaemon.postoffices=badenplace

gcidaemon.retention=true

gcidaemon.store.seen=false

gcidaemon.state=true

gcidaemon.freeze=true

gcidaemon.message.store.handler=true

# mail configuration for alerts

mail.host=127.0.0.1

mail.from=cryodaemon@complianceinternet.com

mail.transport.protocol=smtp

gcidaemon.mail.to=cryoadmin@corporateinternet.com
```

```
gcidaemon.mail.subject=GCIDaemon

# ldap configuration

gcidaemon.ldap.host=10.10.10.17

gcidaemon.ldap.login=cn=admin, o=office

gcidaemon.ldap.password=snoopy

gcidaemon.ldap.groupdn=o=office

gcidaemon.ldap.advanced.lookup=true

gcidaemon.ldap.local.domains=groupwisetest.com

# mercator configuration

mercator.db.driv=com.mysql.jdbc.Driver

mercator.db.url=jdbc:mysql://localhost/gcidaemon?autoReconnect=true

mercator.db.uid=gcidaemon

mercator.db.pwd=gcidaemon

# cryoserver configuration

gcidaemon.cryoserver.host=gcidaemon

gcidaemon.cryoserver.from=cryodaemon@complianceinternet.co.uk

gcidaemon.cryoserver.to=cryouser@complianceinternet.co.uk

gcidaemon.cryoserver.dropdirectory=/opt/cryoserver/cryoserver/data/uk-ln-sp-001/spool

# post office configuration

badenplace.hostname=10.10.10.17

badenplace.port=144

badenplace.key=R0NJRGFlbS9uAEUwNTQ3MzYxMEVBMTAwMDA5QjY0OUUwMDYzMDAzNDAwRWA1NTczNjIwRURxMDAwMDlCNxQ5RTAqNjMwMDM0UDA=

badenplace.storepath=/opt/gcidaemon/msgstore/

badenplace.configpath=/opt/gcidaemon/conf/

badenplace.dateformat=dd-MMM-yyyy HH:mm:ss Z

badenplace.delay.connect=1000

badenplace.delay.mailbox=1000

badenplace.delay.message=1000
```

```

badenplace.delay.folder=1000

badenplace.import.log=/opt/gcidaemon/logs/import.log

# logging configuration

log4j.rootLogger=debug,R

log4j.appender.R=org.apache.log4j.RollingFileAppender
log4j.appender.R.File=/opt/gcidaemon/logs/gcidaemon.log

log4j.appender.R.MaxFileSize=10Mb
log4j.appender.R.MaxBackupIndex=1

log4j.appender.R.layout=org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern=%d{yyyyMMdd HH:mm:ss} %p %t %c{1} %m%n

```

Global Configuration

<i>gcidaemon.postoffices</i> <i>gcidaemon.legacy.postoffices</i>	A comma-separated list of post office names, that are used as property labels in the post office configuration sections. There is a list for Normal Mode operation and another for Legacy Mode.
<i>gcidaemon.retention</i>	If set to <i>true</i> then retention dates are set.
<i>gcidaemon.state</i>	If set to <i>true</i> then the unique ID of each message is stored in the database so that duplicates can be eliminated.

Post Office Configuration

Each post office is assigned a name which is used as the first part of each configuration label for the post office. The post office names are listed in the global configuration *gcidaemon.postoffices* property.

For example:

```

gcidaemon.postoffices=potest1, potest2

gcidaemon.legacy.postoffices=potest2

potest1.hostname=123.123.123.123

potest2.hostname=123.123.123.10

```

<i><postofficename>.hostname</i>	The IP address or hostname of the GroupWise post office
--	---

<i><postofficename>.port</i>	IMAP Port used to connect.
<i><postofficename>.key</i>	The Registered GroupWise trusted application name plus the key, encoded using Base64. A global setting may also be used.
<i><postofficename>.dateformat</i>	The date format used by the GroupWise IMAP server. The default value should be sufficient for most configurations.
<i><postoffice>.delay.connect</i>	Delay before connecting to post office in milliseconds.
<i><postoffice>.delay.mailbox</i>	Delay before connecting to a user's mailbox in milliseconds.
<i><postoffice>.delay.folder</i>	Delay before connecting to a folder within a user's mailbox in milliseconds.
<i><postoffice>.delay.message</i>	Delay before processing a message in milliseconds.
<i><postoffice>.reconnect</i>	If non-zero the daemon restarts after this period (specified in minutes), reconnecting to both the IMAP and LDAP servers. A value of zero disables this feature. The default value is zero.
<i><postoffice>.timeout</i>	The IMAP socket timeout, specified in milliseconds. A value of zero disables socket timeout (i.e. the IMAP client will wait indefinitely for a response). The default value is 60.

Alert Configuration

This area is used to configure the alert messages for the Cryoserver support team. Using these details the GCIDaemon will send an e-mail alert every time it is started, stopped or hits a serious error.

<i>mail.host</i>	The mail server used to send out SMTP alerts.
<i>mail.from</i>	E-Mail address that the alert comes from.
<i>gcidaemon.mail.to</i>	E-Mail address to send the alert to. (Only currently supports 1 address).
<i>gcidaemon.mail.subject</i>	Subject of the alert. Preferably put the company name in here as well.

LDAP Configuration

These properties specify how the daemon should connect to the LDAP server.

<i>gcidaemon.ldap.host</i>	The IP Address of host name of the LDAP server.
<i>gcidaemon.ldap.login</i>	The DN for logging into the LDAP server.
<i>gcidaemon.ldap.password</i>	The password for logging into the LDAP server.

<i>gcidaemon.ldap.groupdn</i>	The DN under which to search for users.
<i>gcidaemon.ldap.advanced.lookup</i>	Set to <i>True</i> to enable additional LDAP searching for some hard-to-identify email recipients.
<i>gcidaemon.ldap.local.domains</i>	A comma-separated list of email domains. The daemon will check email addresses in these domains against the LDAP server to see if they are mailing lists, in which case they will be expanded.

Database (Mercator) Configuration

Mercator is the Object-Relational Manager (ORM) that manages the daemon's interface to the database.

<i>mercator.db.driv</i>	The fully-qualified class name of the JDBC driver used to connect to the database.
<i>mercator.db.url</i>	The JDBC URL of the database.
<i>mercator.db.uid</i>	The user ID for logging into the database.
<i>mercator.db.pwd</i>	The password for logging into the database.

Cryoserver Configuration

These properties control how the daemon formats and transfers messages to Cryoserver. Messages extracted from GroupWise are passed to Cryoserver as attachments to wrapper messages that contain further information about them required for storing and indexing.

<i>gcidaemon.cryoserver.host</i>	The hostname to use in the Received: header of the wrapper message.
<i>gcidaemon.cryoserver.from</i>	The email address to use in the From: header of the wrapper message.
<i>gcidaemon.cryoserver.to</i>	The email address to use in the To: header of the wrapper message.
<i>gcidaemon.cryoserver.dropdirectory</i>	The directory where wrapper messages should be dropped. This is normally the Cryoserver spool directory.

Logging Configuration

The daemon uses *log4j* for logging which provides a highly configurable logging system. The notes below assume the basic configuration shown in the sample configuration file. For full information on configuring *log4j* see <http://logging.apache.org/log4j>

<i>log4j.rootLogger=debug,R</i>	Sets the level of logging. The useful levels are: <i>debug</i> (most log messages), <i>info</i> , <i>warn</i> and <i>error</i> (fewest log messages).
---------------------------------	---

<i>log4j.appender.R.File=/opt/gcidaemon/logs/gcidaemon.log</i>	Set the name of the log file.
<i>log4j.appender.R.MaxFileSize=10MB</i>	Set the maximum size to which the log file will be allowed to grow before it is rolled.
<i>log4j.appender.R.MaxBackupIndex=1</i>	Each time the logs are rolled, the current file is copied with the suffix .1, the old .1 file becomes .2 and so on. These suffixes are known as backup indexes and this option allows you to set the highest backup index after which rolled files are simply deleted.

Starting and Stopping GCIDaemon

To start/stop GCIDaemon:

1. Log in to the server running GCIDaemon.

Stop/start the Windows service or use the Linux commands to start/stop the background task as follows:

To start the Normal mode GCIDaemon	<code>/opt/gcidaemon/bin/gcidaemon.sh start</code>
To stop the Normal mode GCIDaemon	<code>/opt/gcidaemon/bin/gcidaemon.sh stop</code>
To start the Legacy mode GCIDaemon	<code>/opt/gcidaemon/bin/gcilegacy.sh start</code>
To stop the Normal mode GCIDaemon	<code>/opt/gcidaemon/bin/gcidaemon.sh stop</code>

The Wrapper

GCIDaemon is run inside a Java service wrapper so that it can work in the background. The documentation for this wrapper can be found at:

<http://wrapper.tanukisoftware.org>

The GCIDaemon configuration file for the wrapper is found at:

`/opt/gcidaemon/conf/gcidaemon.wrapper.conf`

or,

`/opt/gcidaemon/conf/gcilegacy.wrapper.conf`

Usage:

`gcidaemon.sh [start|stop|console|status]`

Notes:

- The `console` parameter is used to run GCIDaemon in the current terminal session where logs are displayed directly onto the screen and also placed into log files. This setting is only recommended for debugging purposes as closing the terminal session will stop the application.
- The `Status` parameter is used to check if the GCIDaemon service is currently running or if it has shut down.

GroupWise Manual IMAP Operation

A telnet session in DOS (Windows) or Linux can be used to emulate an IMAP session. Use this to confirm that each post office has IMAP enabled and that the Trusted Application state is working.

```
>telnet potest1 143

Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet>
```

Windows Telnet Only

If any mistake is made during the input of a command, the backspace will not work. The backspace is sent as part of the command.

Each command sent to the IMAP server should have a tag associated with it. These usually take the form of `A###` where # is a number. For example, `A000`, `A001`, `A002`.

This tag is used to associate commands with their responses from the server, as many commands may be issued and processed at once the user needs a way to see what response is associated with each command.

To log in to the GroupWise server via IMAP telnet to the IP address on the POA IMAP port (Default 143).

A000 CAPABILITY

This command tells you whether trusted application authentication is present on the server. If not refer to the GroupWise Cryoserver installation guide for instructions on configuring this.

Typical output from this command is:

```
* CAPABILITY IMAP4rev1 AUTH=XGWTRUSTEDAPP XGWEXTENSIONS

A000 OK CAPABILITY completed
```

The * at the beginning of the first string simply tells us that this is a server broadcast message and not associated with any particular tag or thread. The tag number is returned after this line with a **OK CAPABILITY completed** statement. This tells us that the command completed successfully. If this returned a **BAD** statement then the command did not work or was input incorrectly.

A000 XGWEXTENSIONS

This command checks that the relevant extensions are installed on the GroupWise system.

A000 AUTHENTICATE XGWTRUSTEDAPP

This command tells the IMAP server that we will be authenticating as a GroupWise trusted application. We are then prompted with the '+' symbol to enter the authentication key. To send the authentication key type:

```
XGWTRUSTEDAPP
R0NJRGF1bW9uADFBOUZGM0MxMDMyQTawMDA5NDg1RkUwMD1FMDAzNDawMUE5RkYzQzIwMzJBM
DAwMDk0ODVGRTAwOUUwMDM0MDA=
```

This key should be replaced with your trusted application key. If this is successful you will receive the following message:

```
A000 OK XGWTRUSTEDAPP authentication successful
```

A000 XGWTAULIST

Lists all the users within that post office.

A000 LOGIN username

Logs into a particular users mailbox where username is the user's username returned from the **XGWTAULIST** command.

A000 STATUS INBOX (MESSAGES RECENT UIDNEXT UIDVALIDITY UNSEEN)

Returns details about the mails in the inbox.

A000 XGWRETENTION

Returns the retention date of the current mailbox that you are logged into.

A000 XGWRETENTION "12-Dec-2006 13:00:00 +0000"

Sets the retention date on the mailbox you are currently logged into.

A000 EXAMINE "Inbox"

Performs a read-only examine of a folder within a mailbox. Returns the number of emails that exist and a number of other details.

Troubleshooting

Original email stored as attachments in Cryoserver

This is caused by the Spool Mode setting in the Company Details area. Log into Cryoserver as a super-user and set this to RFC3462.

Unable to log into Cryoserver using Novell/GroupWise username and password.

If a user is displayed with a *Invalid username or password* error when trying to log in using their Novell/GroupWise credentials then this would suggest a problem with LDAP authentication.

Use the LDAP browser to confirm that the *NGWObjectID* user attribute is being broadcast. Repeat the LDAP Configuration steps again to confirm that all the details are correct. If this fails the problem most probably lies with permissions.

The CryoserverLDAP user requires read permissions (possibly compare permissions as well) to the post offices in order to retrieve usernames and perform a password match. Without these permissions, Novell/GroupWise logins will fail.

In order to test this, in the *Company Details* area of Cryoserver, change the LDAP directory user and password to an administrator. If users are able to log in after this then the problem lies with the CryoserverLDAP user permissions.

GCIDaemon exists with a Thread Terminating error.

This would suggest a problem with the configuration file. Do a *grep* on the logs for the word 'java', and you should be able to see any exceptions that have been thrown by the GCIDaemon.

This can also occur if the configuration file format is incorrect. Double check all entries and if necessary, re-install the configuration from the install disk.

Cryoserver is not processing messages (SMTP GCIDaemon only)

If GCIDaemon appears to be working correctly but Cryoserver is not processing any messages check that the to address under the *[cryoserver]* section in the configuration file is set to *cryouser@complianceinternet.co.uk*

Also, if tag-mode is not NONE then make sure that the server name (Default: *cryodaemon*) is present in the Servers super-user area of Cryoserver.

Log displays the message: NO XGWTRUSTEDAPP or similar.

This error means that GCIDaemon is unable to log into the post office using the trusted application key. Either it is wrong or you are connecting to a post office that is outside of the trusted application registration domain. Remove and re-register the trusted application and place the key (without trailing spaces) inside GCIDaemon configuration file.

or,

the MTA is not running for the GroupWise server. This will prevent the Trusted Application key from being transferred from the Domain to each Post Office by the GroupWise system.

Log displays the message: BAD XGWTAULIST or similar.

This command is issued by GCIDaemon to get the current list of users on the post office. If it fails then either the GroupWise system does not meet the minimum requirements (GroupWise 6.5 with Service Pack 4) or the post office IP address or port is incorrect and you are connecting to a different service such as the GWIA.