GWAVA Inc.

GWAVA Retain

Administration and User Guide

Version 3.5

Contents

Post-Install Tasks

After running through the initial install guide for your OS, you are ready to configure Retain. From this point on, Retain works the same regardless which platform it is running on.
To get Retain ready for regular use, some final one-time procedures need to be run.

- Retain Server needs to be configured.
- Configure the relevant module(s).
- At least one Retain Worker needs to be configured.

Initial Setup Overview

1) Choose your storage path.
2) Retain prompts you for access information to your SQL Database Server.
   - You must create this database beforehand. (See install document appendix for documentation for the supported SQL servers.)
   - Retain creates the tables, indexes, and prepares the database for use.

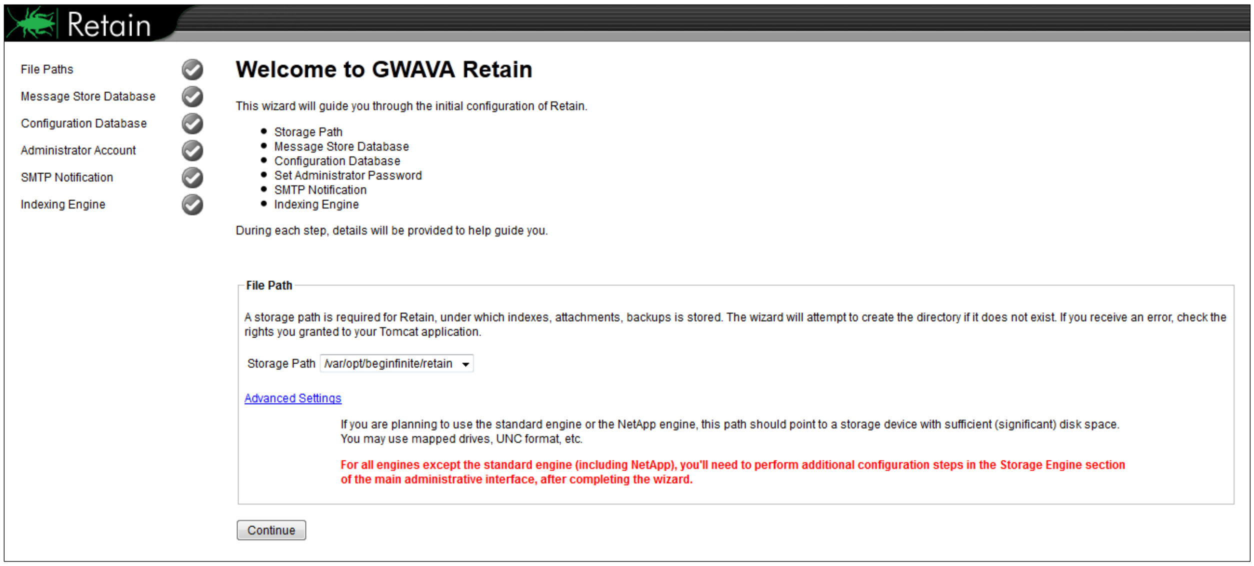
   You will be prompted to provide SQL connection information for both the configuration and message store databases. For convenience and simplicity most installations store this information in the same database. The database(s) will be used to store Retain configuration, cached address books, and all saved message data.
3) Create an administrator account with the default username, admin. It is the first account to be created.
   - This account is special:
     - It has ALL admin rights
     - It never expires
     - It always uses "offline authentication", (authenticates using a password stored in the SQL configuration database).
   - Additional accounts can be created as desired with as many rights as you wish. User accounts may possess a mixture of administrator level and user level rights. As a result, users may have some admin level rights, but would not be considered an administrator.
4) Retain prompts you for the following SMTP information for notification and forwarding. (If no SMTP is present, this step may be skipped by typing the word 'skip' in the SMTP field.)
   - SMTP Server to use for sending messages. (DNS or IP) (use DNS whenever possible)
   - From address. Enter the address that you want to appear in the "From" field on the messages Retain sends.
   - To address. Enter the address to which Retain will send notification.
   - Username: Enter the username to use for authentication with the SMTP server for relaying mail.
   - Password: Enter the password for this username.

   DNS host names are generally recommended instead of IP Addresses in almost all cases due to ease in central management and repair if a server moves or is replaced.
5) Select the indexing engine. There are two different indexing engines available for use with Retain: Lucene and Exalead. Exalead is to be used with larger systems and requires a separate dedicated server. Lucene is a high performance embedded indexer, which requires fewer servers, but is more memory intensive and does not offer high availability features. Please see the install guides and system requirements for more information on which is appropriate and should be used. Exalead is priced separately; see your appropriate sales representative.

After initial setup, configuration of a module and creation of a profile, schedule, worker, and job are required before messages can be archived.

GWAVA Retain Initial Setup

1) Open your web browser.
2) Go to
`http://<your-RetainServer-ip>/RetainServer`
3) Follow the wizard.
You will see this screen initially:



Please pay special attention to the Storage Path and the Advanced Settings (see next page). ***For descriptions of the different engines, see the Storage Manager section. If you select a storage system that is not local, be sure to visit the Storage Manager after the initial setup to ensure that all information has been provided.***

4) You are now ready to start your initial Retain configuration. Specify a storage path for Retain. Accept the default path unless you have a reason to choose a different one. See the next page for an important note about storage paths. If you are specifying a custom storage path, Retain must have rights to the location. For Linux instructions see *Custom Storage Path Rights*, at the end of the Linux install guide.
5) Click “Continue”.

About Storage Paths

Retain was designed to be very flexible in allowing you to choose where the data will be stored. Choosing the right hardware and software storage combination is crucial. Storage itself is a function of the operating system and hardware you choose.

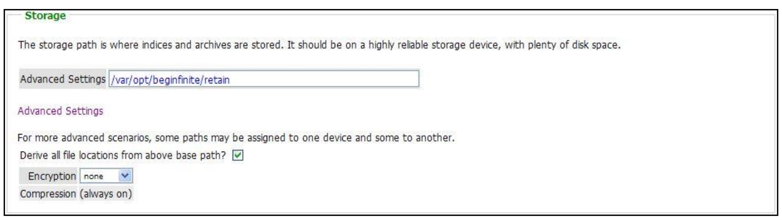
As storage needs approach enterprise levels, the need to specify your data storage locations becomes more critical. Some hardware and operating systems have a hard limit of 2 Terabytes, for instance. In situations like these, a SAN might be a good choice for consideration. (Please visit the Storage Manager section to view options for different SAN systems.) Either way, it's imperative that you take the time to investigate your storage needs BEFORE you begin.

When choosing your storage system, bear in mind the following considerations:

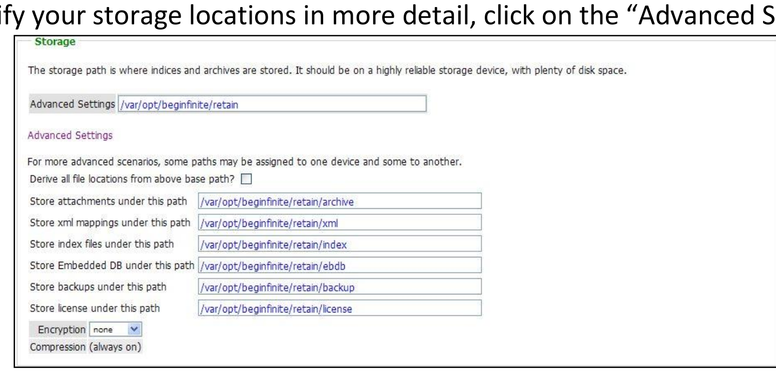
- 2 TB limit. Will storage needs ever exceed this?
- OS Version and kernel to support the storage system of your choice.
- File system and partitioning.
- Is a SAN right for you?
- Speed and reliability.
- Backup/restore is your responsibility.

Advanced Storage Options

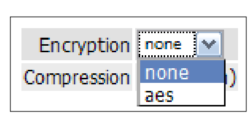
For this reason, Retain offers the advanced storage options. (Located under Server Configuration.) You can specify where you want Retain to store its information.



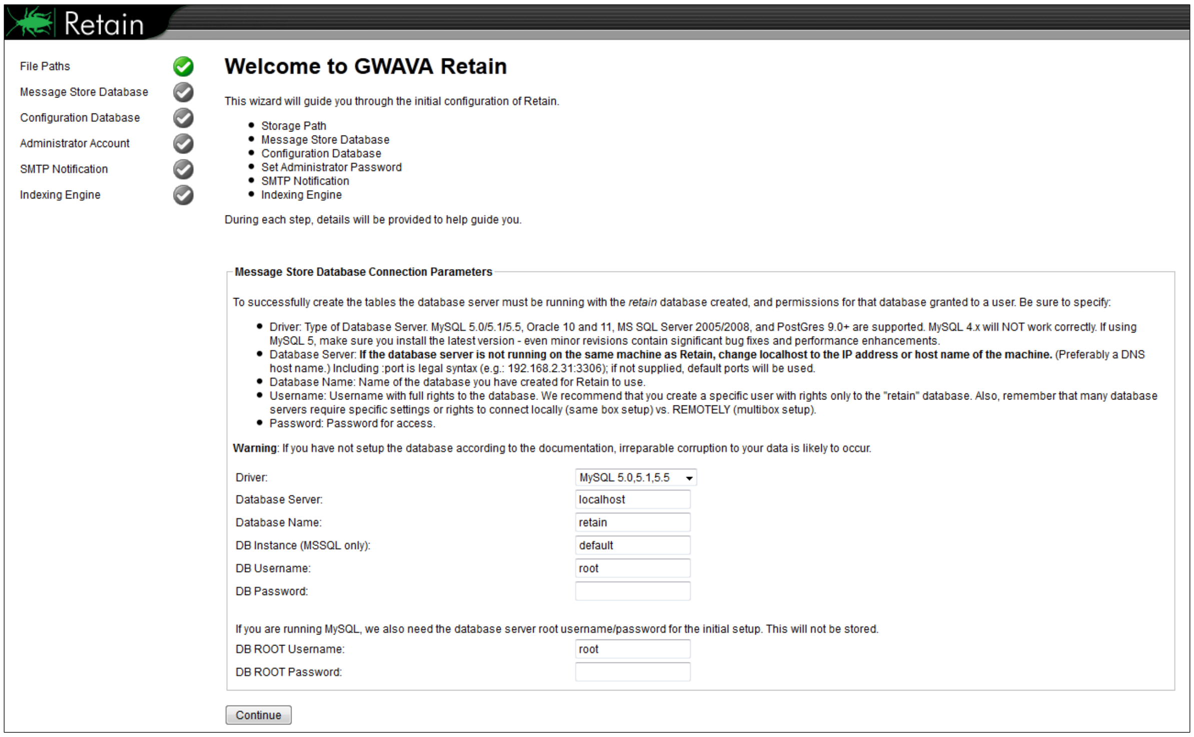
By default, all data is stored under one master path, specified in the Storage section. From the Retain Server main screen, you can also find this under Server Configuration under the Index/Storage tab. If you wish to specify your storage locations in more detail, click on the "Advanced Settings".



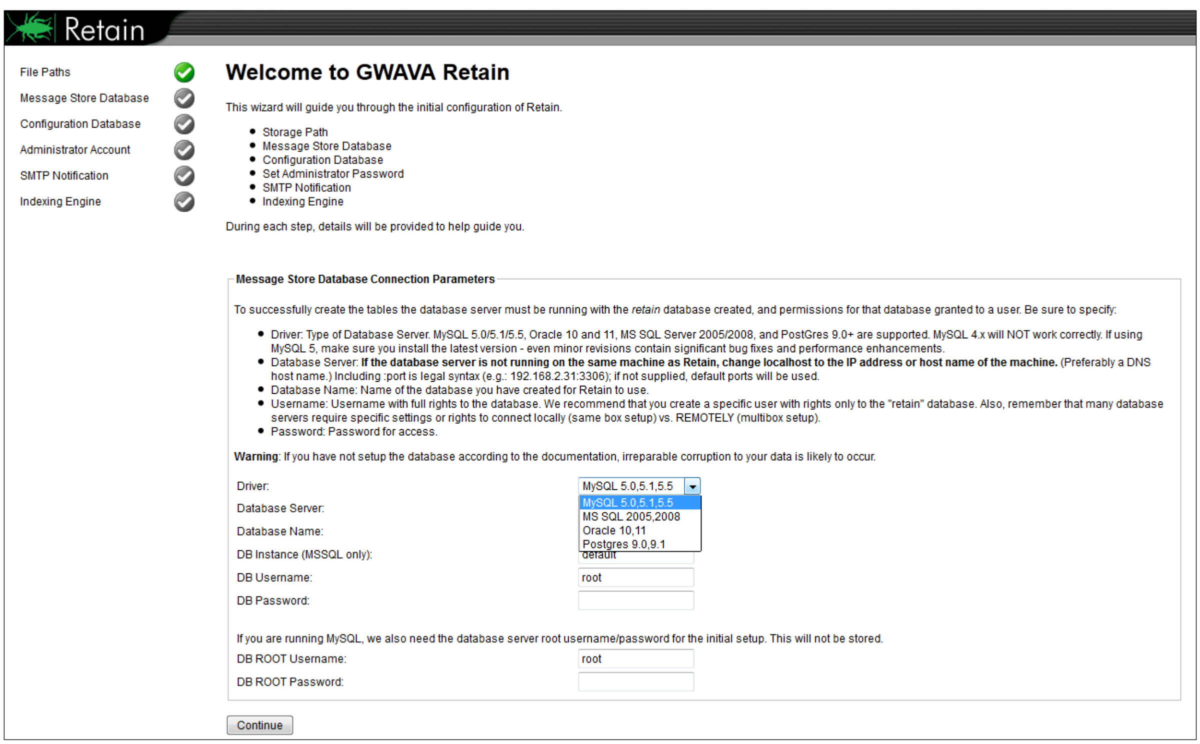
These fields are automatically populated if you only specify the main storage path. You may change them to point anywhere you wish. You may also change the storage locations later due to storage space needs. Please see the Partitions section for details. You also specify to encrypt the data as it's stored. We strongly recommend for performance and recoverability that you do NOT encrypt using Retain but consider Block level encryption options (such as BitLocker) that have escrow keys and are processed directly at the operating system level.



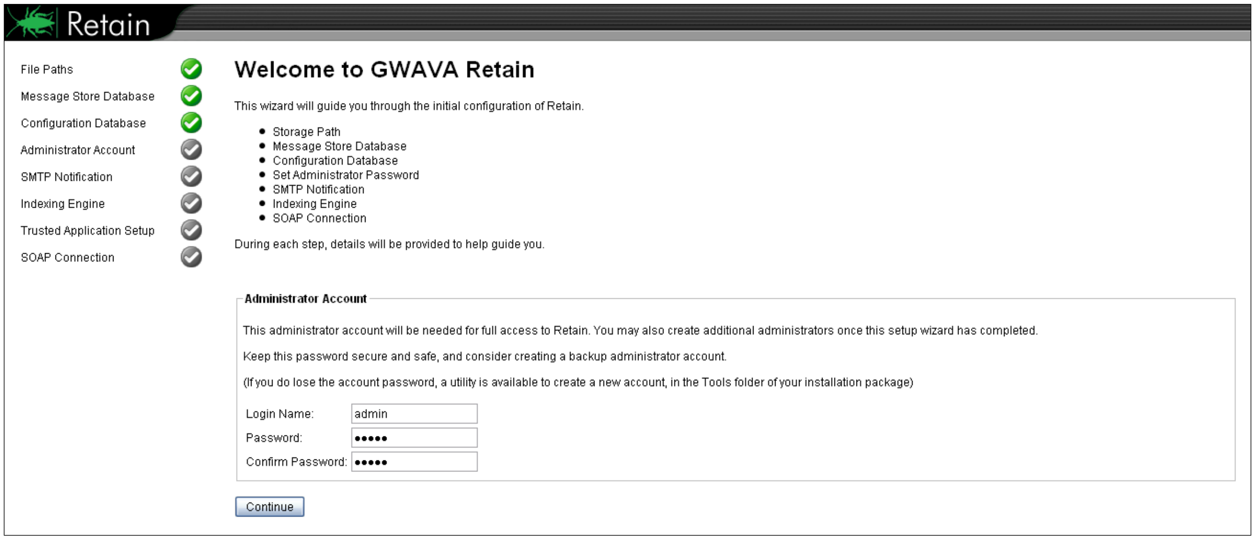
Database Setup



6) Next, this screen appears for entering the database connection parameters. This is the same information from the database created during the preparation phase. (See Install guide) The connection information must be supplied for both the storage and Configuration databases, though they can be housed in the same database. Assumed default is shown.

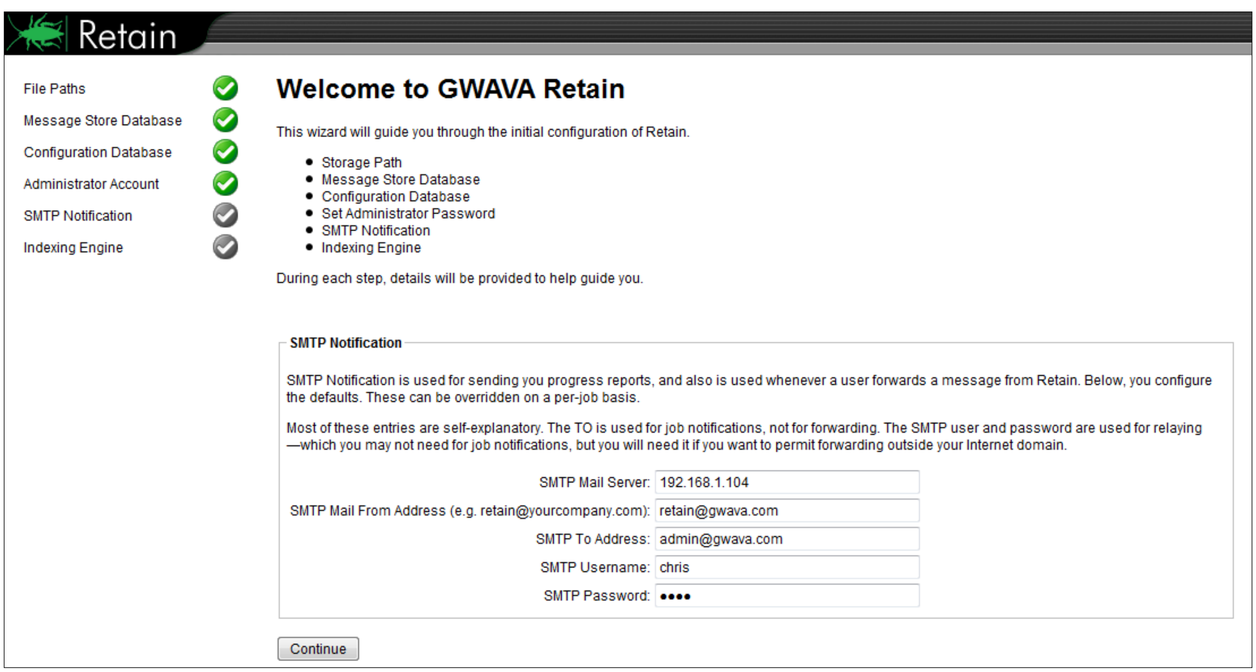


7) Now, supply a password for Retain's administrator account (admin). **Do not forget what you choose here!** (Use the Recover Admin utility if you have lost the administrator password.)

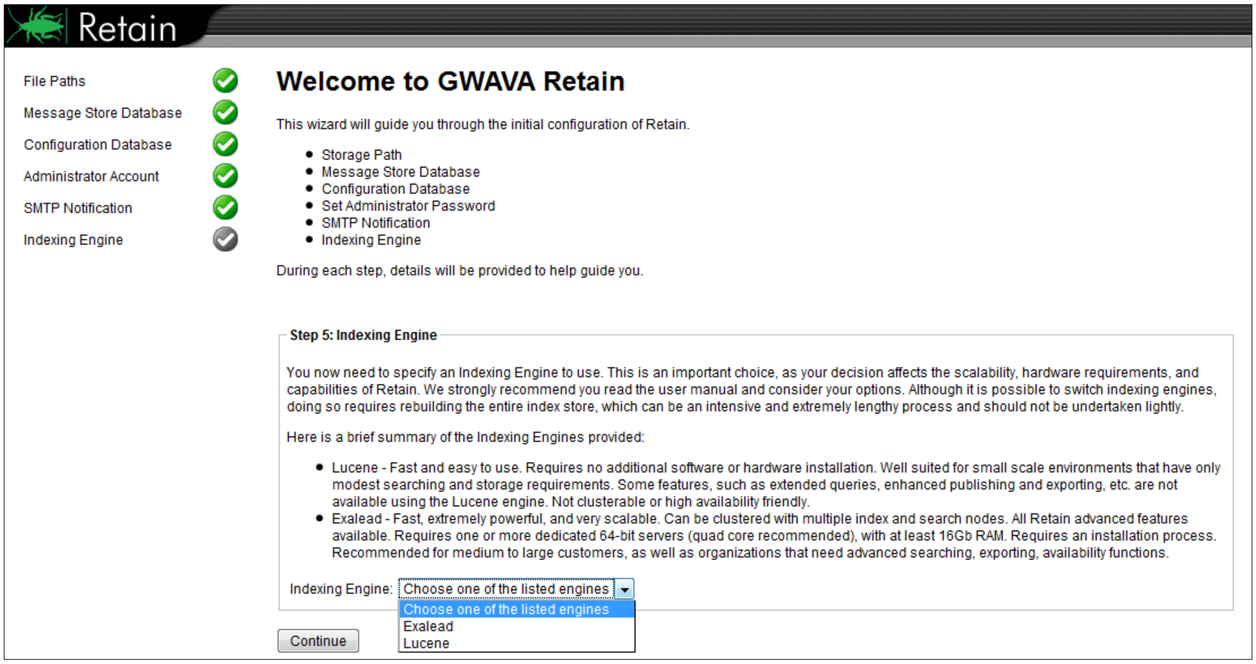


NOTE: Retain allows the creation of many user accounts that share administrative roles. The initial account created is not particularly special; it's merely a convenience to create one "super user" with all of the Administrative rights granted. DO NOT delete this account. If the admin account is deleted, please contact support or refer to the Recover Admin tool to restore a full administrator account.

8) Enter the information for an SMTP relay host that Retain will use to send mail. Setup will attempt to send a test message. You cannot proceed with installation until the SMTP test message is successfully delivered. If you see an error, check firewall settings, (including local desktop/server firewalls such as McAfee, Symantec, and SUSE).



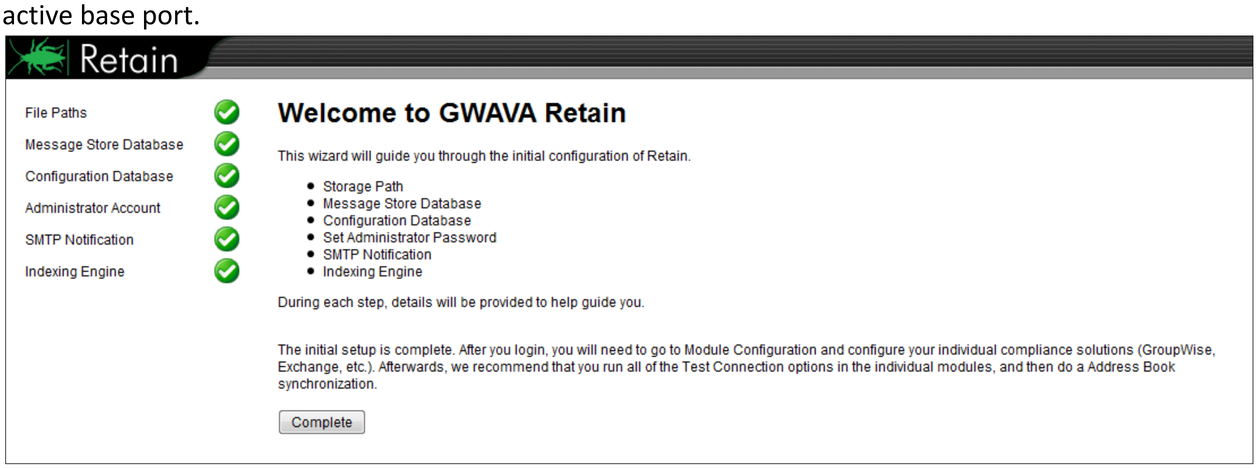
9) Index Engine Selection



➢ Lucene is the default indexing engine, and is included in Retain. It is well suited for smaller installations and requires no further configuration or management.

➢ Exalead is a more robust and powerful search engine, providing high availability and clustering features, as well as more advanced search operations. It requires additional hardware, as well as an additional license, which you may obtain from your sales representative. **Exalead should not be installed on the same server where Retain server is installed.**

If you wish to use Exalead at this point, it MUST be installed and configured before this step is completed. If selecting Exalead, provide the IP address or DNS name of the Exalead server and the active base port.



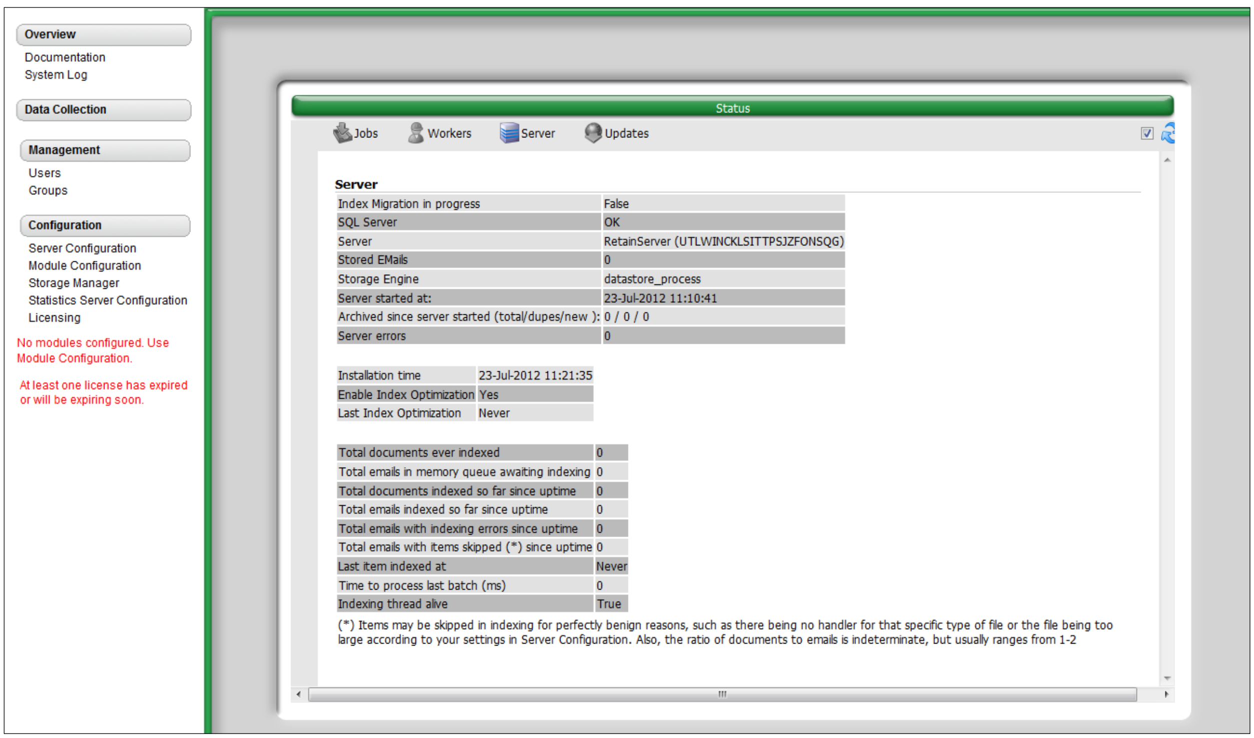
Initial setup is now complete. Select the 'Complete' button to be presented with the login prompt.

Setting Up GWAVA Retain

Logging In

1) From your web browser, type: http://<YourServerIP/RetainServer
2) You'll be brought to the login screen:

3) After you log in, you will see the main administration page: (Non administrators will only see the Search Interface.)



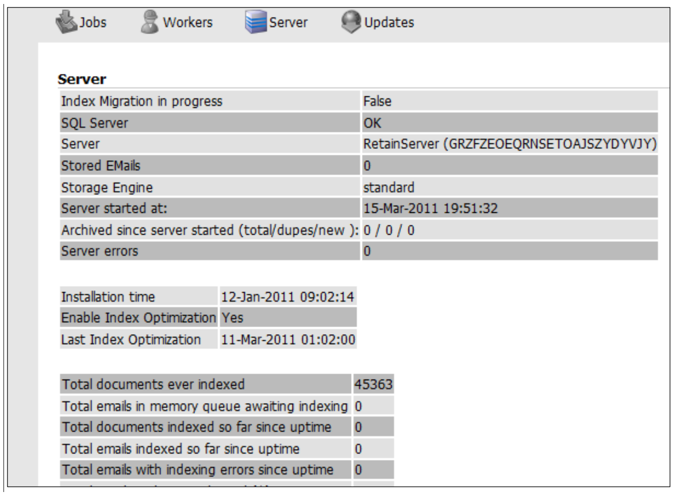
An informational screen is displayed, showing among other things the latest job activity, server health information, and software updates that are available.

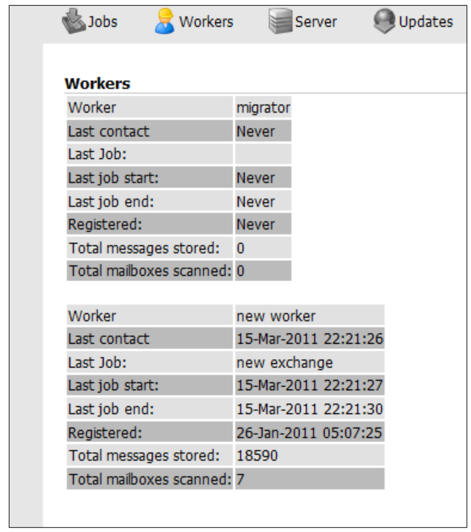
Note: Only users possessing at least one administrative role will see the administrator's screen on login. Other users will be forwarded to the Search Interface (covered later).

Status and Updates

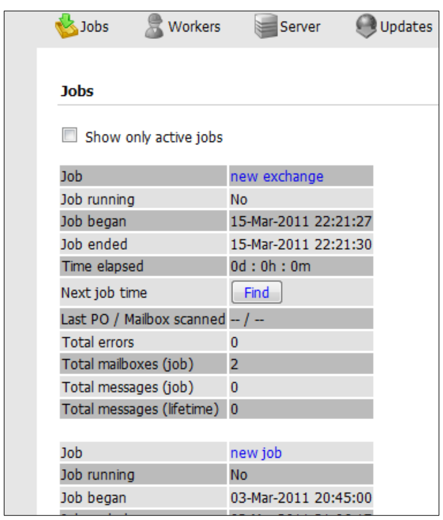
The status page has four different tabs which show the status of your system. The status page is set to display the tab that is deemed to require the most attention, or is deemed to hold the most important information at a given time. For instance, if an error has occurred, that tab will be shown, likewise the update tab will be shown by default if there is an update available. The tabs are discussed below.

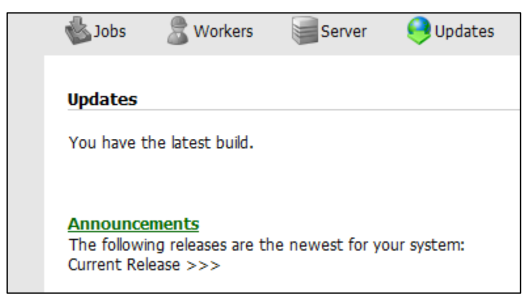
The Server tab shows the basic status of the Server with the messages archived and maintenance information. The Workers tab shows the workers connected, and the status of each.





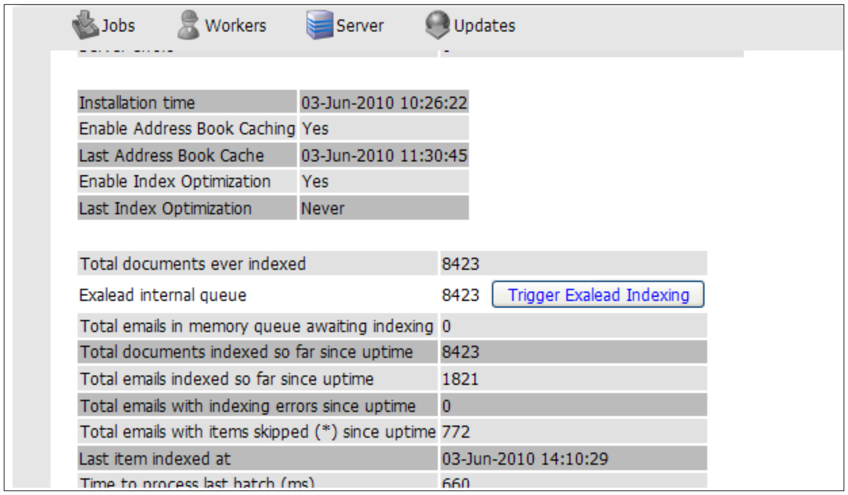
The Jobs page shows the jobs that are assigned to the server and their status. You also can select the "show only active jobs" checkbox, and only jobs that are currently running will be displayed.





The updates tab displays whether there is a later version of Retain available. This tab will be displayed by default only if there is a new update available.

If you are using Exalead as your indexing engine, you will see a 'Trigger Exalead Indexing' button on the 'Server' tab of the Status and Updates page. Selecting this button will force an immediate indexing run by Exalead.

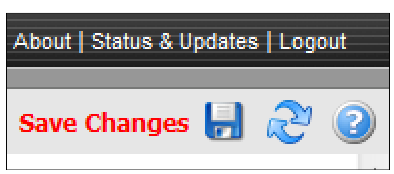


After many messages are sent to the Exalead server for indexing, these items are queued. In some cases, there may be a noticeable delay in the processing of that queue, as other processes (such as searching) take high priority. To force an immediate indexing run, press this button.

Warning: Repeatedly using this button can overwhelm your Exalead server, and should NOT be necessary in normal operations.

Saving Changes

Retain uses a web interface for all administration, and is unaware of changes made on the webpage until the information is returned to the Server. To make sure you keep all changes you have made in the interface, select the "Save Changes" button to commit the change to the Server. When you make a change, the website is aware and you will see the 'Save Changes' button become colored at the top right of the screen:

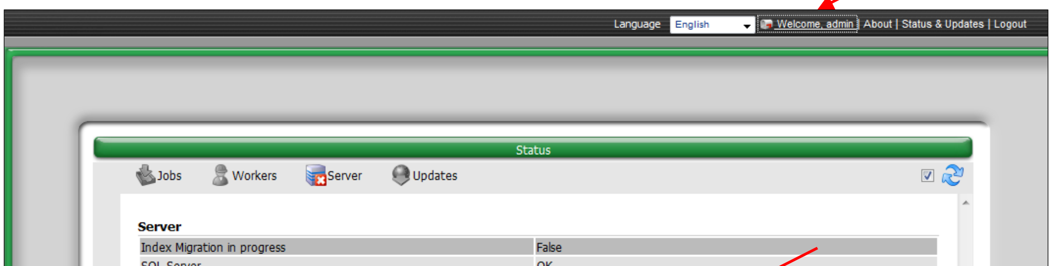


When the "Save Changes" lights up, click on the disk icon to save any changes you have made on this screen otherwise your changes will be lost.

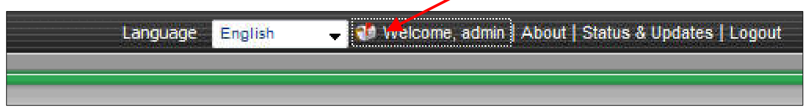
Notifications

Notifications are automatically sent to the administrator whenever data in Retain is moved. Moving data consists of system migration, exporting, forwarding, restoring, and publishing. By default, the address used is the address supplied during severs activation.

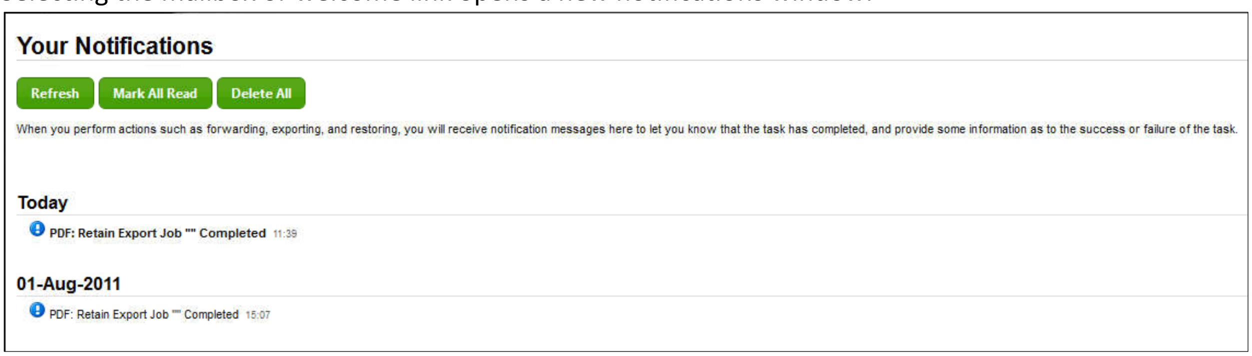
To spawn the notifications page, click on the 'Welcome' link at the top of the page.



When notifications are pending, the red flag on the mailbox is lifted.

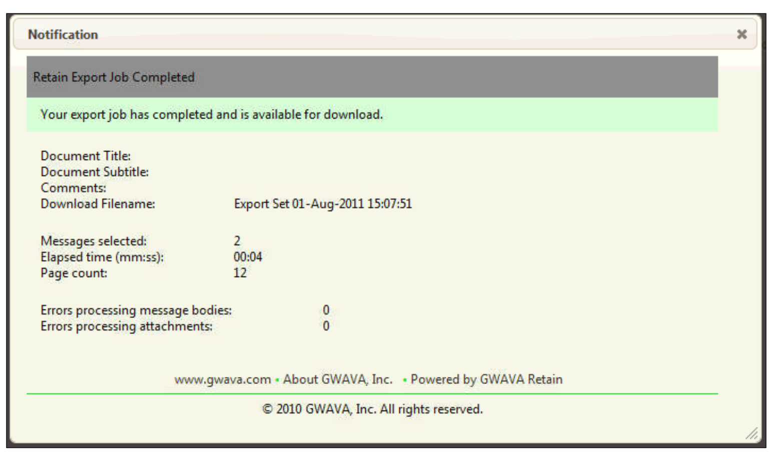


Selecting the mailbox or welcome link opens a new notifications window.



The highlighted notifications are new, unread notifications and events. Selecting the event notification provides all the pertinent information regarding the event.

If there are any errors, a truncated error log is provided which details the error and the reason for the error.



Modules

Retain integrates and works with several different message systems. Data collection will not be available until one or more modules are configured for the Retain system.

<u>Note</u>: Depending on what license you have purchased for your Retain system, different modules may require an additional license. Check the licensing page to see what licenses you own. An Evaluation license, issued upon initial install, lasts 30 days and grants licenses for all modules

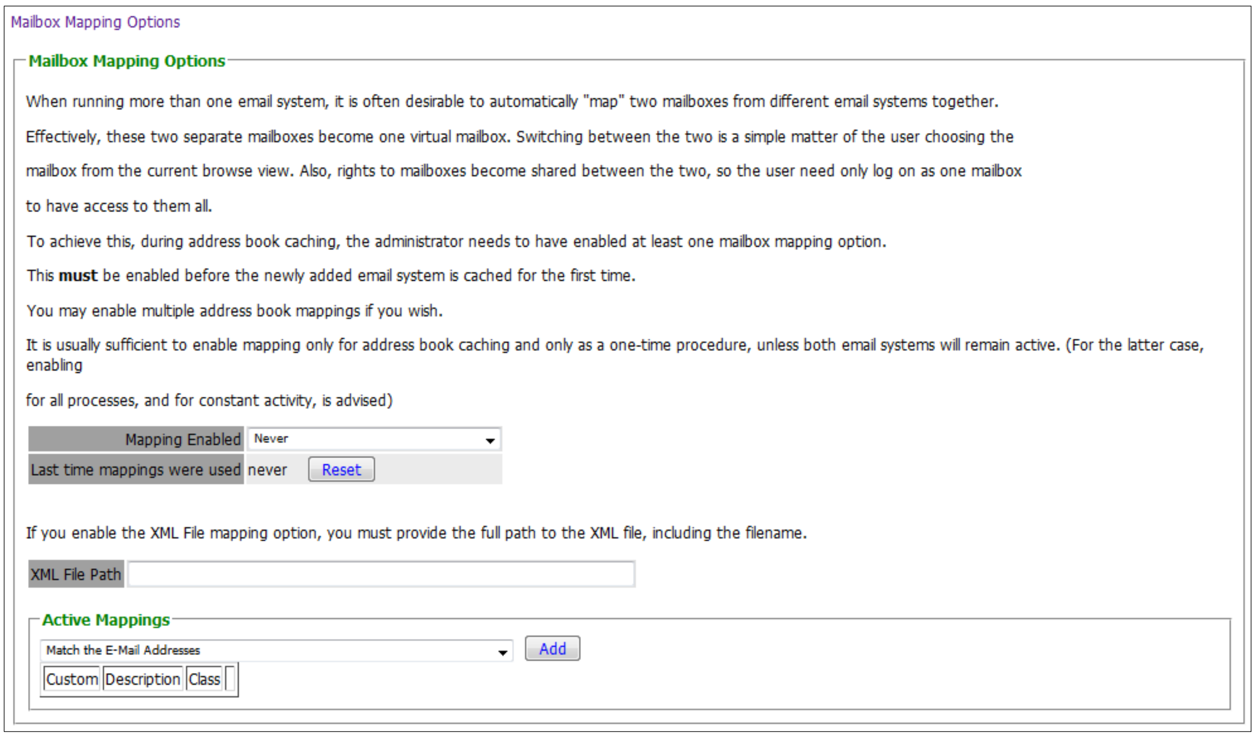
To configure a module, select the 'Module Configuration' page from the Configuration menu.

Each module link will open a new configuration window or tab. If the modules are not configured correctly, messages will not be collected. Profiles and Jobs are separated into module specific sections and no jobs can be configured without first configuring a module. Select the appropriate module(s) for your system by clicking on the module icon.

Certain settings or actions for both Exchange and GroupWise message systems must be configured before Retain can communicate with them. Make sure to complete or check the following changes and settings for each system before continuing. (Links lead to sections in the appendix.)

Mailbox Mapping Options

Mailbox mapping automates the merging of users' mailboxes that have both GroupWise and Exchange accounts, combining the GroupWise and Exchange archives under the same user in Retain. Retain merges the internal UID's of accounts to reflect the same user. **After mailbox mapping has been activated, an immediate caching of the address books of both systems is required. Mailbox mapping is not permanent; however, "un-merging" must be performed manually via the Mailbox Merger / Splitter tool found on the 'bug' or 'about' screen**. If a refresh of the mailboxes is not performed before users attempt to login or other activity is present on the server, the merge may fail, leaving extra entities created in the Retain archive which must be removed manually. Furthermore, the merge option is a once-off option. Please contact support for further options.



To map one mail system to another, both message systems, Exchange and GroupWise, must be functioning and have the desired accounts created on the system which allows for identification of the different users.

Accounts may be matched via email address, display names, or specified by an administrator supplied XML file. The Address book MUST be refreshed immediately in order to merge the users. The merge will not complete unless the Address Book is cached afterwards, and the merge cannot be re-run.

How the merge runs depends on the different users in the local system. If both message systems are to remain active, with users being added and removed from the system, it will be necessary to have mailbox mapping on all the time. Merged addresses are also required for the GroupWise to Exchange migration to function.

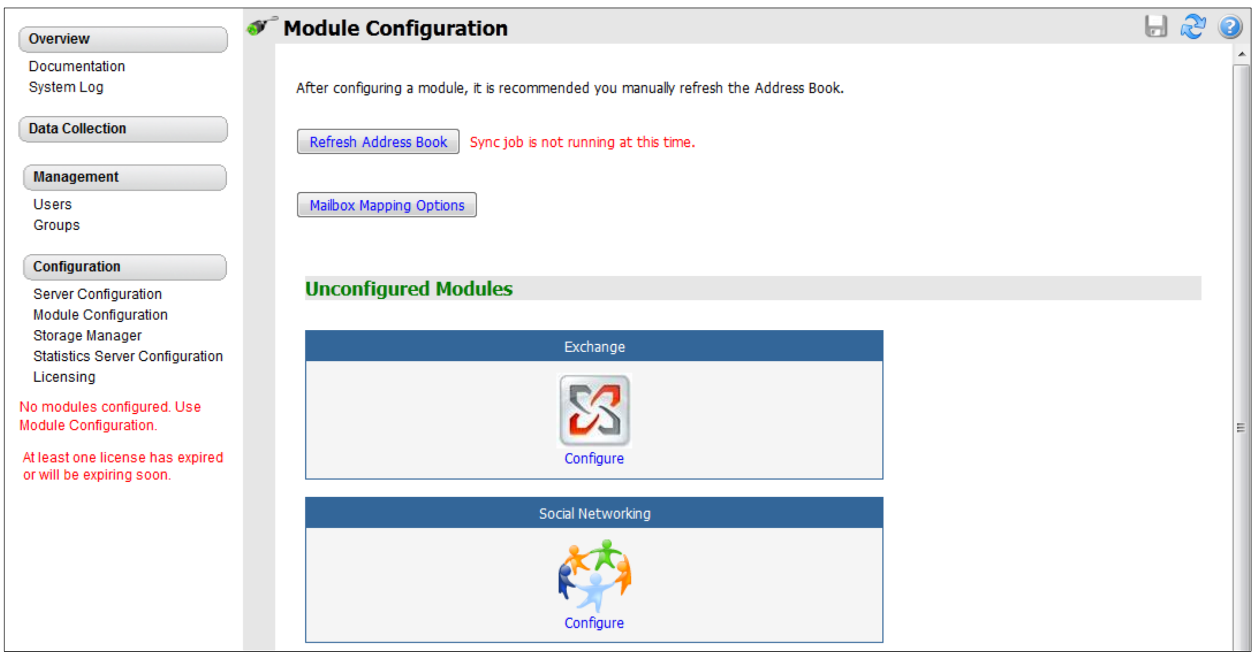
Exchange Module

Retain supports:

- A single forest Active Directory system, (Exchange and standard users)
- An Exchange Resource Forest, (One Exchange Forest linked to one or multiple User Forests)
- Office 365

Retain does NOT support multiple linked Exchange Forests. Ensure that the Exchange settings have been configured correctly before continuing the Exchange module setup.

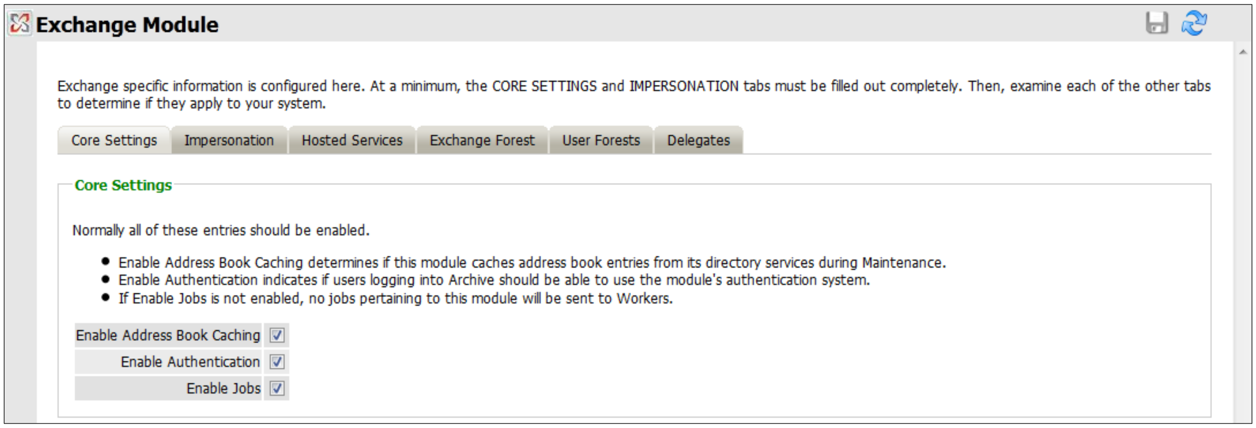
The Exchange module must be configured in the Retain Server before any communication between Retain and an existing Exchange message system can occur. Open the Retain management page on the Retain Server, and select Module Configuration.



Select the 'Configure' option in the Exchange module. A new window or tab will open with the module configuration.

NOTE: Ensure that your Retain Server DNS is set to the same DNS server that your Exchange server uses. The Exchange module uses these DNS setting to auto discover critical information about Exchange stored in Active Directory and will not function correctly unless both systems are pointed to the same DNS server.

Core Settings



Normally all of the checkboxes on this tab are always left selected. It is rare that you would ever deselect any of them. Two cases where you might would be troubleshooting, (as instructed by Technical Support), and retiring an old email system.

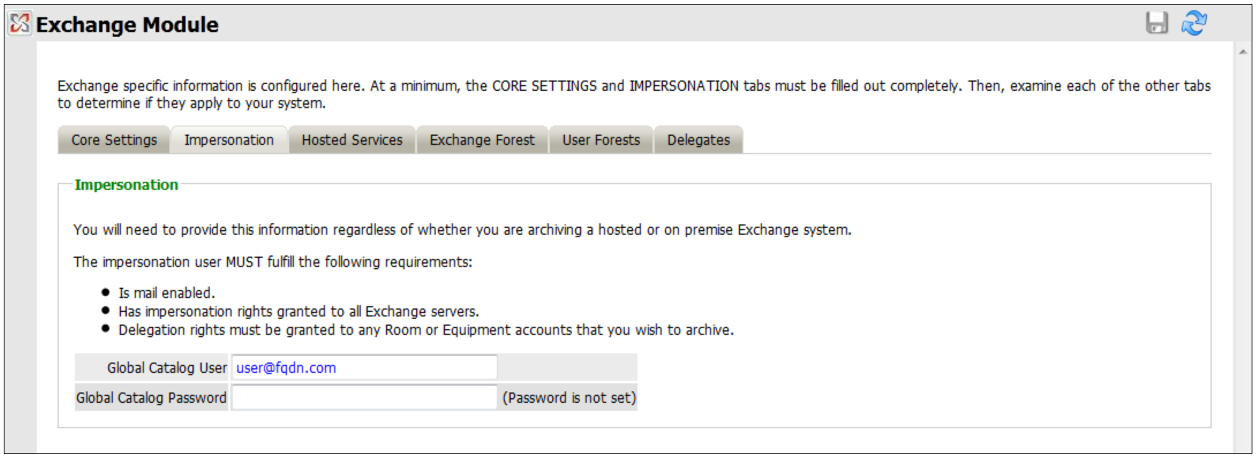
The Enable Address Book Caching function allows Retain to regularly cache the online email systems address book and synchronize it with Retain. This is critical for administration, authentication, and archiving purposes. It is recommended to cache the Address Book once every 24 hours to keep the Retain storage system up to date. By default, maintenance is set to cache the Address Book once every 24 hours.

The Enable Authentication checkbox determines if end-user authentication is performed when the user logs into Retain. If it is deselected, the Retain system will NOT authenticate the user against the email system and the user will not be able to log in unless another authentication method is enabled.

The Enable Jobs checkbox determines if configured data retrieval jobs are ever passed to the Worker. Even if the individual job is fully configured and enabled, if this checkbox is switched off, no jobs configured for this module will be processed.

Impersonation

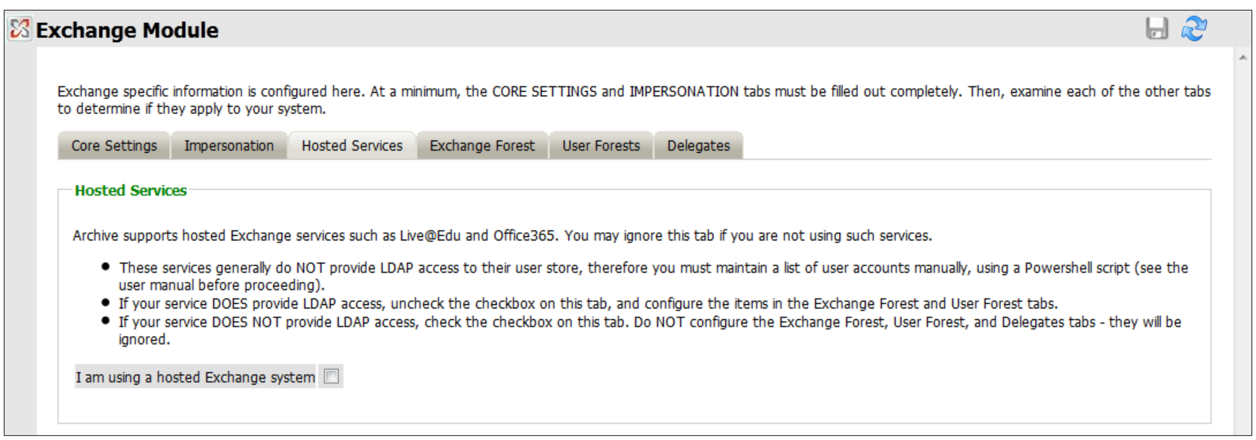
If the Impersonation and Core Settings tabs are not completely configured with the correct information, the hosted system will not be archived correctly.



Hosted Services

If the Exchange system is a hosted service system, Retain must be configured to support the hosted system setup.

Setting up the system is no more taxing than setting up a normal system, though a hosted system requires that the Impersonation and Core Settings tabs are completely and correctly filled out. Other tabs are only applicable depending on the settings of the hosted system, configure as appropriate.



Mark the checkbox to enable Retain support for hosted Exchange services.

IF the hosted system in use is an Office 365 system, further configuration on the Office 365 system is required. Because Office 365 Exchange Servers do not directly expose LDAP information, a Powershell script must run periodically to cache user and group information.

The Script requires PowerShell 2.0. Without this script, you cannot run jobs on Office365, or authenticate users.

Setup

1. Install PowerShell 2.0 (not needed for Windows 7 or Windows Server 2008 R2)
2. Install the Office 365 PowerShell cmdlets
3. Allow PowerShell script execution
4. Adapt and execute the “sync365.ps1” script provided by GWAVA
5. Automate the script to run regularly.
6. Place the two resulting csv files in Retain

1. Install PowerShell 2.0

The appropriate version for the Windows system can be found here:
http://www.microsoft.com/powershell

Windows 7 and 2008 R2 already come with PowerShell 2.0
(Even if the version says 1.0, really it’s 2.0)

2. Install the Office 365 PowerShell cmdlets

The cmdlets can be found here:

http://onlinehelp.microsoft.com/en-us/office365-enterprises/hh124998.aspx

Two setup files are needed from that page:
- Microsoft Online Services Sign-In Assistant
- Microsoft Online Services Module for Windows PowerShell

Execute them both in above order.

3. Allow PowerShell script execution

The Default Execution Policy is set to restricted, it can be viewed by entering this command in PowerShell:
Get-ExecutionPolicy

The script provided by GWAVA must be run in PowerShell while **running under Administrator rights**.

Set-ExecutionPolicy RemoteSigned

4. Adapt and execute the “sync365.ps1” script provided by GWAVA

Select the “sync365.ps1” script provided by GWAVA in Tools/Exchange/Office 365 folder.

Right click on the script and select “modify”.
This will open the script in the Microsoft Integrated Scripting Environment (ISE) editor.

At the top you can find 3 settings: $User, $PlainPassword, $ExportBasePath.

- Set $User to the UPN of an administrator account in Office 365.
- Set $PlainPassword to the plain text password of the administrator account.
- Set $ExportBasePath to a directory where the two resulting csv files will be saved. If the path does not yet exist, it must be created manually as the directory will not be created automatically.

Keep in mind that your backslashes must be quoted, and a final backslash is not needed.
Example:
$ExportBasePath="C:\\Temp"

Note: If it is unacceptable to set a password in clear text, please view the following solution:

http://bsonposh.com/archives/338 -presents an alternative, which loads and saves encrypted credentials from file.

Execute the script by clicking the play button. This process can take a while for many users. Once the script has completed, a message indicating that the script is done should be displayed along the bottom status bar.

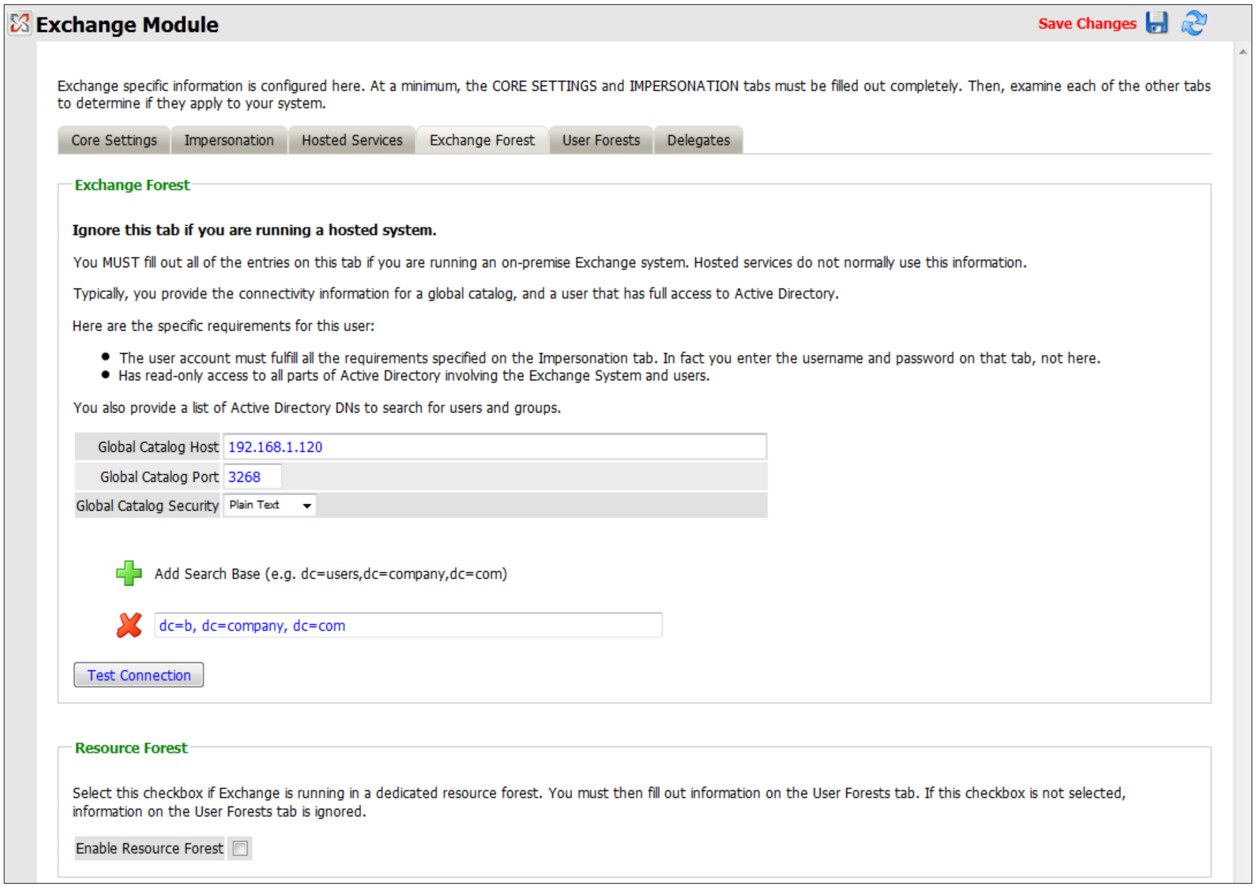
5. Automate it: to run automatically with Task Scheduler at least once a day

The frequency of automation is up to the administrator. However, the script needs to be run at least once a day, and, due to step 6, the files need to be copied to the Retain Server. To see how to utilize task scheduler to automate the script, see http://support2.gwava.com/kb/?View=entry&EntryID=2409

6. Get the files over to Retain Server

In Step 4 the ExportBasePath was set and should contain the two csv files. These files must be automatically copied to the RetainServer/WEB-INF/cfg directory once the script completes. That might require setting up a mapped network drive, or the acceptable solution for the local system. While the ExportBasePath may be mapped directly to the Retain Server, it is recommended to have the csv files copied afterwards.

Retain needs to know login information and existing domains before any archiving can be accomplished. Open the “Exchange Forest” tab and enter the login information.



Retain uses Active Directory extensively when integrating with Exchange. Its uses include: populating the address book, authentication, and access to the Exchange System.

There are settings required for Exchange, see the Exchange settings section in the appendix.

On the Exchange Forest tab, you configure all of the Active Directory information you need for an Exchange forest. There is no need to fill out any information on the User Forest tab unless the users exist in a separate forest from the Exchange Forest.

On the Exchange Forest tab, specify whether to use SSL or not for the Global Catalog Security, (strongly recommended), and the "search base". The search base is the LDAP path to the base of where Retain will start searching for valid Exchange users.

The Global Catalog Port defaults depend on whether SSL is used for security or not. SSL is STRONGLY recommended. (Default ports are 3268 for plain text, and 3269 for SSL.) Adjust as appropriate for your system.

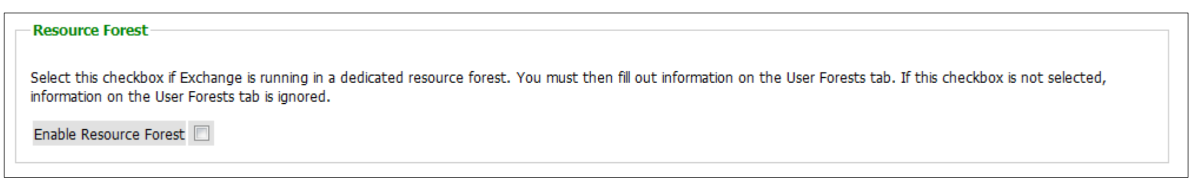
You also must provide the credentials of an Active Directory user. This user is "special" It must have full read rights to Active Directory, be a mailbox-enabled, user, and be granted various Impersonation and Delegation rights. More on this is discussed in the Exchange settings section in the appendix. The username MUST be in UPN format, (user principal name).

This search base, in LDAP form, must be "high enough" in the tree to include ALL users, groups, and servers. Multiple search bases can be specified, though it often results in a less efficient interface. These are LDAP search bases which allow Retain to resolve all users, groups, and servers of interest in the forest.

After the Search Base has been added, test the connection to ensure information and connection works. The test performs a simple login to confirm that the user exists, the Exchange Server is reachable, and that the credentials are accepted. The test does not confirm impersonation or delegation rights necessary for the Service Account.

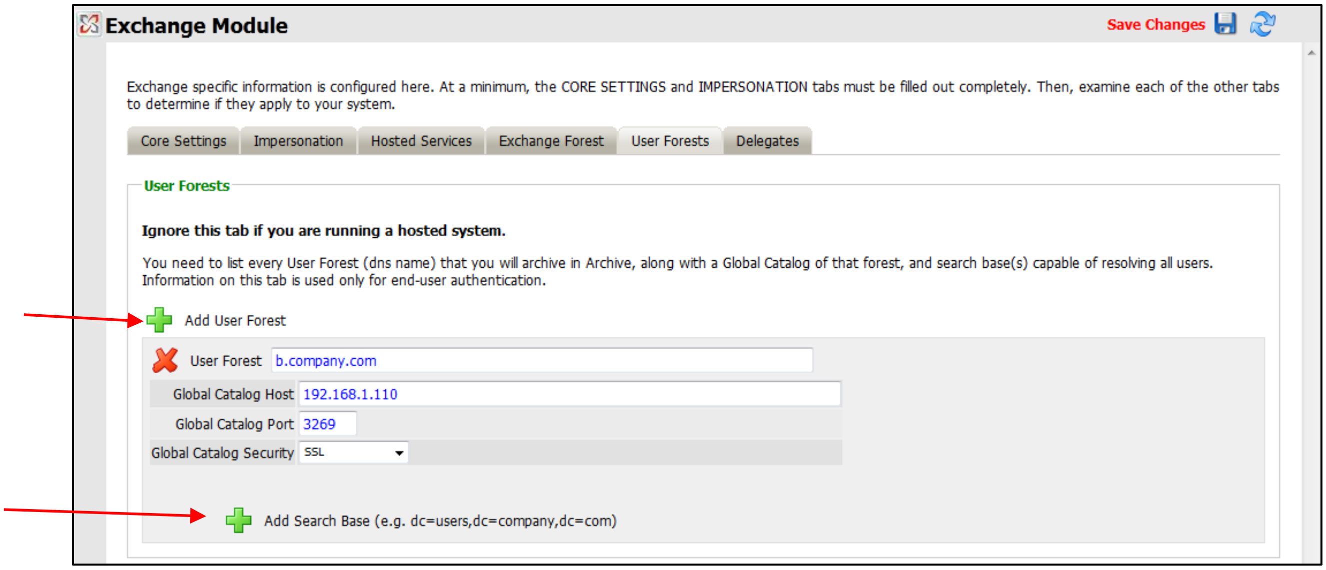
If the test results in an error stating: "FAILURE: User doesn't exist or is not mail enabled," It indicates that the user's mailbox is unavailable. A mailbox is not required for Retain to utilize the specified user. If the user Retain utilizes does not have a mailbox, this error may be ignored. However, if the user specified does have a mailbox, this may indicate connection issues.

The Exchange Forest tab is the only tab required by the Server and the Worker to archive mail from the Exchange system. The User Forest tab, however, is required for Exchange systems utilizing a resource forest, to allow the end user to log into Retain.



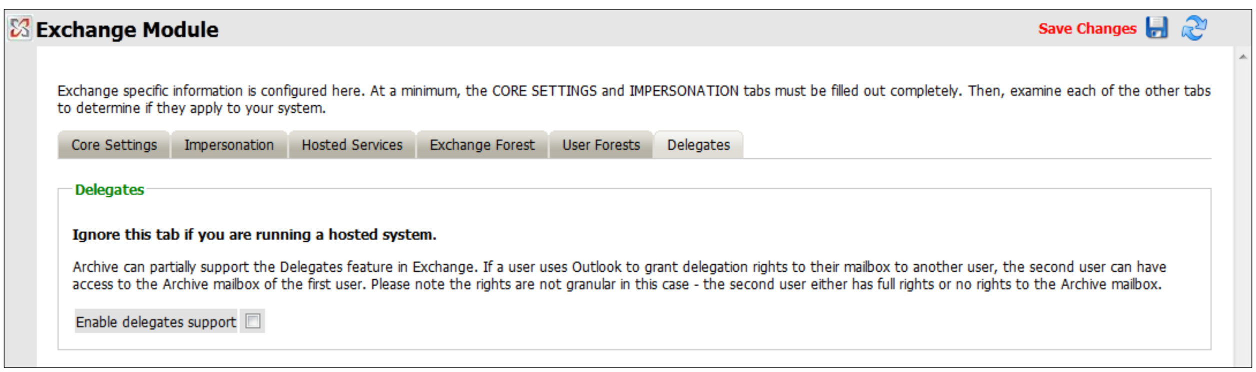
If the system contains a Resource Forest, enable the checkbox on the Exchange Forest tab and save changes. If the Resource Forest checkbox is not enabled, the User Forests tab will be non-functional and all settings contained on that tab will be ignored. The checkbox must be unchecked in a single forest Active Directory deployment, but must be checked in a multiple forest Active Directory deployment.

Check all information to ensure that it is correct and save changes, and then configure the User Forest if required.

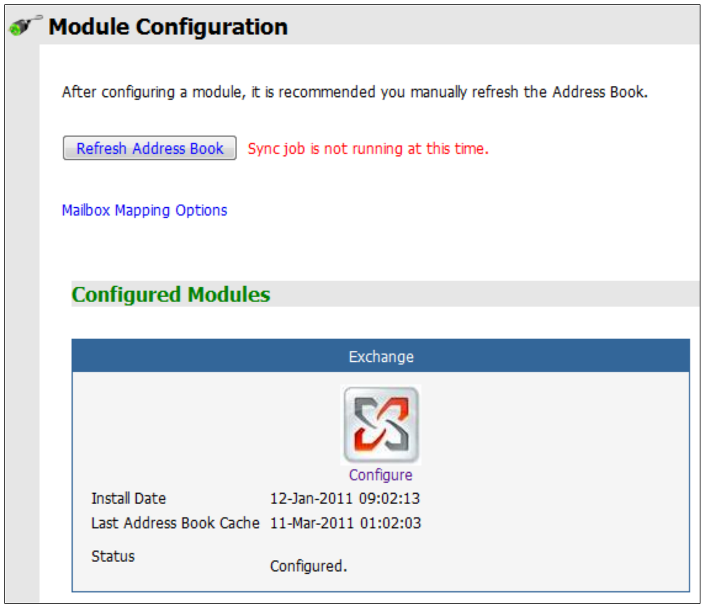


The User Forest must have an entry for each user forest attached to the system. Select the green '+' button and input the LDAP information required by the Forests' Global Catalog server: IP address or hostname, port, security, (SSL is STRONGLY recommended), and all search bases to include all the users. No administrative credentials are required. Each end user's provided credentials will be used on login.

Save all changes before closing the Exchange Module page.



After saving changes, return to the Retain server Module Configuration page, and trigger a refresh of the Address Book.



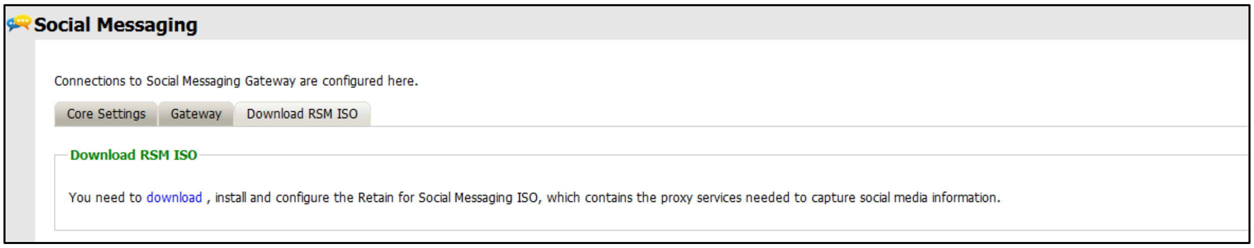
Depending on the size of the address book, it may take several minutes to return with information, but a successful configuration will return a correct address book cache date and no errors. The date should reflect the date of when the address book refresh was triggered.

The Status may show “Address Book Cache Never Run” or may list commonly misconfigured or missed items if the Refresh job fails.

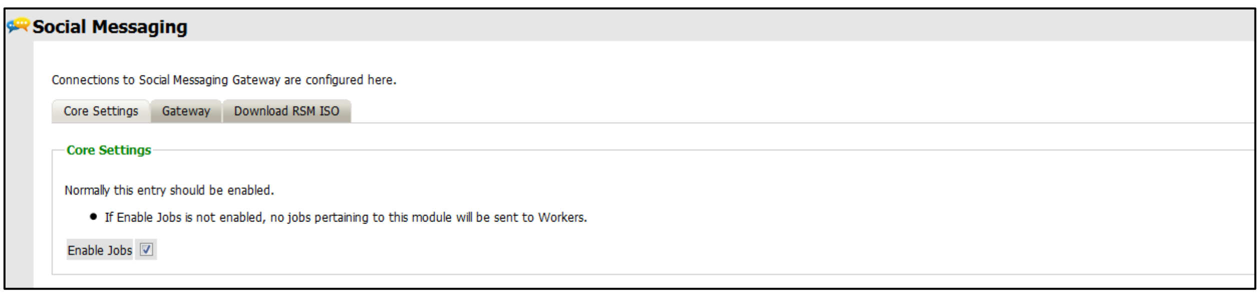
Once the status is ‘configured’ and the Address Book has been cached, Retain can connect to and archive messages from the Exchange server. The system is ready to have workers, schedules, profiles, and jobs configured, and those options will now appear on the main administrative interface.

Social Messaging

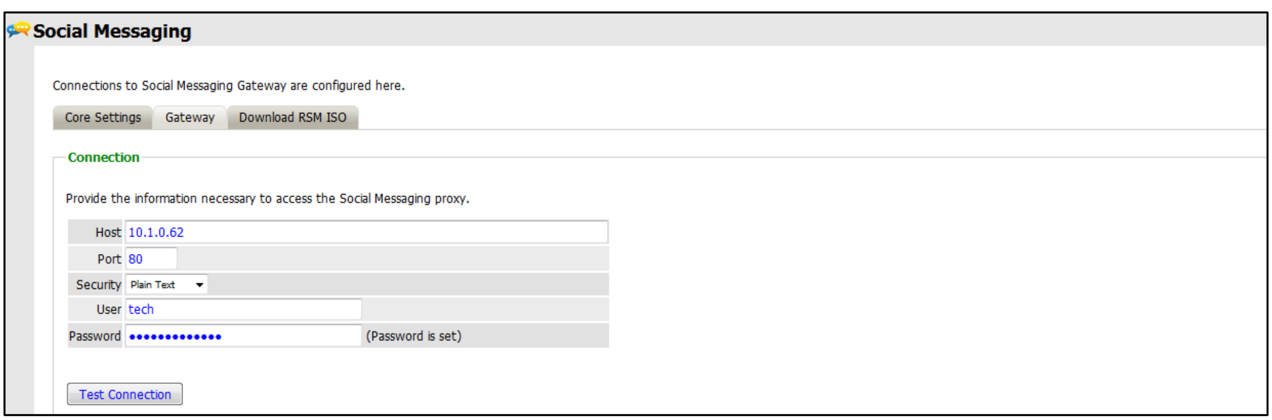
The Social Messaging module allows Retain to archive Social Messaging communications from Facebook and Twitter. To configure the Social Messaging module, all that is required is to provide the connection information and address to the Retain for Social Messaging Gateway. If the RSM Gateway is not yet installed or available, a direct download link is provided on the last tab.



The “Enable Jobs” box must be checked to have any jobs function against the RSM Gateway. See the Retain for Social Media installation guide for more information.



On the Gateway tab, the connection information must be filled-out. Either place the host name or the IP Address of the RSM appliance and the connection port for the administration interface. Default is shown.

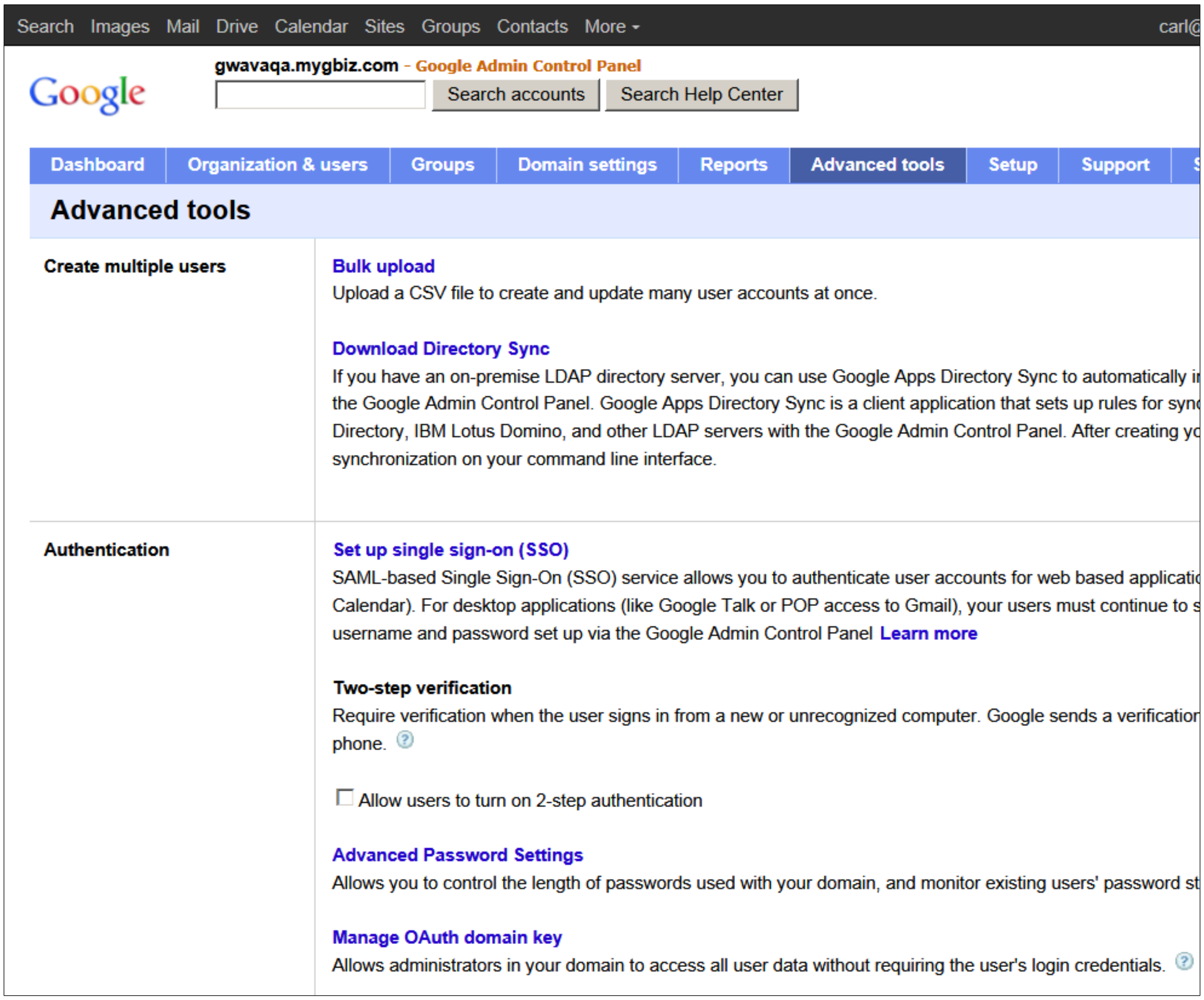


Security and user login credentials are required to connect to the RSM. The user must have administration rights to gather data from the Gateway. By default the user account is ‘tech’ with the password ‘retain’.

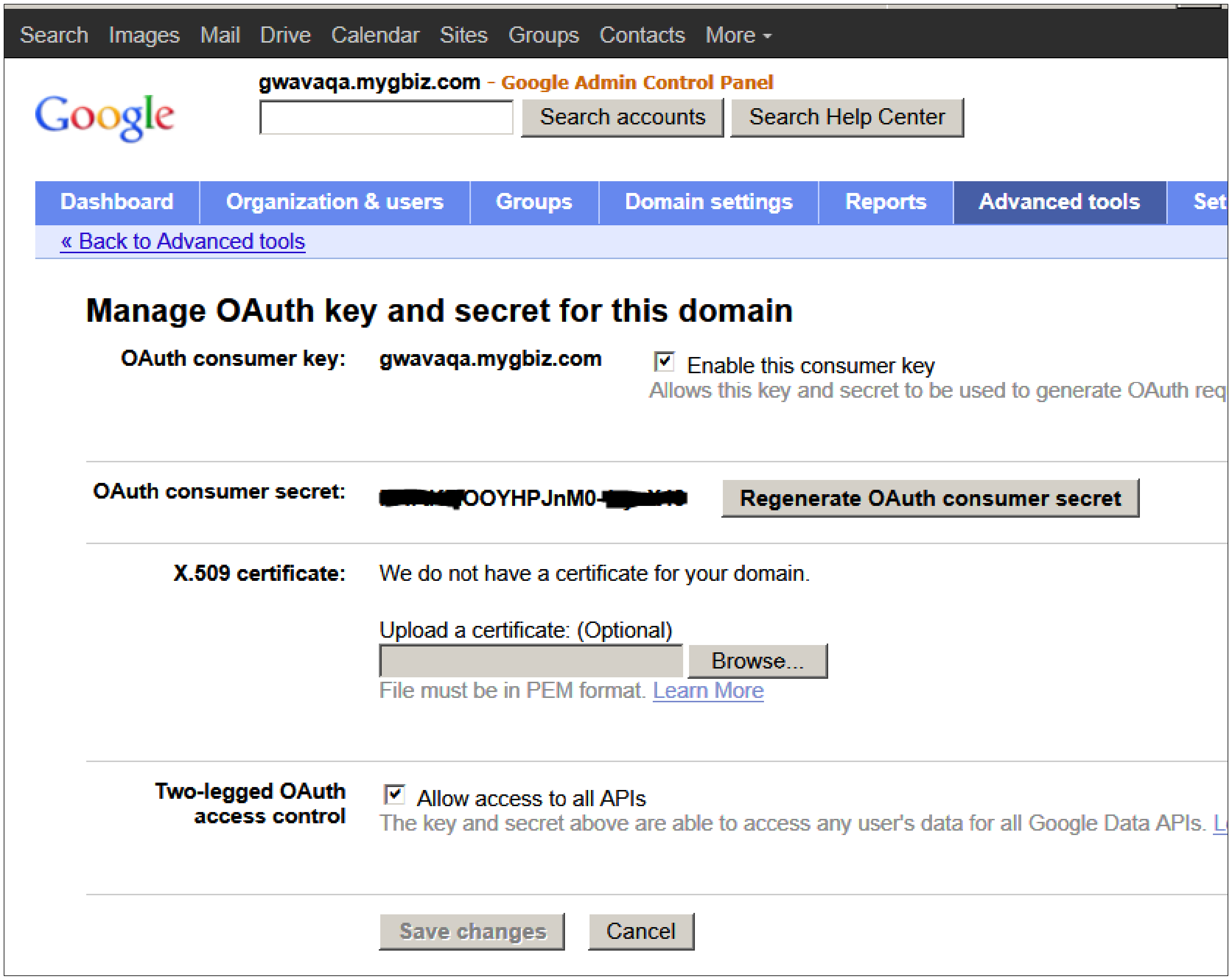
Save changes and the module is configured.

Google Apps Module

The Google Apps module allows Retain to archive Gmail data items from Gmail. To configure Retain for Gmail archiving, Retain needs Gmail to be configured to allow Retain access, and the appropriate information entered into Retain.
To Configure Gmail for Retain access, login to the Gmail Admin Control panel and select 'Advanced Tools.

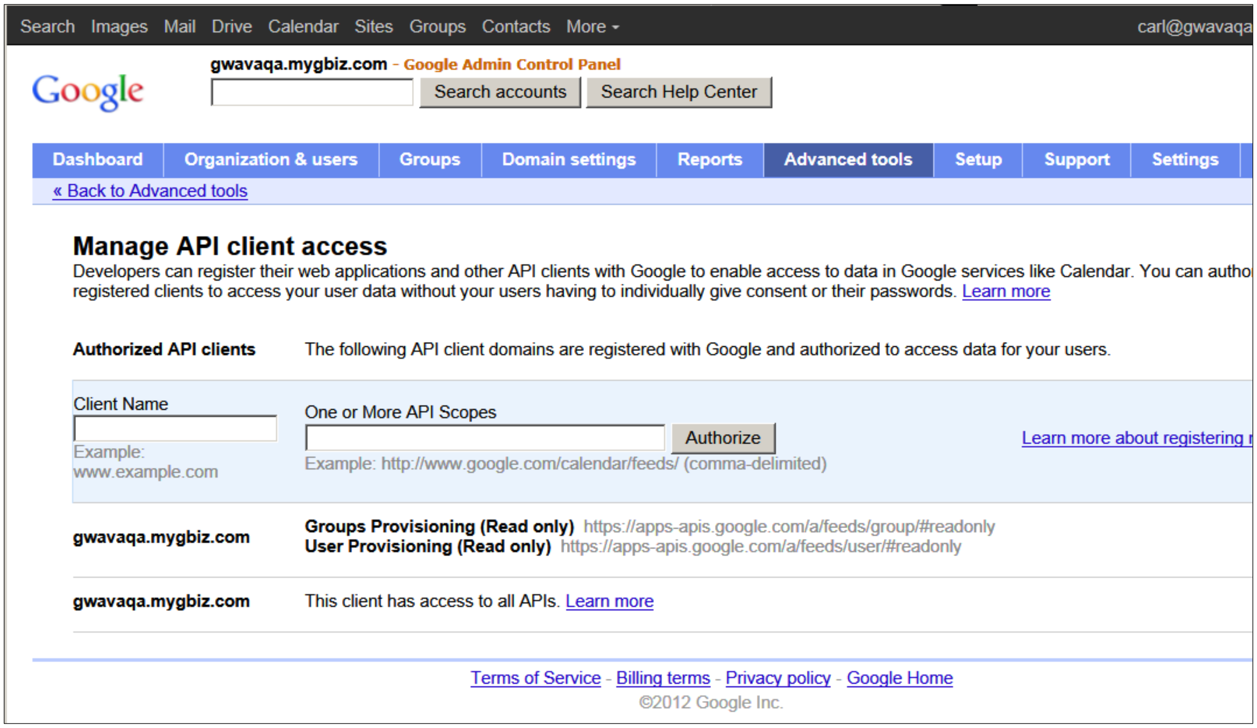


Under the “Authentication” section select “Manage OAuth domain key”



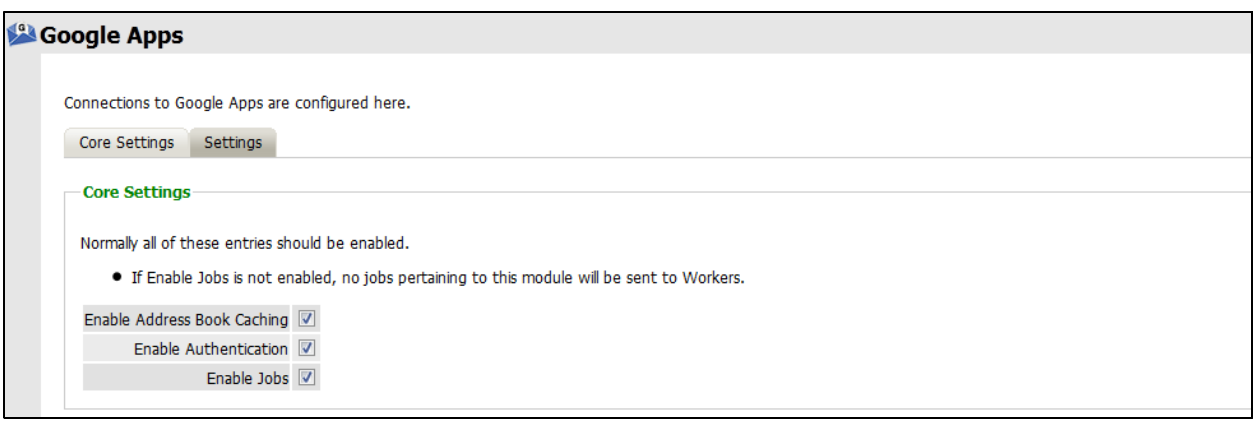
Make note of the OAuth consumer secret and check the “Two-legged OAuth access control” checkbox to allow access to all APIs. This is how Retain will be able to access Gmail.
Click “Save changes”.

Click again on “Advanced tools”, then on “Manage third party OAuth Client access”

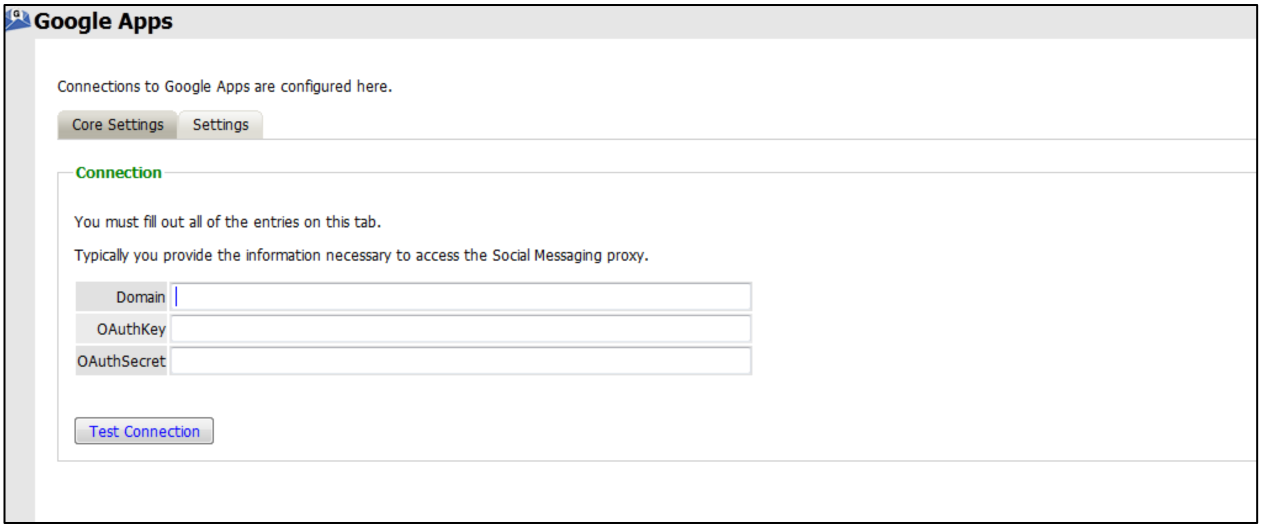


In the client Name field enter the name of the Gmail domain. In the “One or More API Scopes” field, enter this:
https://apps-apis.google.com/a/feeds/group/#readonly, https://apps-apis.google.com/a/feeds/user/#readonly

Click the “Authorize” button.
Once authorized, the Google Apps module can now be configured.



Address book caching must be enabled to gather and maintain an updated list of users. Authentication is used to allow access to the Retain message store for users based on their existing Gmail account. If the Enable Jobs option is not enabled, no jobs may be completed with the Google Apps module.



In order to connect to the Google system, Retain requires the domain and administrator login information. Retain archives the Gmail system through IMAP, and will login and download the message data to the Retain data store.

Test the connection to ensure that the configuration has been completed correctly.

Jobs and profiles for Gmail will not be visible until the address book has been cached. After the module has been cached, all configuration options for profiles, workers, schedules, jobs and data storage will be enabled and visible.

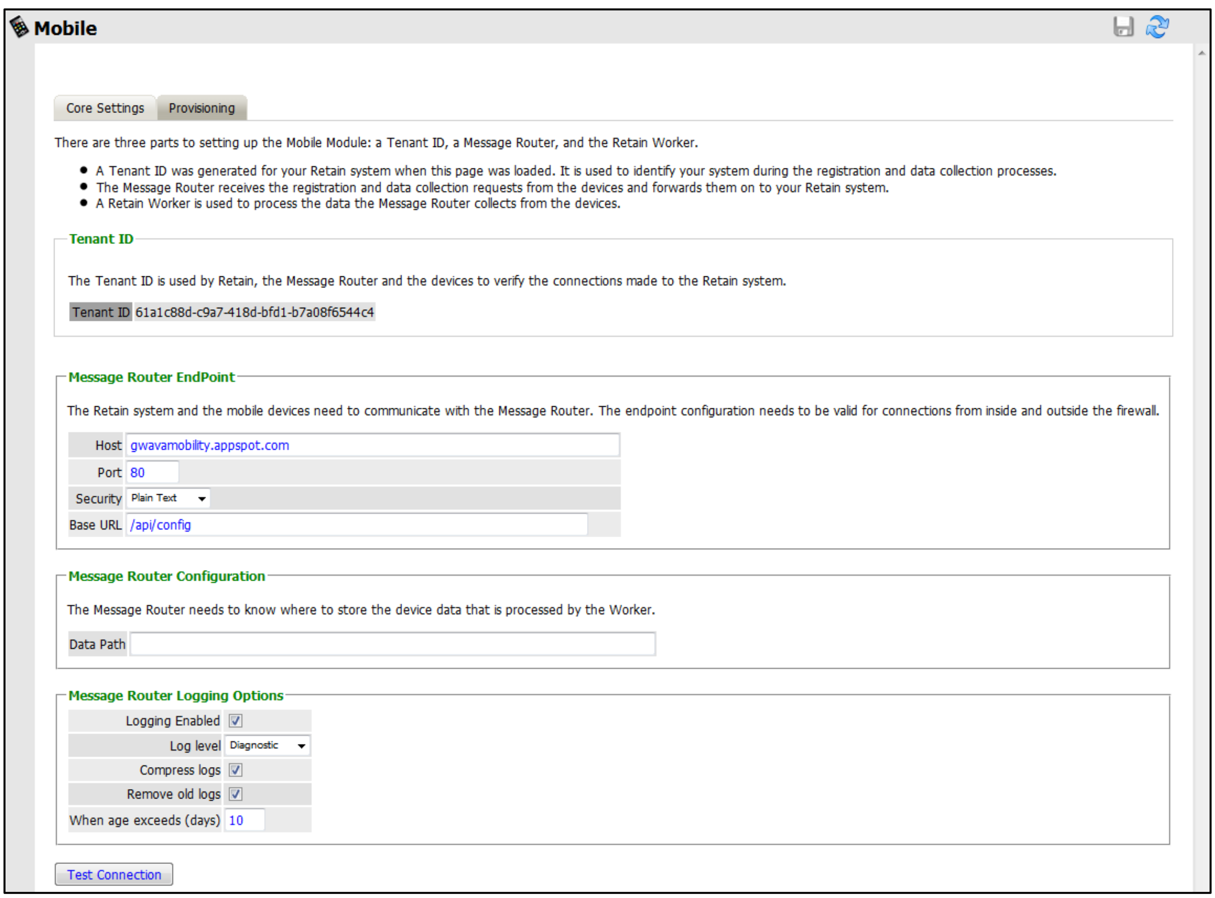
Mobile Module

The Retain for Mobile module allows the capture and archiving of MMS, SMS, and phone call information from Android smartphones. (Android 2.2.2+ is supported.) To enable mobile data archiving the following tasks must be completed, in order:

1. The Router must be installed and be available outside the host network. (in DMZ)
2. The Mobile Module must be configured, and a Mobile worker created.
3. The Retain Android application must be installed to users' phones.
4. Devices must be registered under 'Device Management'.
5. Users must use the registration email to verify device registration with the GWAVA server.
6. The data path folder(s) must be manually created.

The Retain Router should be installed in the DMZ area of the host network. The Router must be available to the internet and the Retain Server. The Router and Worker may be installed on the same machine, or apart, however both the Router and the Worker must have access to the Data Path location. If they are not to be installed on the same machine, a mapped drive must be created to the location. See the install guides for more information.

The Retain.apk application is found in the Retain program installation folder in the '…/Retain330/mobile/android' directory. Use your existing mobile device management system to distribute the APK to devices. (The application may take up to 15 minutes to receive configuration after it is registered. No data will be archived until the application is registered and configured.) The application sends collected information, approximately every hour, to GWAVA Inc. systems, where the organization's data is then directed to the corresponding Retain Server's router. As such, there are no schedules for the module.



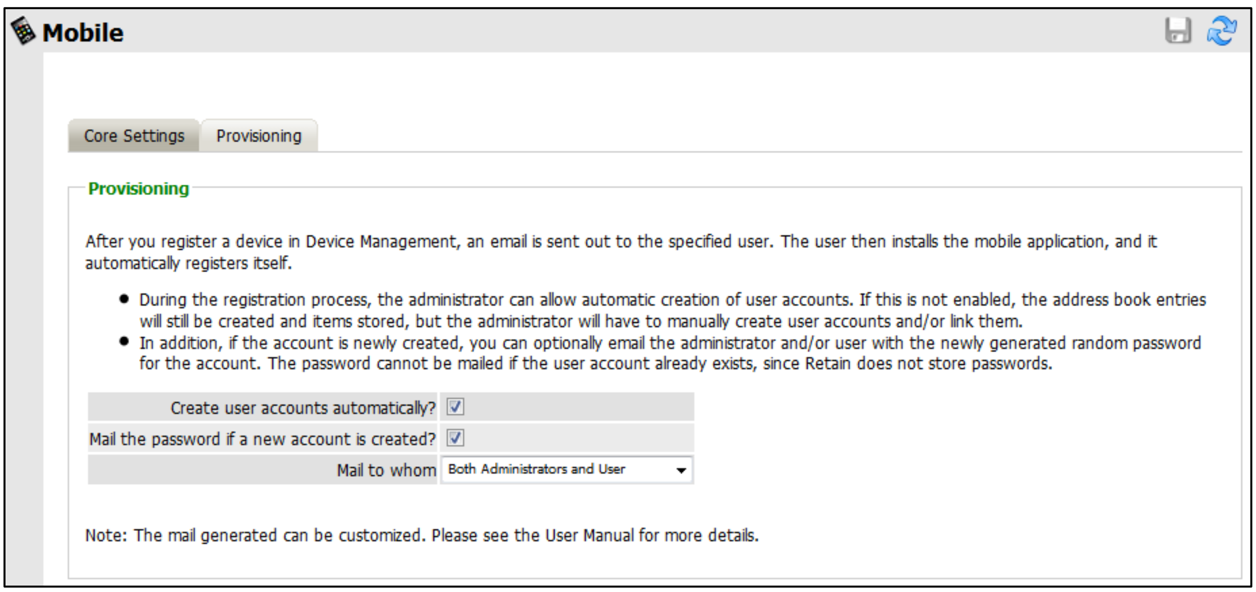
Host Name

The host name of the router endpoint must be accessible from outside the network. This is the connection information which GWAVA will use to deliver the mobile messages to the Retain Server. While an IP Address will work in this field, DNS is strongly recommended.

Data Path

The data path is the store location for messages received by the router, but not yet input into the Retain Server. This must be a location which the router will have constant and reliable access to. This location must also be accessible to the worker assigned to the router. A mapped drive will be required if the data path is not located on the same box as the mobile worker and mobile router. This path should be the path to the data directory from the Router, and should be absolute. Folders will not be created automatically. If the data path is being created on a Linux system, the ownership should be tomcat:tomcat. After entering the configuration, test the connection.

Provisioning options allow for automatic user accounts, and associated passwords mailed to the designated address. Defaults are shown.



After the module configuration has been saved, a worker must be created to allow the information to be accepted into the Retain Server. The Mobile worker, Profile, and Device Management menu pages will not be available until the Mobile Module has been configured, and the configuration has been saved.

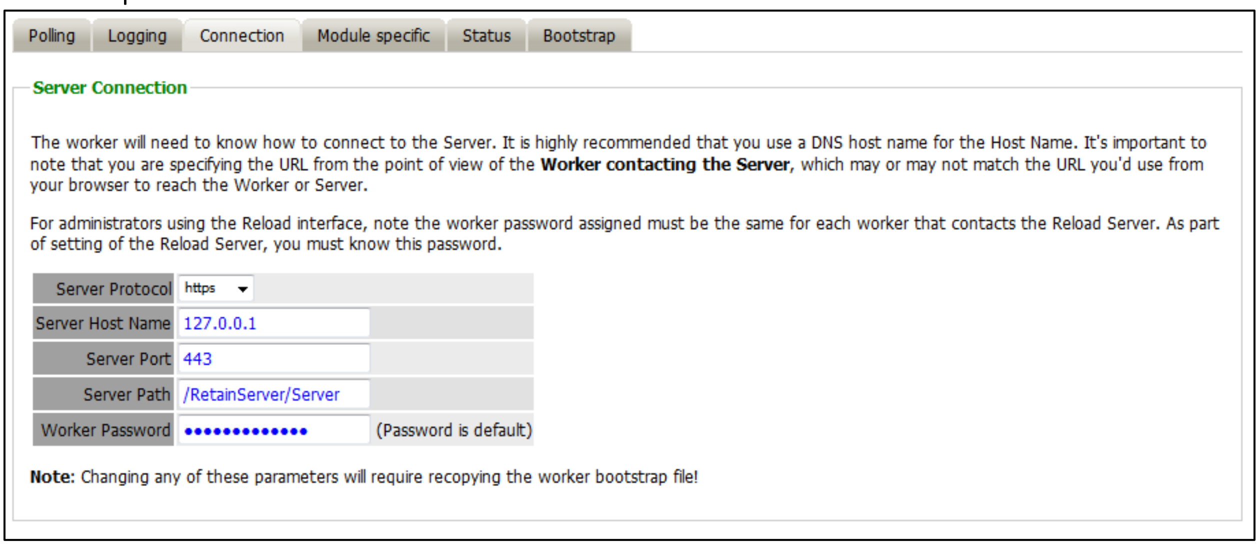
Worker

The Mobile worker is a special worker configuration which contacts the Retain Router with all the information it needs to function. This includes the configuration settings for the data path and connection information. In general, the Mobile Worker is configured the exact same as most workers in the Retain system, however there is one setting for the Mobile Worker which is specific to the Mobile Module; the data path. The data path is essential for the worker to function with the Mobile Module.

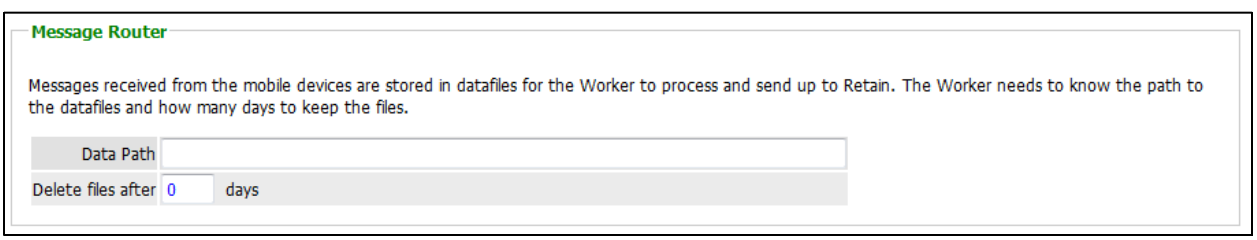
The mobile data is delivered to the Retain Server through a router service, which must be informed how to contact the Retain Server. While the Router is gathering information between jobs, the mobile data is stored. The stored location is specified by the data path. This is why the Router and the worker must have direct and constant access to the data path; the data path stores the message data collected by the Router and retrieved by the Worker.

To ensure connection to both the data path and the Retain Server are correct, the Connection and the Module Specific tabs must be reviewed and configured. The Connection tab holds the connection address which the Retain Worker will use to contact the Retain Server. Depending on where the Server and the Worker are located in the network, and because the Worker may be installed alongside the Router in the DMZ, the connection information must be accurate to allow a clean connection to the Retain Server. An IP Address will work, but the DNS hostname of the Retain Server is also recognized and supported.

The port and address must be open or forwarded through security and firewalls from the Worker to the Server. In addition, the Retain Server will not accept connections without the password set here. The password is randomized and doesn't need to be changed. Set the correct information and move to the 'Module Specific' tab.

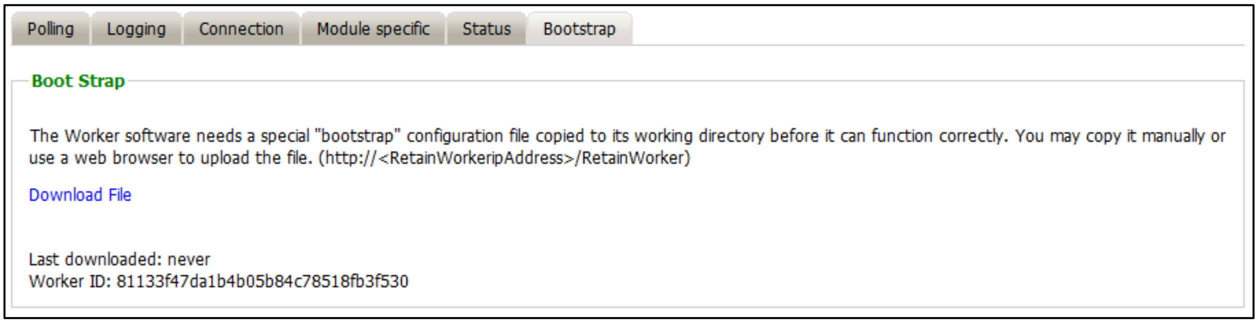


Under the Module Specific tab, the only field that applies to the Mobile Module is the field at the bottom marked 'Message Router'.



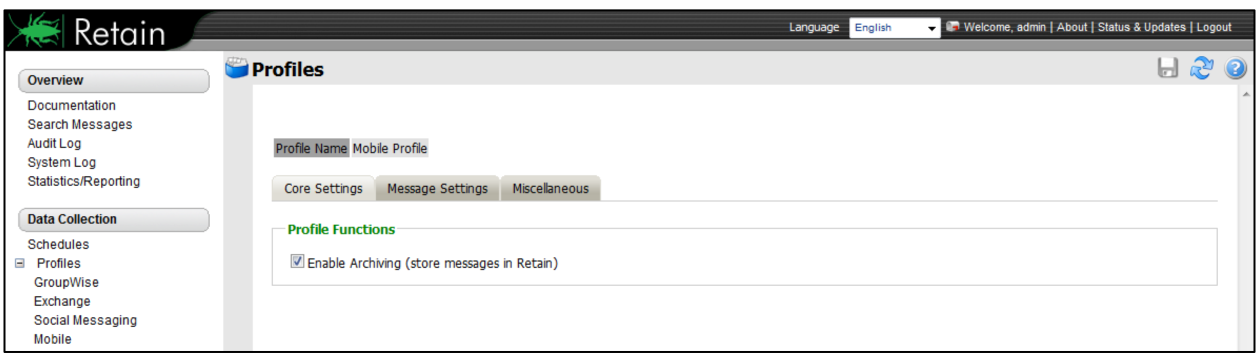
The path that the Worker will use to connect to the mobile Data directory should be placed here. This may be a mapped drive or a local path. The path should be absolute. The connection to the data directory is essential to the worker function, if this is unavailable or blocked, mobile jobs will fail.
The worker will delete files after adding them to Retain according to the time frame listed. A setting of '0' will tell the worker to delete files immediately after importing them into the Retain Server.

Once the Mobile Worker has been configured, save the changes. Once the settings have been saved, the worker will be created, and the configuration saved to the bootstrap file. The bootstrap file must be uploaded to the Retain Worker before the Worker will function. Select the 'Download File' link to save the configuration file. Browse to the worker's page, (http://<RetainWorkerIPAddress>/RetainWorker), and upload the configuration file. Once uploaded, the worker automatically reads the configuration and checks with the Retain Server for jobs.

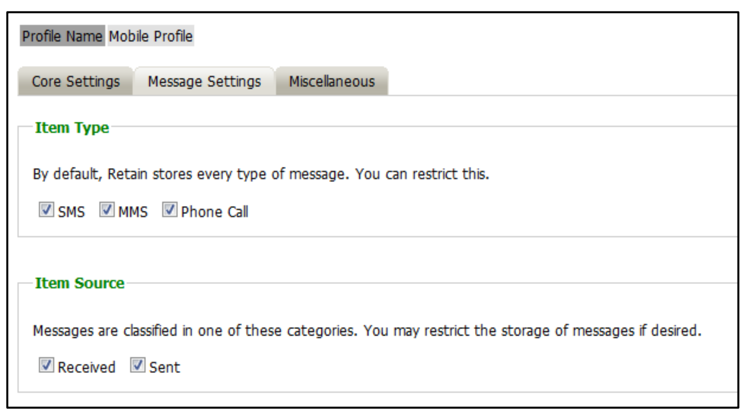


Profile

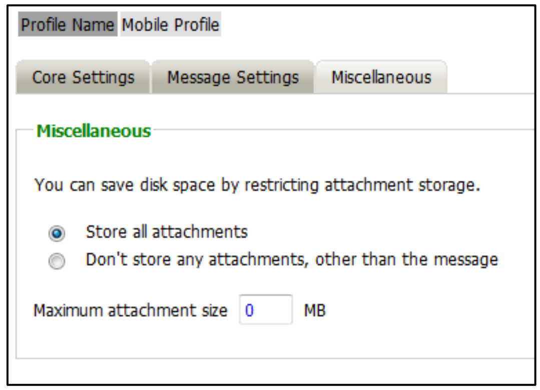
The Mobile Profile allows the administrator to dictate what types of message data is collected from registered mobile devices. The profile is universal, and once configured works for the entire mobile system.



The Mobile Profile is fairly straight-forward. To enable message data collection for the mobile system, the profile must be activated.



Under Message Settings, the different types of messages which can be archived from Mobile devices are listed and configured. The message source and type are available for selection or exclusion.



Finally, the Miscellaneous tab allows for configuring attachments. Attachment size and general attachment settings can be configured here. If there is a maximum limit, set it in the field below.

Before the profile can be saved, some setting must change for the Retain Server to recognize that something needs to be saved. If no setting has been modified, toggle a setting to trigger the save changes icon to activate and then save the changes.

If changes are not saved, then the profile will not be saved. Jobs cannot be run unless the profile has been saved.

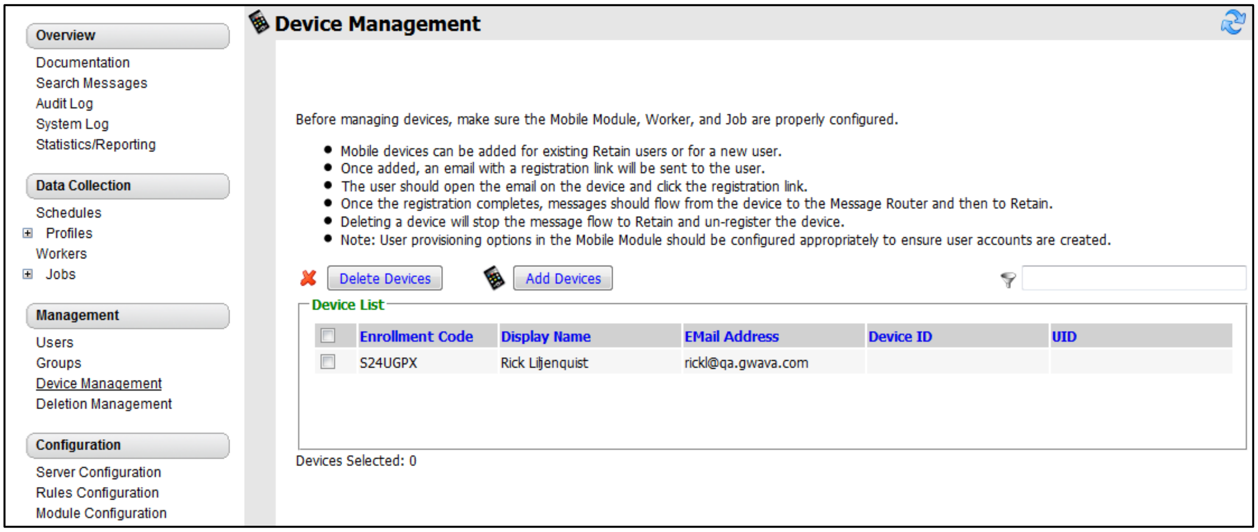
Once the module, worker, and profile have been configured, devices must be added through Device Management.

Device Management

Devices are added to and deleted from Retain through the Device Management interface. Multiple devices may be selected, and all selected devices remain selected until either action is taken, or the administrator has navigated away from the page.

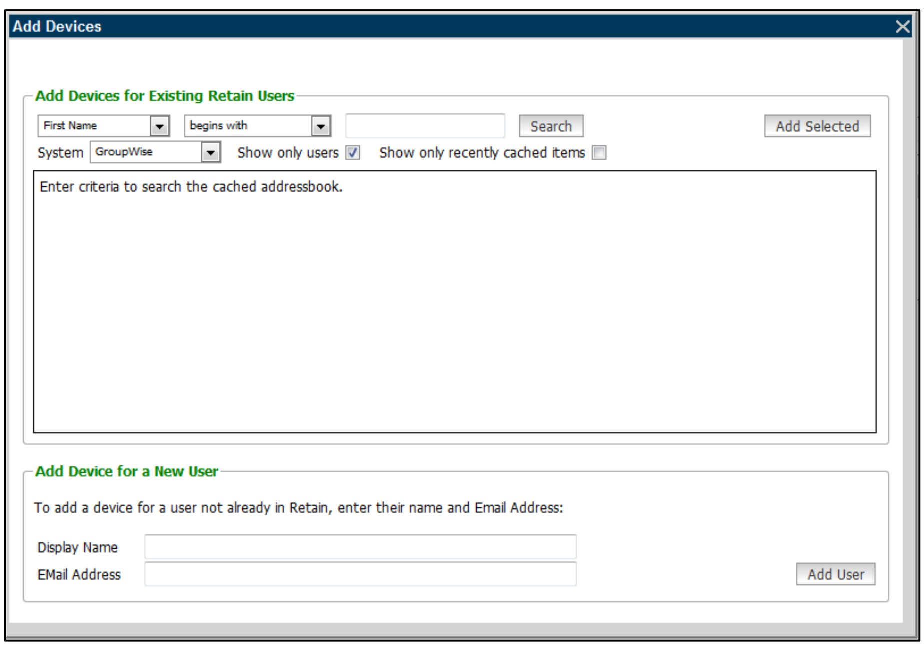
Once a device is added to the interface, Retain creates an email which contains an activating link. Users need to open this email and follow the link on their mobile device. The link should be activated through the Retain application on the Android device. The activation email can be customized. The template this email is generated from is located in the file:
…\RetainServer\WEB-INF\classes\config\mobile\registeruser.html
The email sent to users may be customized, including any specific instructions for the organization, can be added or modified here, and all emails sent to users will contain information placed in this template. For information on customizing the registration email template, see appendix I.

When a user is sent an email, the Retain system creates a unique device and user identification key, and ties it to the organization from which it came, allowing the Retain system to 'route' the appropriate messages to the owning Retain Server. Devices which have installed the application and activated through the emailed link, will display in the Retain Server as 'registered', in that they will show a code, a device key, and a UID key. Once registered, device data including SMS, MMS, and phone call data will be archived in the Retain System.



To add a device to the Retain system, open the Device Management window and select the 'Add Devices' button.

The Add Devices window opens, which allows administrators to select and add multiple users. The system may also add users which are not cached in the Retain system, but they must be added one at a time. Manually input the name and associated email address at the bottom and select the 'add user' button.



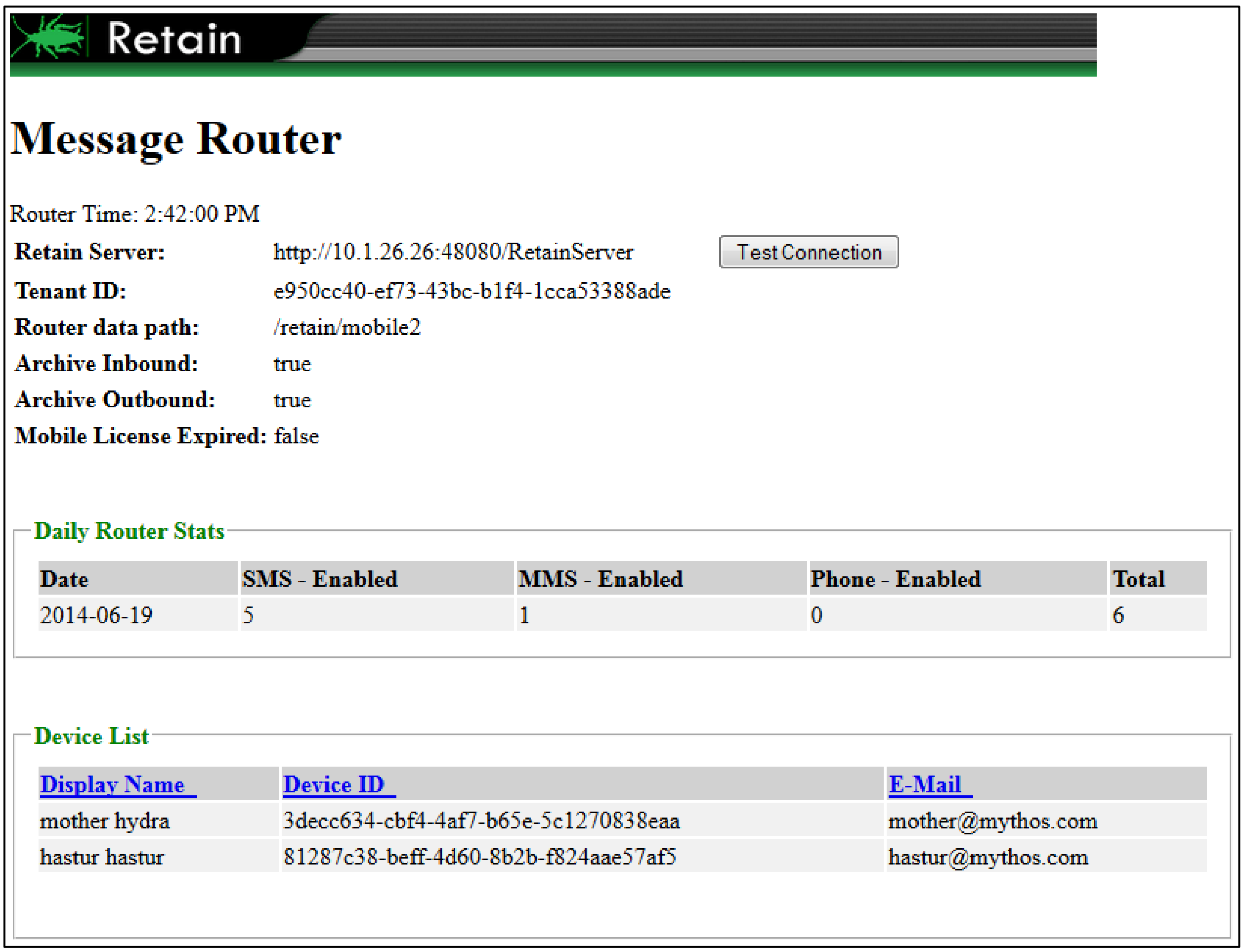
Mobile Router Page

The Retain Router has its own webpage. This page can be used to test the connection to the Retain Server, as well as verify that communication is open and that devices registered in the Retain Server are listed in the Retain Router.

To access the Router page, open a browser and enter the connection URL.
http://Retain_Router_IP_or_Domain/RetainRouter

For example: http://192.168.1.21/RetainRouter

The resulting page should look very similar to this:



Devices which are active are listed along with daily statistics. The daily statistics are reset every night, and full statistics are kept in the Retain Server.

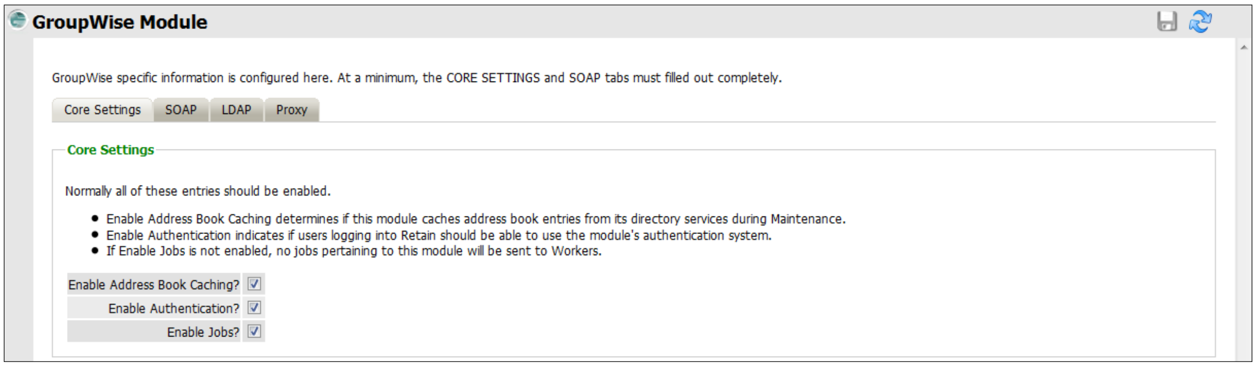
This page is mainly an informational page.

GroupWise Module

The GroupWise module must be fully configured before Retain can archive or communicate with the GroupWise mail system. Retain must be provided with an IP address and port of a readily accessible Post Office (fast access), appropriate login credentials, and a trusted application key.

The GroupWise module page opens first with the Core Settings.

Core Settings



Normally all of the checkboxes on this tab are always left selected. It is rare that you would ever deselect any of them. Two cases where you might would be troubleshooting, (as instructed by Technical Support), and retiring an old email system.

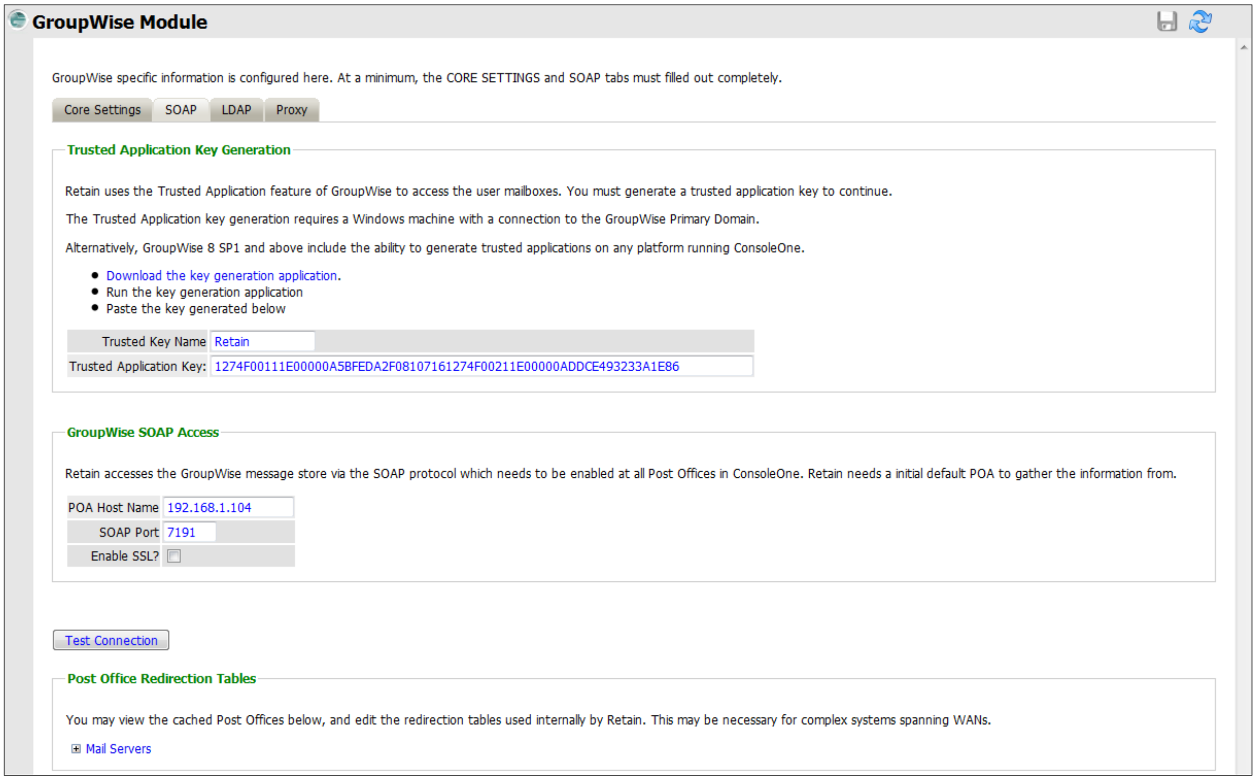
The Enable Address Book Caching function allows Retain to regularly cache the online email systems address book and synchronize it with Retain. This is critical for administration, authentication, and archiving purposes. It is recommended to cache the Address Book once every 24 hours to keep the Retain storage system up to date. By default, maintenance is set to cache the Address Book once every 24 hours.

The Enable Authentication checkbox determines if end-user authentication is performed when the user logs into Retain. If it is deselected, the Retain system will NOT authenticate the user against the email system and the user will not be able to log in unless another authentication method is enabled.

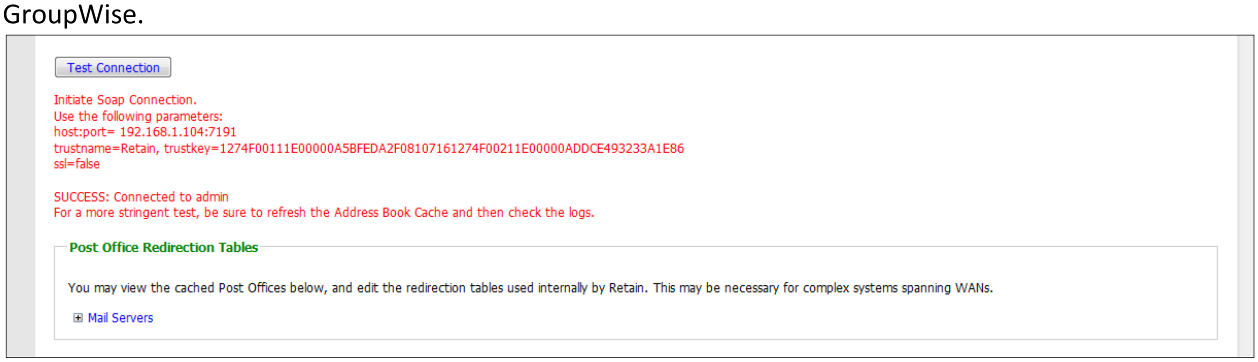
The Enable Jobs checkbox determines if configured data retrieval jobs are ever passed to the Worker. Even if the individual job is fully configured and enabled, if this checkbox is switched off, no jobs configured for this module will be processed.

SOAP

Provide the POA Host Name and SOAP port. IP addresses are acceptable, but host names are preferred as IP addresses may change. SSL is supported, but comes at the price of speed, and will slow down the archiving process. Create a Trusted Application key for Retain, either manually from Console One for GroupWise 8.x and higher, or via the provided Key Generator provided and linked from the page. For instructions, see the trusted app key section in the appendix.

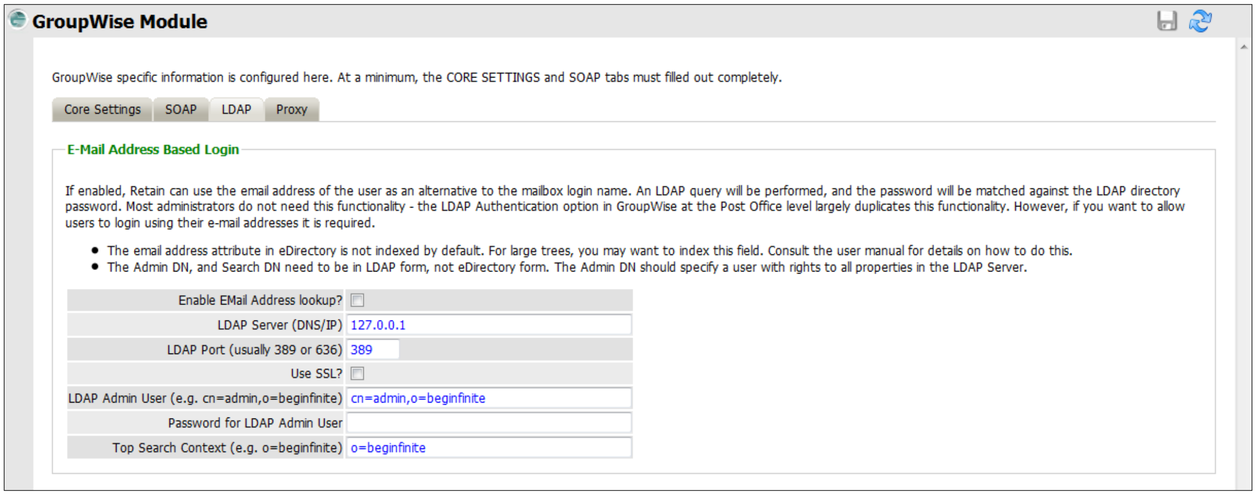


The SOAP access information must be provided, and the connection tested and verified before the system can connect. After providing the required information, click the 'Test Connection' button. The results are displayed. A successful result must be reached before Retain can archive messages from GroupWise.



If mail server Redirection is required for mail servers which are not contained on the local WAN and must have the connection addresses manually specified, the appropriate information may be modified in the redirection table. Most installations will not require any modification.

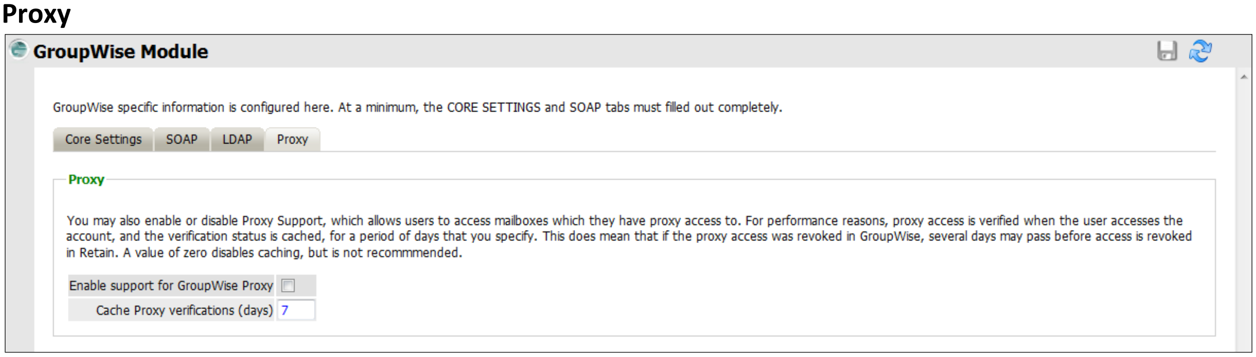
LDAP



LDAP may be used for individual users wishing to access their respective archives. If LDAP is setup and desired to be used for Retain user authentication, it must be fully configured in the GroupWise module.

Utilizing LDAP allows users to log into their respective archives using the user's full email address. This authentication requires that the email attribute be marked indexed in ConsoleOne.

Proxy



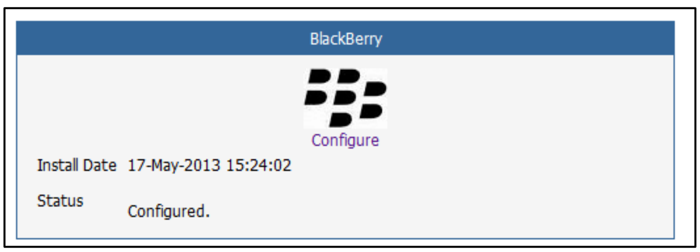
Users who have been given proxy to another account in GroupWise may be granted access to proxy accounts in the Retain archive as well. For performance reasons, Retain caches proxy verifications for a period of days.(Default is '7' days.) Revocation of proxy access might not be reflected immediately in Retain. The caching period may be reduced or even disabled, (a value of '0' disables caching), but this is not recommended.

BlackBerry Module

The BlackBerry module allows the collection of BlackBerry phone data from the Enterprise server into the Retain system. BES 5.x and 10.x are supported. To archive the BlackBerry information, the BlackBerry Enterprise Server must be configured to log phone calls, PIN, BBM and SMS data. The server log files are what Retain uses to collect the information about phone activity, and as such no software or modification needs to be made to any system phones. If the BlackBerry server has not been configured to log the data, Retain will be unable to archive the information. For BES 5.x, instructions to modify the logging in the BlackBerry Enterprise Server can be found in the BlackBerry Enterprise Server help file. (Found under Start | Programs | BlackBerry Enterprise Server | Help | BlackBerry Manager Help)

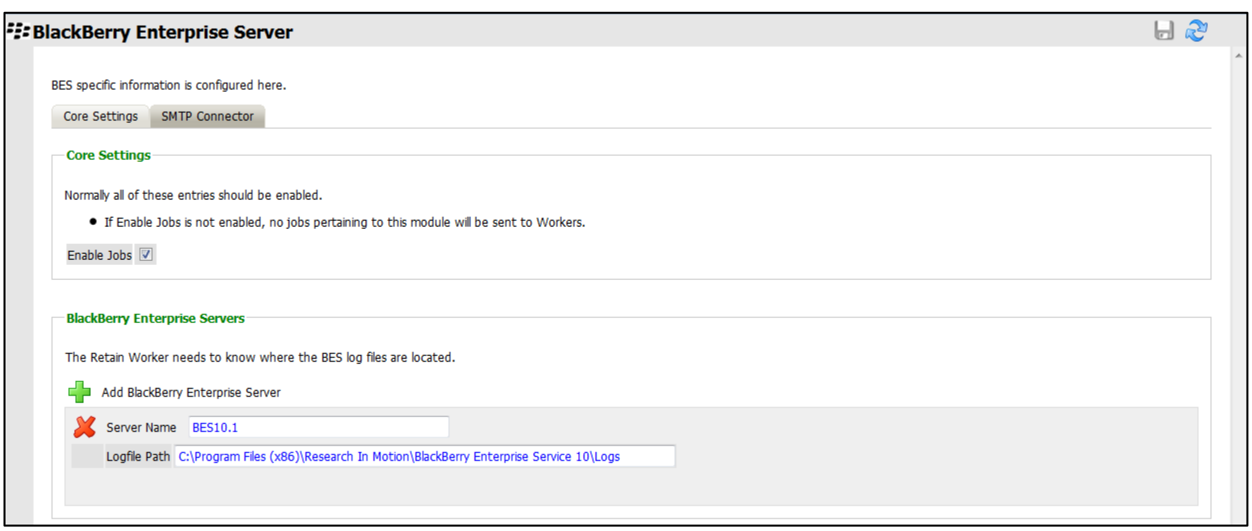
For BES 10.x, users must be set on EMM – Regulated mode and have the logging set to 'yes' for all types desired. Balanced mode users will not have logs created for them in the BES system and as a result will not be archived.

Installing the BlackBerry Module is incredibly simple. Essentially, the module needs to be enabled and configured with the BES log file location. Afterwards, the data is treated the same as any other data entering the Retain archive. Data is archived in the database under the user/phone it originated from and can be searched and viewed through the Search Messages interface.



To enable the BlackBerry Module, select the 'BlackBerry Module' from the module page and click 'configure'.

The BlackBerry module needs to be enabled on this page to make it active in the Retain system. Before data can be archived, the BES log file path must be provided.



The log file location must be the address to the log files from the Blackberry Server. Regardless of where the worker is installed, local or remote to the Blackberry Server, it must have direct file access to the logs. This access can be accomplished through a shared folder or location, but it must be available to the Retain worker. Appropriate access through firewalls or network security must be made available if the worker is not installed on the BES system.

SMTP Connector

In order to allow the forwarding of BES items out of the Retain system, the Blackberry Module needs to be configured with an SMTP connector. This connector will provide an outlet into the mail system, for Blackberry data to be forwarded if desired.

The amount of configuration necessary for the SMTP Connector depends on the specific setup of the SMTP system. If a username and password are required for the host SMTP system, then it must be provided. If it is not required, the configuration of the username and password is optional.

The address of the Mail Server, the SMTP Mail From Address, and the SMTP Mail To Address, must all be configured for the system to function correctly. The ‘to’ address is the destination address where the data will be forwarded to. The ‘from’ is the specified ‘from’ address.

In addition, the ‘Enable SMTP Connector’ option must be enabled in the ‘jobs’ configuration for the Blackberry section.

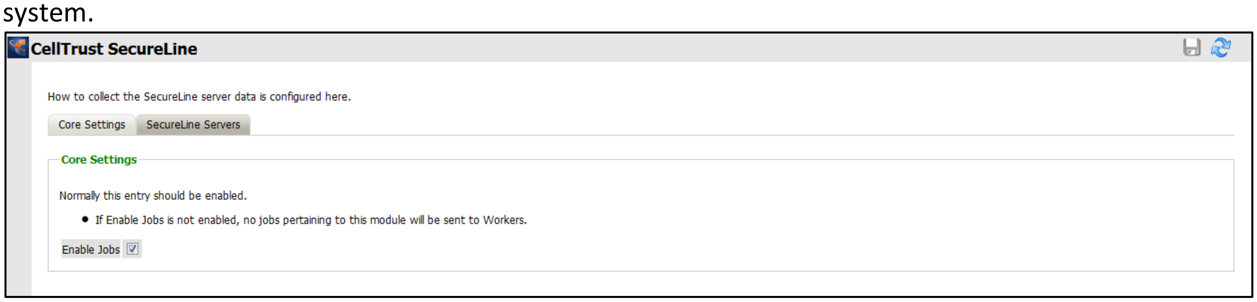
CellTrust SecureLine

The CellTrust SecureLine module allows the collection of phone data from the CellTrust Secureline server into the Retain system. To archive CellTrust SecureLine information, the SecureLine server must be configured to log phone calls, PIN and SMS data. The server log files are what Retain uses to collect the information about phone activity. If the SecureLine server has not been configured to log the data, Retain will be unable to archive the information. See appendix J for Secureline server configuration.

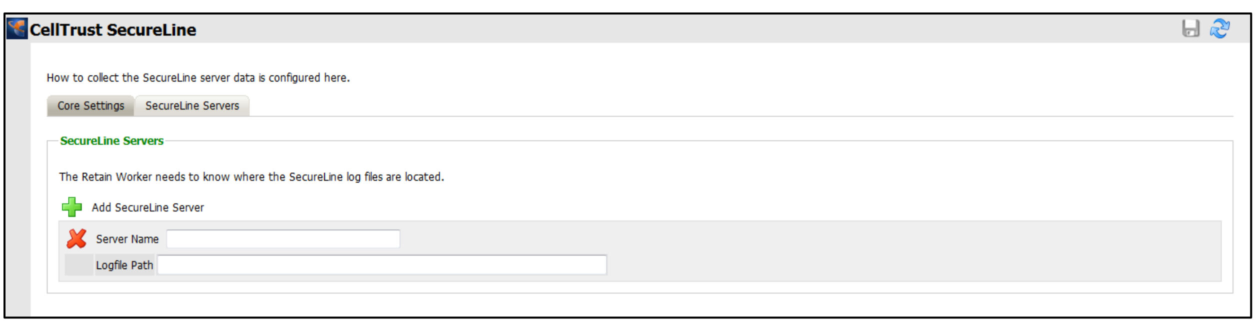
Configuring the CellTrust SecureLine Module is incredibly simple. Essentially, the module needs to be enabled and configured with the log file location. Afterwards, the data is treated the same as any other data entering the Retain archive. Data is archived in the database under the user/phone it originated from and can be searched and viewed through the Search Messages interface.

To enable the CellTrust module, select the 'Configure' link under the 'CellTrust' icon from the module page.

The CellTrust SecureLine module needs to be enabled on this page to make it active in the Retain system.



The log file path for each server in the system is required to archive the phone data. To add a server to the Retain process, select the green plus sign and then configure the server name, (any name will do), and then the log file path.



The log files must be directly accessible to the worker tasked with archiving the CellTrust SecureLine data, whether through direct access or through a mapped drive. The logfile path is the direct file access path to the log files of the CellTrust Secureline server, (/opt/PM/scheduler/external by default), and should be specified as the worker will access the log files.

Archiving/Data Collection – About Workers, Profiles, Schedules, and Jobs

Getting data into the archive is the core functions of Retain. As such, sub-functions have been broken out to give you as much flexibility as possible in deciding your archive policy.
Your archiving policy will cover several points:

- What to archive (jobs)
    - Includes what message server(s) to collect data from.
- What worker
- When will the data be collected (schedule)
- How to collect the data will cover (profile)
    - Types of items or users to archive.
    - Date range of items to be archived.
    - Avoiding redundant data collection.
    - Utilizing storage flags to achieve 100% retention.
    - Whether to store attachments.
    - Advanced criteria, such as attachment names, or folder locations.

Retain Job components

Schedule

The Schedule is the time framework that is set for the job to run on and provides the choice of how often, and when, the job is run. Single time, (job runs once), or a recurring time frame are available. Schedules are universal and are not module or job specific. They may be used for one or all jobs.

Profile

The Profile dictates which kinds of files to retrieve from the message system. All message system items are selectable to be archived, but you may also specify time periods, exclude folders or subjects, and how the data is stored. Profiles are module specific, and the profile section contains sections specified by each module and information only applicable to that module.

The Profile also has a very important function, duplicate checking. This keeps the Retain system from storing multiple instances of the same message. Make sure you check and read the section on Purge (GroupWise), Retention (GroupWise), and Item Store (Exchange/GroupWise) flags.

Worker

The worker is the part of Retain that actually pulls the data from the message system servers. The Worker contacts the Retain Server and gathers information on which jobs are associated with it, when to start them, and which items to get. Workers can only run one job at a time. Workers are not module specific, but may require module specific settings. These settings, where applicable, are found under the module specific tab.

Jobs

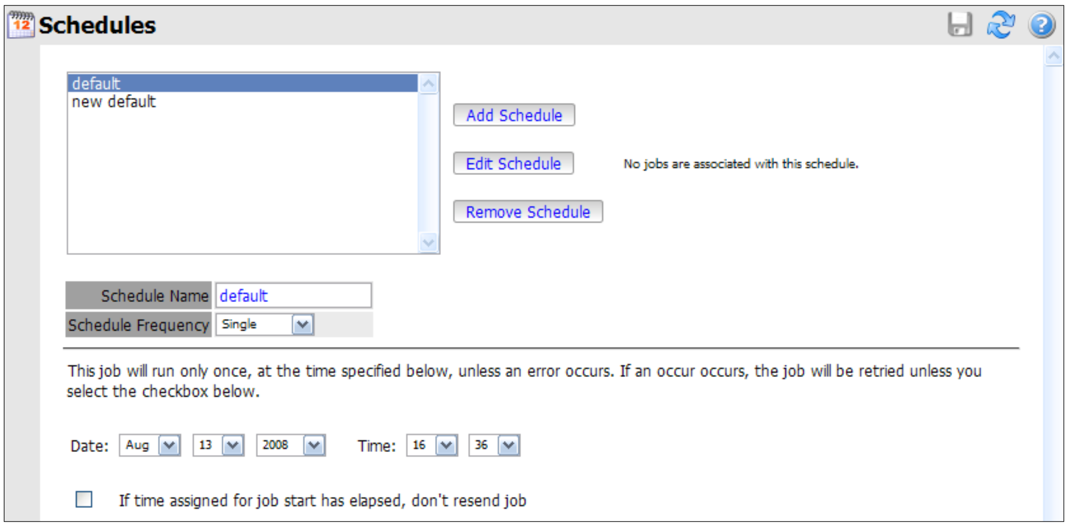
The Jobs section is where the Worker, Profile, and Schedule are all brought together and associated into a comprehensive configuration by allowing the user to tie their configuration to a selected Secureline server and selected user list. The desired SeucureLine server must be selected. The Worker will not start archiving anything until a created job is bound to a Worker, Schedule, and Profile.

Schedules

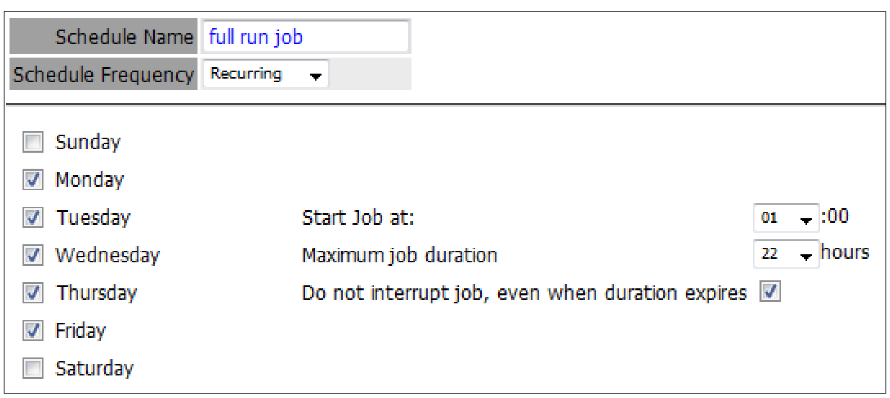
Schedules define **WHEN** to perform the data collection as defined in a **JOB**. A Job defines what **SCHEDULE**, **PROFILE** and **WORKER** to use.

- You can create as many schedules as you need.
- Schedules have no functionality until they are associated with one or more **JOBs**.
- They can be shared across multiple **JOBs**.
- You cannot DELETE a schedule that is currently associated with a **JOB**.
- Schedules can be recurring or one-time.

SINGLE schedules are configured with one start time, and one date.
To keep jobs from queuing up to the worker, select the box to do not resend a job that has an elapsed start time. Otherwise, a job will queue up on the worker if a previous job has not yet completed, causing the new job to start as soon as the current job is complete or terminated.



RECURRING schedules are configured using a start and interrupt time, and which days to start on.



Choose when on which days you want this schedule to trigger a job.
You may specify maximum job duration. If the job runs longer than the time limit you set, it will be interrupted. For cases where you do not want the job to be interrupted – for example, with a job you know will last longer than 22 hours, you may prevent the schedule from interrupting the job.

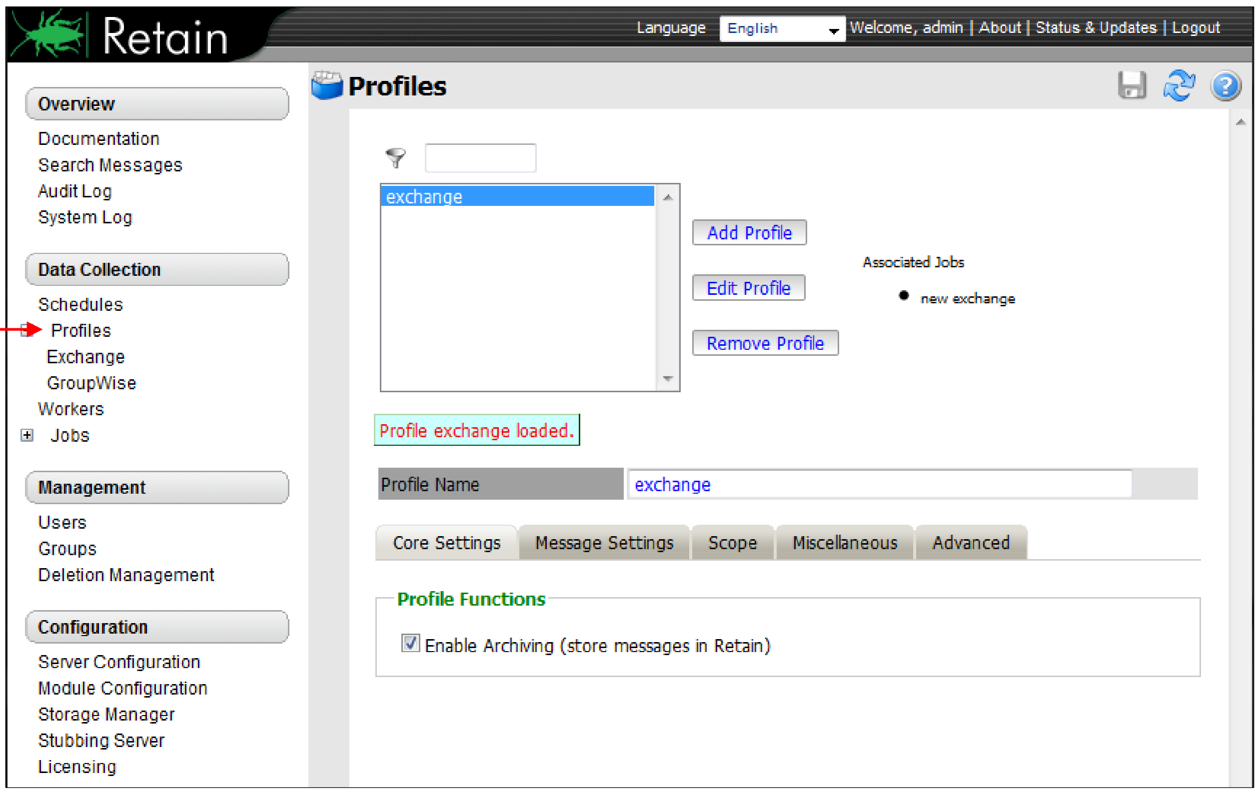
Don't forget to "Save Changes".

Profiles

A profile assigned to a job tells the system what to archive. Message types, status, date ranges, excluding or including specific users, private or public folders or both, and redundancy check settings are all configured under the profile.
The profile defaults to collecting all data, with no date restrictions. After Retain has finished collecting data the first time, you'll want to narrow the date range and criteria considerably, or pay a high price in performance. Each module has a specific profile page, but different profile pages will not display unless multiple modules have been configured. Each module's profile is explained below.

Exchange Profile

After the Exchange Module has been configured, the Exchange Profile will be available for configuration. If an Exchange Profile is not configured, jobs cannot be run against the Exchange system.



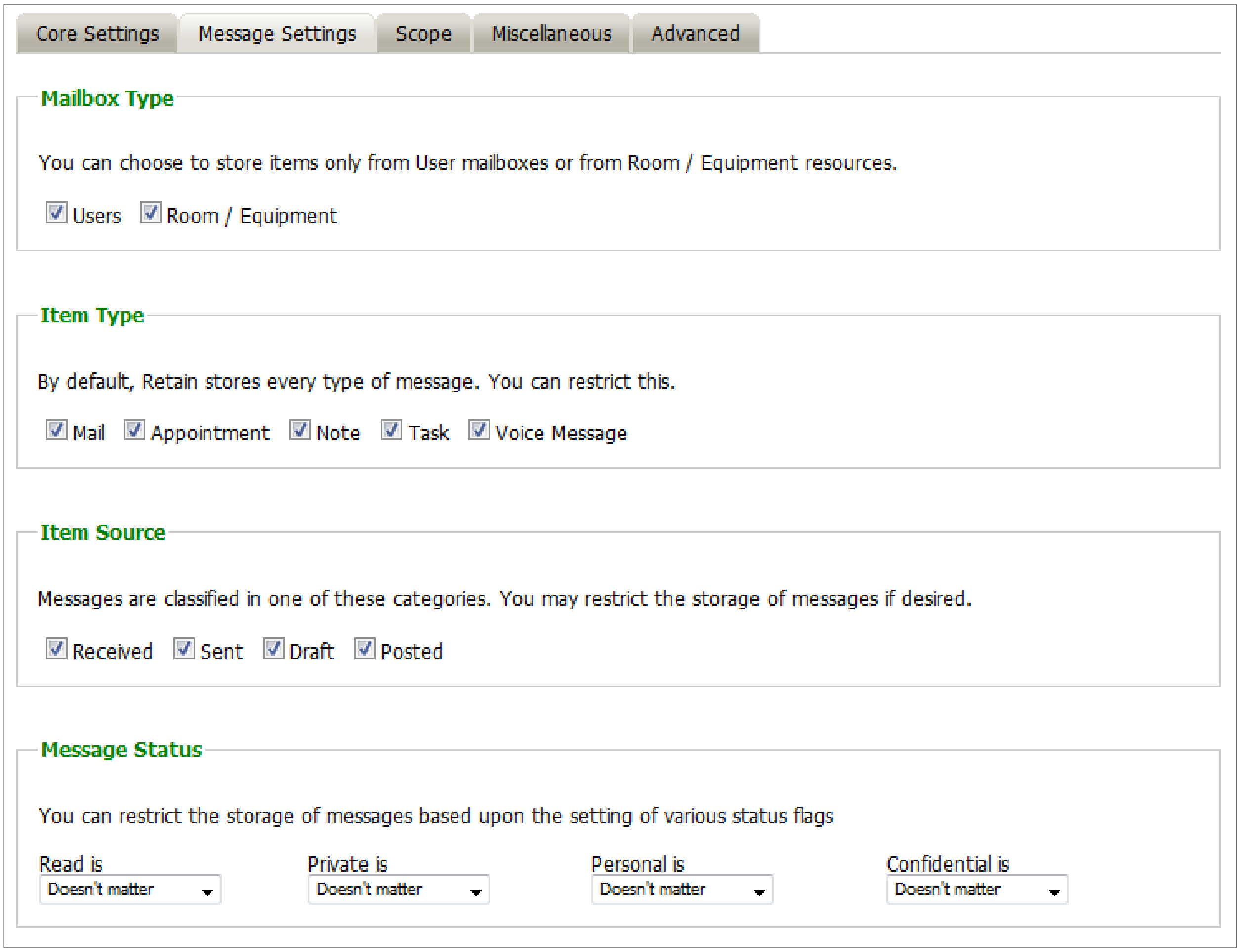
Click on 'Add Profile' and provide a profile name, or select an already existing profile to access the configuration tabs. All changes made on this page must be saved by selecting the 'save changes', disk **icon, at the top right of the page. Tabs may be changed and navigated through without affecting new** settings, but any move to another page will require saving, or abandoning the changes made.

Core Settings

The core settings consist of an enabled/disabled option which must be enabled for any jobs based on this profile to archive anything.

Manage Settings

Retain can archive and select specific types of mail and Exchange system items to be archived. The Manage Settings tab provides access to manage those settings.

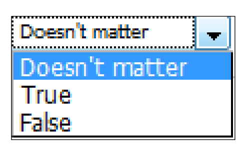


The Mailbox type specifies whether to include or exclude the available types of mailboxes. Because there can be multiple profiles and jobs, it may be advantageous to archive the Users and Room / Equipment mailboxes separately as needed and appropriate for the system.

The Item Type option specifies the different types of messages found in Exchange that can be archived, and allows the exclusion of or inclusion of the different individual types.

The Item Source option allows administrators to exclude or include messages that have not yet been sent or received, or posted.

The Message Status allows messages which have or have not been read or opened, or marked private or confidential to be archived. The different options in the drop-down menu are as shown.

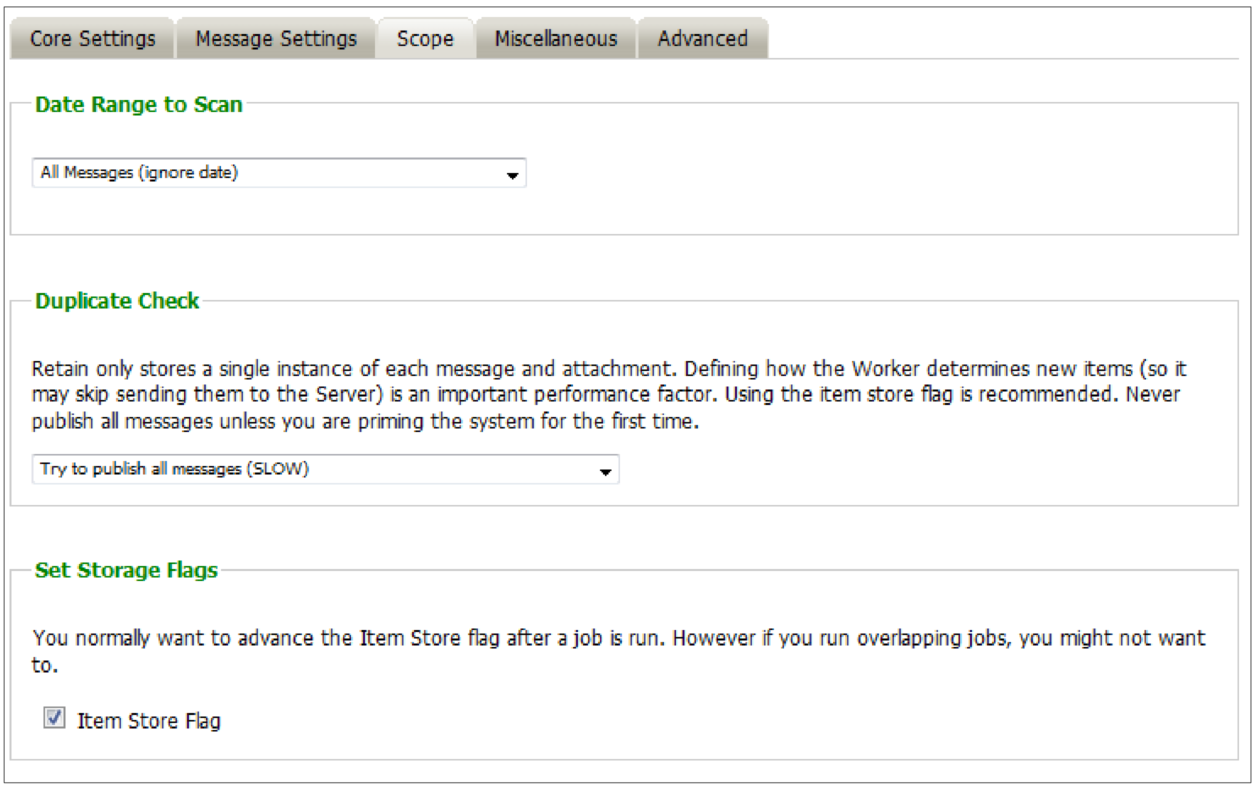


Scope
The Scope tab dictates how pervasive the attached archiving jobs are, and what kind of duplicate checking is done, or not done, in the Retain system.

The Date Range instructs Retain to scan for, and archive, messages after, or before, a certain date. This is useful if only specific chunks or areas of mail are to be archived.

The duplicate check either scans for all messages, or instructs Retain to only look for messages which are newer than the Item Store Flag, which is a time-stamp on the system. All messages younger than the time stamp will be archived by Retain if the item store flag is utilized, but Retain will ignore all messages which are older**. Be sure to set the item store flag for the CellTrust Secureline module to avoid duplicates.**

NOTE: Unlike GroupWise, Exchange does not ensure any compliance when scanning end user mailboxes; users may freely delete their email. The Item store flag does not prevent mail deletion. Only Journaling and archiving a journaling mailboxes, guarantees all items have been archived.

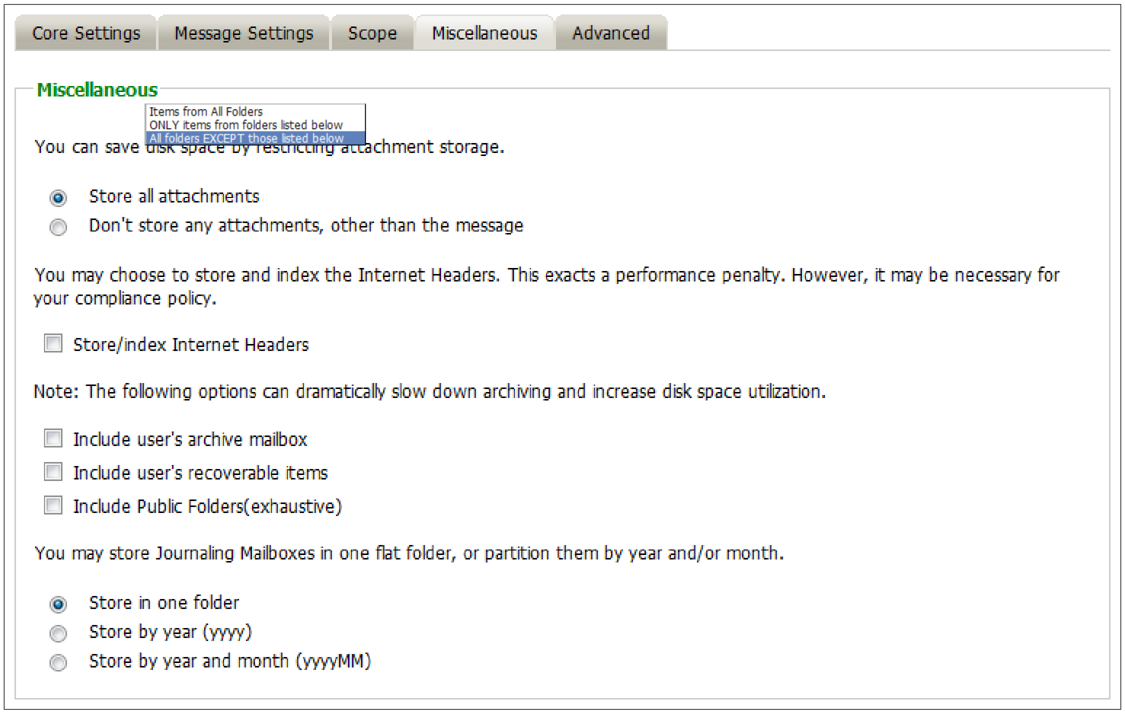


It is recommended that the first job be allowed to scan for all mail that is desired to be archived, with the duplicate check set to ‘publish all messages’. Afterwards, it is recommended to have the duplicate check look for the Item Store Flag, and only check for new mail in the system.

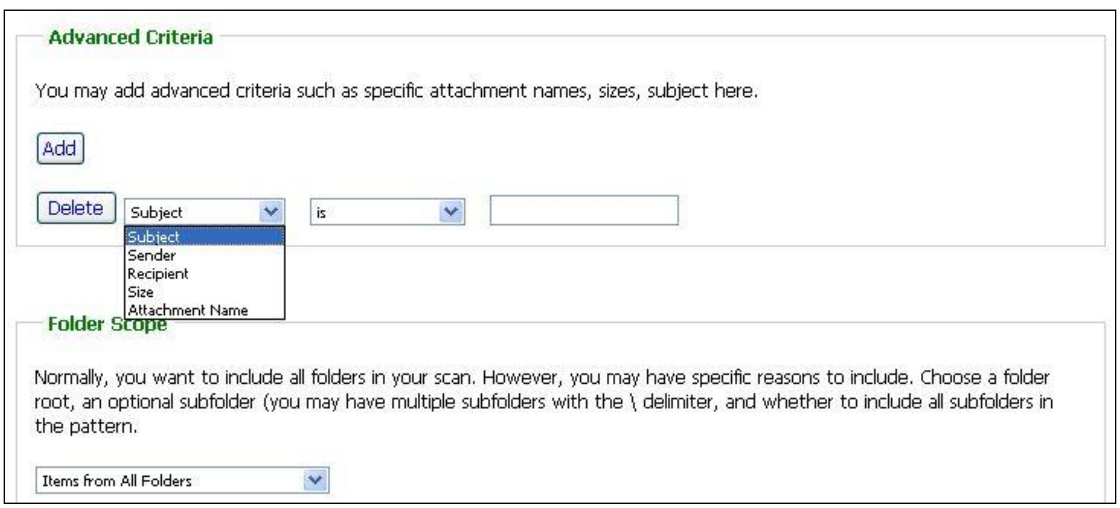
Miscellaneous

The Miscellaneous tab allows access to particular settings detailing how messages are stored and what is archived. Attachments, message information such as the internet headers, and how the data is stored and named, (by folders, year, or year and month), dictate not only the message store structure, but affect the storage size.

Miscellaneous options also allow for the archiving of the 'recoverable items'. To enable checking and archiving of the 'Recoverable Items' for compliance reasons, select the checkbox next to the option.



Advanced



If you want to be more specific as to what to dredge or not to dredge, add the criteria here. Each line will be ***logically AND***-ed together.

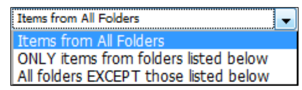
Think “Dredge all items where the following is true:”
Criteria A ***and*** Criteria B ***and*** Criteria C etc

You may select based on:
- Subject
- Sender
- Recipient
- Size
- Attachment Name

Whether they are equal to, not equal to, whether they contain or do not contain the item you specify.

This gives you great flexibility and granularity. It allows you to customize dredges and retention for many different groups, or even individuals.

Folder Scope
By default we dredge items from all folders. You can specify one or more inclusions or exclusions.
Your choices are:

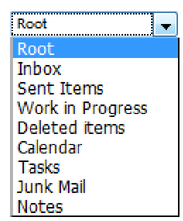


- Dredge everything
- Dredge only these listed folders
- Dredge everything EXCEPT these listed folders

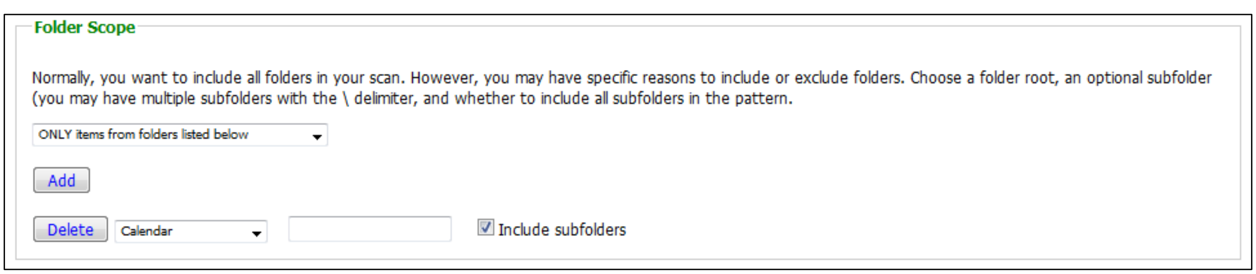
How to specify the list of folders to dredge/exclude:

1) Select ‘Add’ to open a new selection.

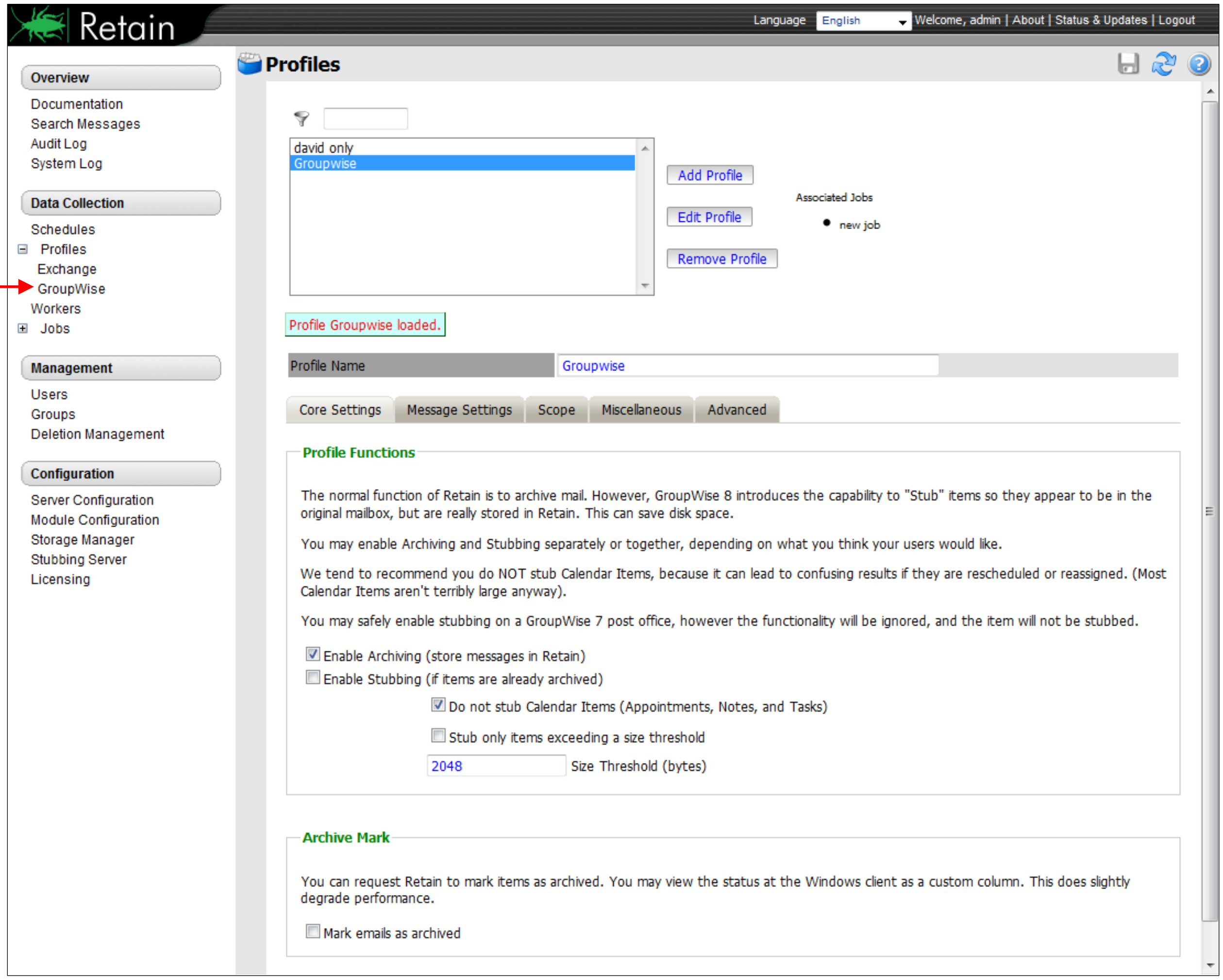
2) Specify a System Folder (mandatory). Example: Calendar.



3) You specify a subfolder of that folder (optional).
   Example: entering “old” would mean the folder “old” under “Calendar”.
4) You can have multiple hierarchies under that with the / delimiter.
   Example “old/mail” would mean the subfolder “mail” under “old” under “Calendar”.
5) You specify if the option includes subfolder.
   Example: If you select “old” and “includes subfolder” is unchecked, “Calendar/mail” is selected. If “includes subfolder” is CHECKED, “Calendar/old/mail” would also be selected.



GroupWise Profile



Core Settings

The Profile Functions tell the Retain Server what to do with the mail it archives from the GroupWise system. If Archiving is not enabled, mail will not be archived by Retain.

Stubbing

Before enabling stubbing, make sure you understand the way stubbing works and how that will work in your system because **once enabled, you cannot reverse the stubbing process**. Stubbing, (requires GroupWise 8), allows Retain to replace archived messages and items in the GroupWise Post office with 'stubs' that link back to the full message or item in the Retain Archive. End users should not notice a difference as they have transparent access to the stubbed item through the GroupWise Post office. The stub behaves much like the native item is still in the GroupWise system.

Stubbing CANNOT be reversed. Plan your system and understand the positive and negative sides to Stubbing before you continue. **To use stubbing, it is strongly recommended that the GroupWise system be at least 8.02HP1. Previous versions of GroupWise do not contain critical stability fixes.**

Why stubbing is good:

- Save Disk space. Mail can be removed from the system without being 'deleted'.
- Users have easy access to items stored in Retain
- Transparent access, no need to login to Retain for common tasks.

Why stubbing may not work for your system:

- Stubbing CANNOT be reversed. (Once a message is stubbed, it cannot be returned to the same position in the system)
- User training for stubbed items may be necessary due to decreased access speed
- No method for protecting stubs from deletion in the GroupWise client. (Recreation is difficult and complicated.)
- Non-mail items should not be stubbed. (Calendar and appointment items behave erratically when rescheduled).
- Stub items are NOT COMPATIBLE with third party API's. These applications view the stubs as posted items only, with no text or attachments.
- Mobile, Web, IMAP, and POP3 clients will only see posted empty items, not actual contents.

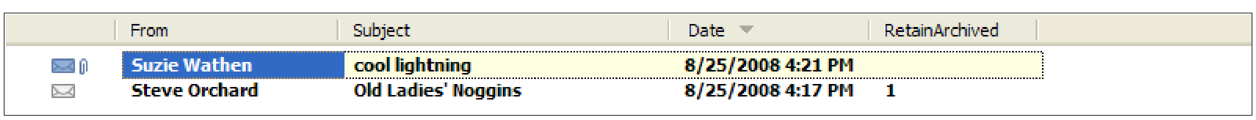
Determine the correct option for your system. If you wish to enable Stubbing, you need to install and configure the Stubbing Server as well. Refer to the install guide for your specific OS, and the Stubbing Server section for configuration. Stubbing can only be active for items which have been archived by Retain.

Calendar Items should not be stubbed unless necessary, as this can cause erratic behavior if archived items are rescheduled. If you wish to only stub large items in your Post Office, you may set a size threshold. Any item larger than the specified size will be stubbed. If this option is not set, all messages will be stubbed, regardless of size.

Archive Mark

Some users may opt to use the Archive Mark in GroupWise for messages that have been archived by Retain. The archive mark is a custom flag and may be modified, therefore is not secure and should not be used for compliance. Archive Mark slightly degrades job performance. Check the check box to enable Archive Mark for the selected profile.

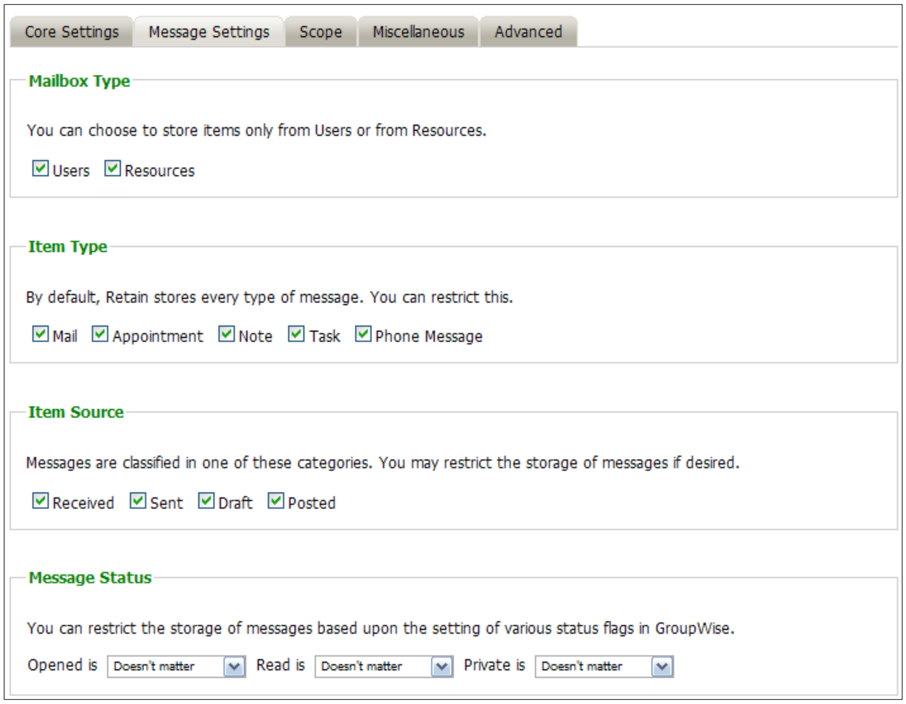
When the Archive Mark is active, Retain creates a custom column for mail, called "RetainArchived" which users and administrators may add to their GroupWise clients to view mail which has been archived. The RetainArchived column indicates an archived mail item by displaying a '1' in the message row, while remaining blank when the message is not archived.



To add the column, in the client: highlight desired mailbox or folder, right-click on columns header, select **More Columns**, select **RetainArchived**, and select **Add**.

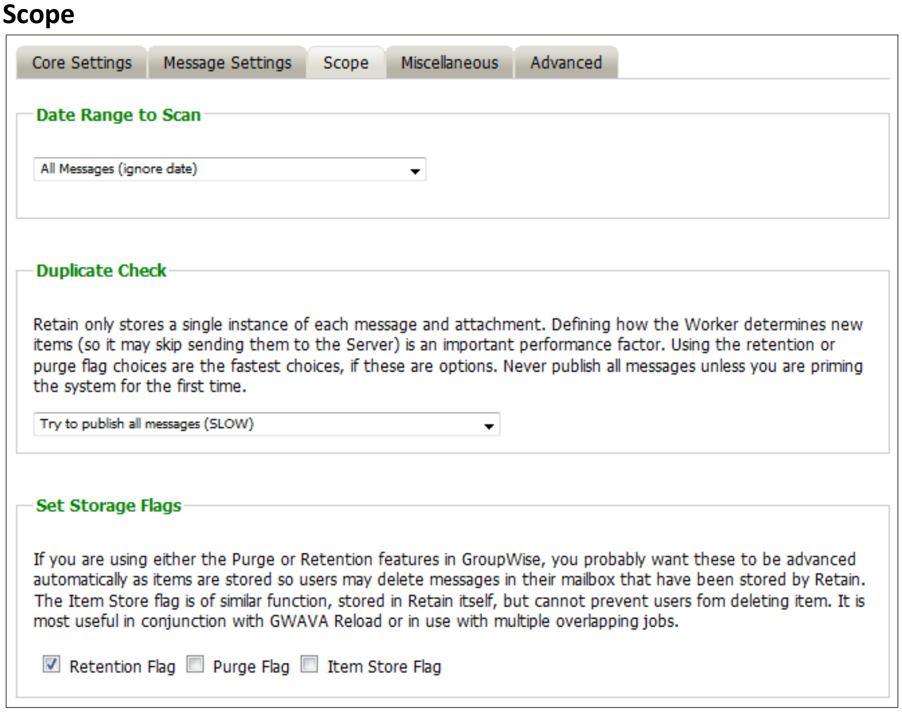
Message Settings:

- Mailbox Type: You can restrict the type of mailbox to users, resources or both.
- Message Item Type: Select what type of items within these mailboxes to dredge.
- Message Source: Select whether incoming, outgoing, draft or posted items get dredged.
- Message Status: You can decide whether to dredge an item based on its GroupWise flags.
  - Default is to dredge all items, regardless of flag status.



By default, all items are selected for collection.

Scope

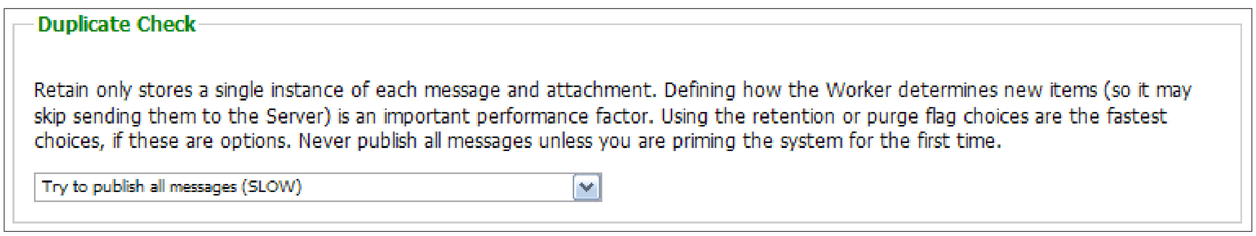


Date Range
The Date Range determines which message items are collected, depending on the date of the message. While the default is to collect all messages, regardless of dates, the administrator will **want and need** to change this. Dredging all messages makes sense **only** when you are collecting data for the very first run (priming the archive). On a day-to-day basis, however, the performance toll will be intolerable.

For instance, you may want to dredge everything once and then make a daily or weekly dredge for items that are '**n**' days old. These limited-scope dredges will run much more quickly and they will save you bandwidth. See below under "duplicate check.

Sometimes, you might just want to dredge items that fall within a specific date range. Specify that here.

Duplicate Check



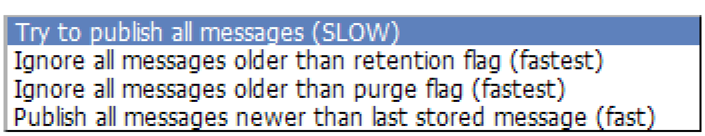
Retain is a single-instance-storage system. In other words, any given message is stored only once, to eliminate wasted disk space. Therefore, there are mechanisms in place to check for duplicates as messages are dredged and stored. The Retain Worker dredges the messages, sends them across a network link to the Retain Server and the Retain Server stores them in the database.

Eliminating duplicates will save network bandwidth and it will eliminate wasted disk space.

The Retain Server will check for duplicates before a message is stored. However, sending megabytes of messages and attachments to the Retain Server only to have them discarded because "they are already here" wastes processor time and the network bandwidth between the Worker and the Server. Therefore, you want to be able to do some checking at the Worker side.

If you are using the Reload™ integration, the item store flag is the only duplicate check flag that will work. The Retention and Purge flags will not work against a Reload backup.

In this section, you will tell the worker how to decide whether to dredge a message.
Here are your options:



"Reload" is a trade mark of GWAVA Inc., 100 Alexis Nihon, Suite 500, Saint Laurent, Quebec H4M 2P1

- **Publish All Messages**: No duplicate checking.
  - Every message is sent to the Server.
  - The Server is responsible for duplicate checking.
  - If there are duplicates, the Server will discard them.
  - This is the slowest option.
- **Use SmartPurge Flag:** Uses the GroupWise flags to determine the newest message.
  - Fastest option.
  - Compares time stamp of the flag to run time.
  - Ignores messages older than flag's time stamp.
  - It is NOT a usable option when dredging from Reload.
- **Use Retention Flag** functions very similarly to the SmartPurge flag.
  See below for a comparison
- **Use Item Store Flag** Use an internally stored timestamp.
  - Similar in function to GroupWise Retention/Purge flags.
  - Determines last message stored.
  - Fast option but not as fast as Retention/Purge flags.
  - Ignores messages older than flag's time stamp.

Set Flags:
As discussed previously, Retain can use the SmartPurge, Retention, and/or the Item Store flags. Select which flags should be "advanced" (in their timestamp values) as items are archived by this profile. Normally, the Retention flag is the one most administrators will wish to use.

NOTE: Generally, if you're using a backup system that leverages SmartPurge, like most backup software, (such as GWAVA Reload), does, you will not want to touch that flag.

About GroupWise's Smart Purge and Retention Flags

The SmartPurge, Retention, and Item Store flags all perform similar functions. The SmartPurge and Retention flags are stored internally in the GroupWise post office on a per-mailbox basis. The Item Store flag is stored by the Retain Server internally in Retain's own configuration database.

Each can be thought of as simply a "timestamp" indicating the last time data was retrieved by a 3rd party application. There are a few subtle differences between the three flags, which are discussed below.

The SmartPurge flag was introduced by Novell in GroupWise version 6.0.
With **SmartPurge** enabled in GroupWise:

- The flag is a timestamp, stored in the user's mailbox.
- Items older than the timestamp can be deleted freely.
- Items newer than the timestamp cannot be deleted.
- A 3rd party application, such as backup software can retrieve and/or set this timestamp value. GroupWise never changes the timestamp value.
- The initial purpose of this was for backup software. Backup software can either manually or automatically, (via the SMS TSAGW component of GroupWise), advance this timestamp once all items are backed up. The backup software can also use this timestamp to "know" that all items older than this timestamp have already been backed up, and can be skipped.
- Retain can use this flag to skip archived items, and automatically advance it as well. However, in practice, you'll rarely want to do this, because backup software, including GWAVA Reload, already uses this flag. There's no way to "share" the flag.

Because makers of retention and compliance software wanted a flag of their own, one that wasn't shared with the backup software SmartPurge flag, the Retention flag was introduced by Novell in GroupWise 6.5.1.

In almost all respects, the Retention flag is exactly identical in purpose and function to the SmartPurge flag. Like the SmartPurge flag, it is stored internally, and is primarily used to prevent premature deletion, and to skip previously stored messages. In fact, these are so identical in purpose, in theory virtually all backup software could switch to using the Retention flag, and all Retention software to the SmartPurge flag, and you'd notice almost no difference. The primary difference is simply it's a different value, used by different vendors.

There are some *small* distinctions:

- It's enabled and configured in a different location in ConsoleOne.
- It cannot be enabled or configured until a Trusted Application (like Retain) is installed and specifically requests it be made available.
- The SmartPurge flag is turned on/off globally. The Retention flag can be configured at the Domain, PO, or user level.

Most customers using Retain will want to use the Retention flag. It's logical and consistent to do so, and avoids conflict with backup software. It is recommended that you use this flag unless there is a compelling reason not to. A few possibilities are discussed below.

Retain can use the SmartPurge and Retention flags. In addition, a third flag, the Item Store flag is also available for use. The Item Store flag is similar to the other flags, but has some important differences:

- It's stored in the Retain Server's configuration database, instead of in GroupWise. This rarely matters much, but it does mean that the existence and storage of the flag is not dependent on the existence of the mailbox.
- Just like the SmartPurge and Retention flags, it can be used by Retain to skip previously archived messages, enormously increasing performance.
- Unlike the SmartPurge and Retention flags, it <u>cannot</u> be used to prevent users from prematurely deleting message items before they are stored by Retain. Given this severe limitation, the administrator might well wonder why this flag is useful...

It's true that you cannot prevent premature deletion using the Item Store flag. However, there are two scenarios where the Item Store flag becomes useful or even essential:

- The first is if for some reason the administrator needs to run multiple jobs or profiles on mailboxes that overlap. In this case, two separate flags are needed so the two different jobs can keep track of where (or more accurately WHEN) to continue archiving from. Admittedly, this is a rare scenario, but without a separate flag, your options would be severely limited.
- More commonly, consider the case of GWAVA Reload. Customers have expressed interest in using the backups created by GWAVA Reload to feed Retain, avoiding unnecessary network bandwidth utilization. But you cannot do this with the built in SmartPurge or Retention flags!
    - GWAVA Reload already uses the SmartPurge flags, and date ranges and profiles between Reload and Retain don't necessarily (and in fact rarely do) match.
    - The Retention flag would be perfect, but Retain isn't able to change the Retention flag. Or more accurately, it is changing it <u>on the Reload box</u>, not on the live GroupWise server.

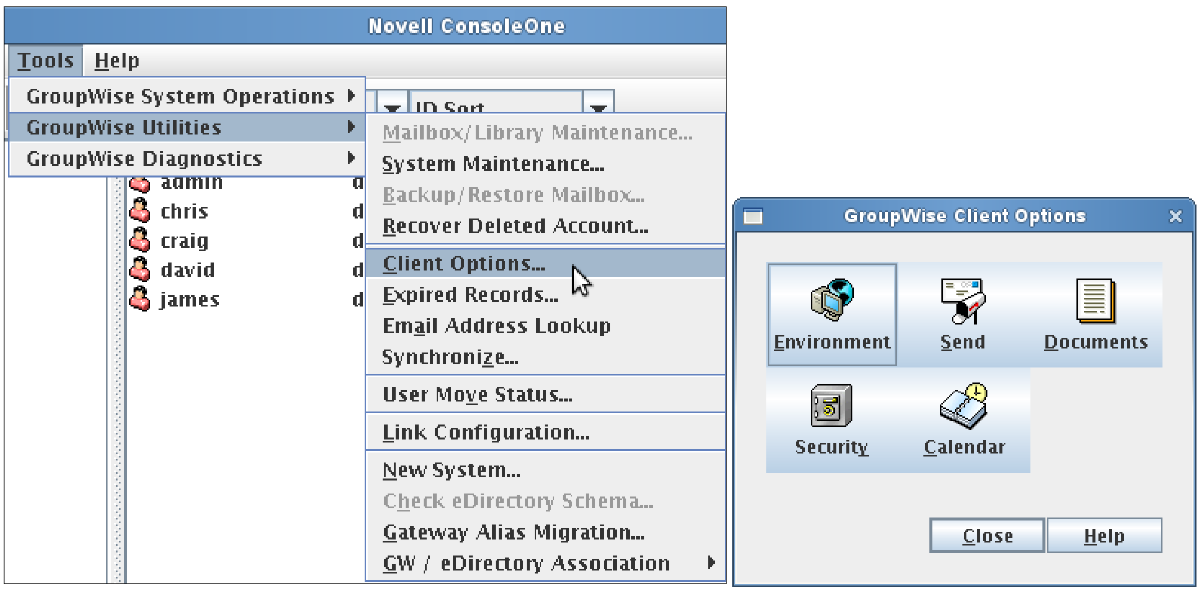
Hence, the changes will never be synchronized with GroupWise, leading to the disastrous results of:

- Users will never again be able to delete e-mail from the live GroupWise system.
- Retain will rescan the entire post office every night, because Reload will make a new backup, with an unchanged Retention flag!

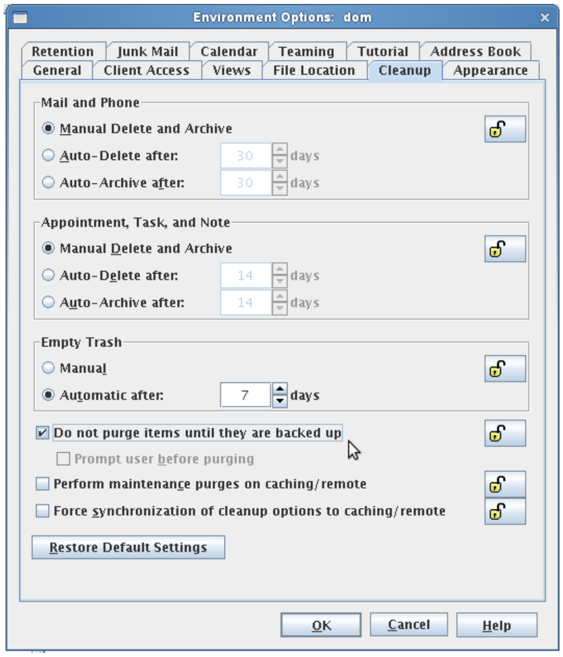
➢ The situation is resolved by using the internal Item Store flag.

Setting up SmartPurge and Retention flags in GroupWise 7

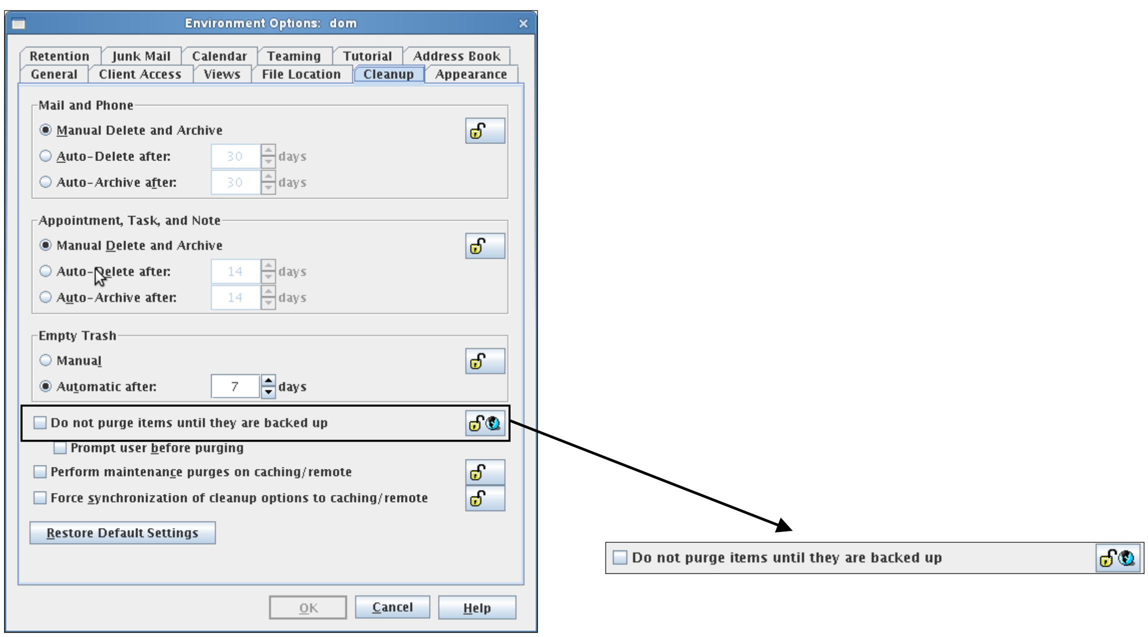
(Smart Purge Setup under GroupWise 8 is similar.)
Setup for both flags is accomplished in ConsoleOne:



1) Go into ConsoleOne
2) Select your domain or post office
3) Go to Tools | GroupWise Utilities | Client Options
4) Select Environment and the ‘Cleanup’ tab



Once here, SmartPurge is set up like this:



In the Cleanup tab, UNCHECK the box on "Allow purge of items not backed up" to ENABLE SmartPurge. Lock it to prevent users from disabling it.

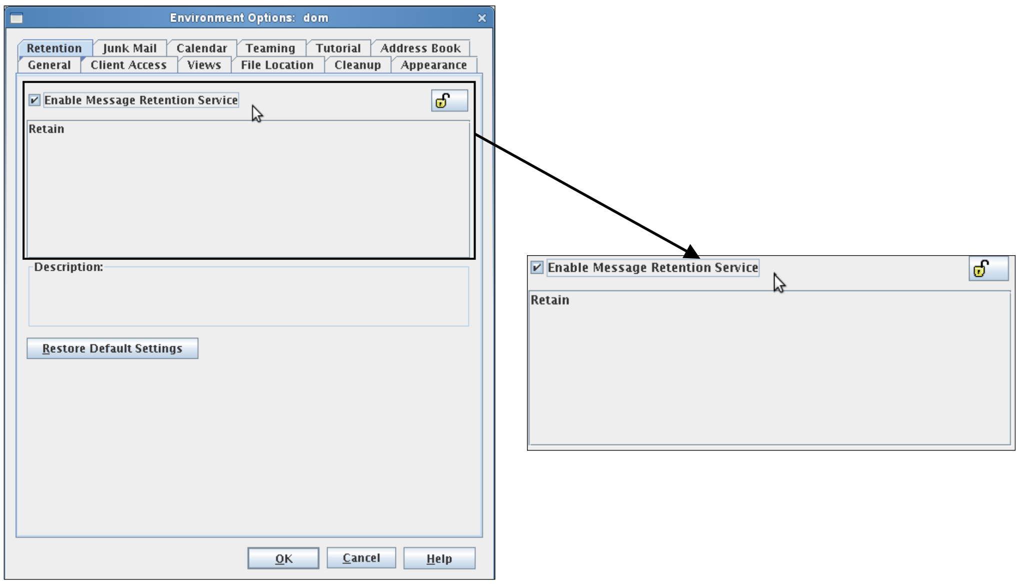
(GroupWise 8 uses reverse logic with the purge option. GroupWise 8 lists to "Do not purge items until they are backed up." Reverse the setting for the desired effect.)

Several different backup-retention services may currently use this same timestamp. Plan your system accordingly as Retain also uses this flag. The SmartPurge feature ONLY uses the backup / purge flag set as shown above. If another flag is desired, use of the Item Store Flag is recommended.

Retention Flag

The Retention flag is set up a little differently than SmartPurge. (This is only used when Stubbing.)

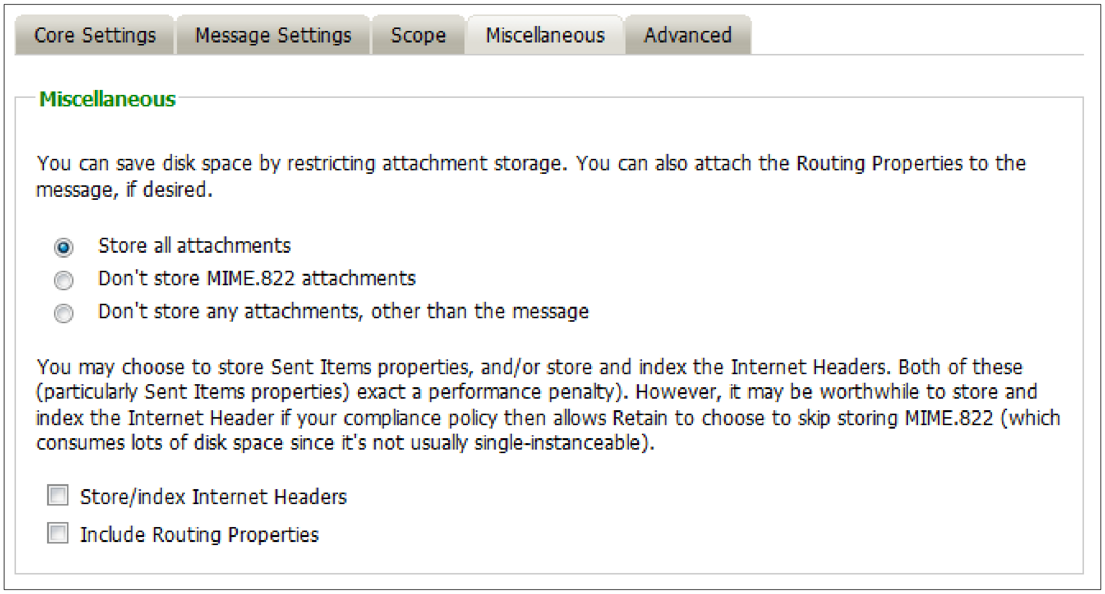
1) A Trusted App requesting Retention Services must be created. (Done at Retain setup time).
2) The Retention flag is enabled on a per domain/po/user basis.
3) From the 'Retention' tab under Environment Options, the setting should look like this:



Notice in this example that Retain is listed as a trusted application. This was done during our post-install tasks when we ran the Trusted Application Key program.

Next, CHECK the box to ENABLE the Retention Flag service. Lock it on.

Miscellaneous



Miscellaneous: What to do with attachments

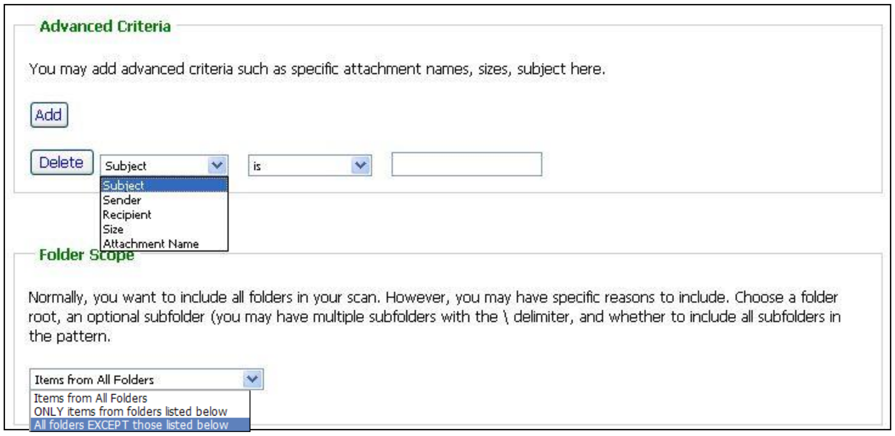
Most of the time, you will want to store all attachments. That is the default.

But if you don't want to store attachments, you can control this here. Note that the attachment names and sizes will still be listed when viewing the message, but the attachments will be clearly marked as unavailable.

Retain can stores the Index or Internet Headers and the Routing properties of messages. This information is stored in a XML attached to the message document and is searchable.

Store/index Internet Headers
This option tells Retain to store the headers in the SQL database. In order to use the header search option in the search interface you must have this option selected. To save disk space and still satisfy storage compliance, select this option and select "Don't store the mime.822 attachments". All other parts of the MIME file are already being archived, so if you store and index the Internet Header, you will already be archiving all information required.

Advanced



Advanced Criteria
If you want to be more specific as to what to dredge or not to dredge, add the criteria here. Each line will be ***logically AND***-ed together.

Think "Dredge all items where the following is true:"
Criteria A ***and*** Criteria B ***and*** Criteria C etc.

You may select based on:
- Subject
- Sender
- Recipient
- Size
- Attachment Name

Whether they are equal to, not equal to, whether they contain or do not contain the item you specify.

This gives you great flexibility and granularity. It allows you to customize dredges and retention for many different groups, or even individuals.

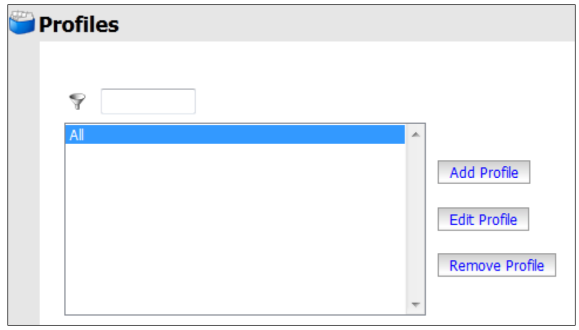
Folder Scope
By default we dredge items from all folders. You can specify one or more inclusions or exclusions.
Your choices are:
- Dredge everything
- Dredge only these listed folders
- Dredge everything EXCEPT these listed folders

How to specify the list of folders to dredge/exclude:

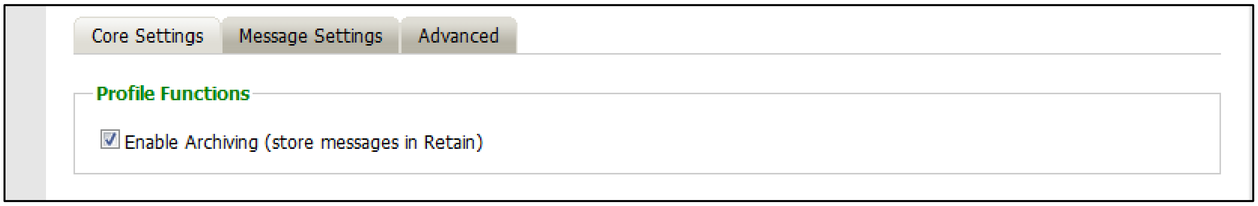
6) Specify a System Folder (mandatory). Example: Calendar.
7) You specify a subfolder of that folder (optional).
   Example: entering "old" would mean the folder "old" under "Calendar".
8) You can have multiple hierarchies under that with the / delimiter.
   Example "old/mail" would mean the subfolder "mail" under "old" under "Calendar".
9) You specify if the option includes subfolder.
   Example: If you select "old" and "includes subfolder" is unchecked, "Calendar/mail" is selected. If "includes subfolder" is CHECKED, "Calendar/old/mail" would also be selected.

Social Messaging Profile

To create a new profile to archive social messaging data, first select the 'add profile' button and name the profile. Then continue configuring as desired.



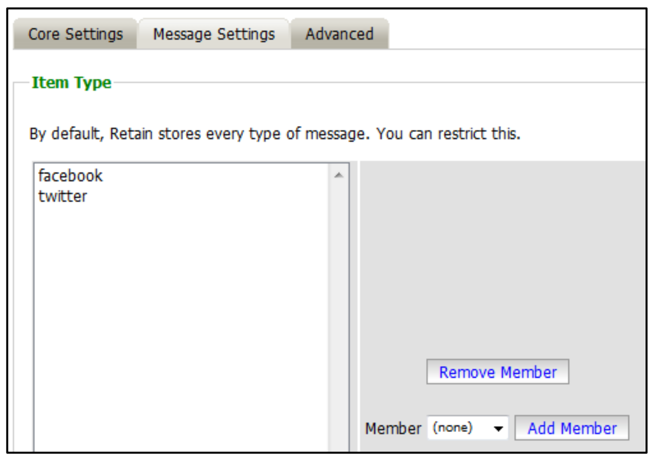
The **Core Settings** tab holds the enabling setting, which allows jobs connected to this profile to run. This must be checked before jobs will run.



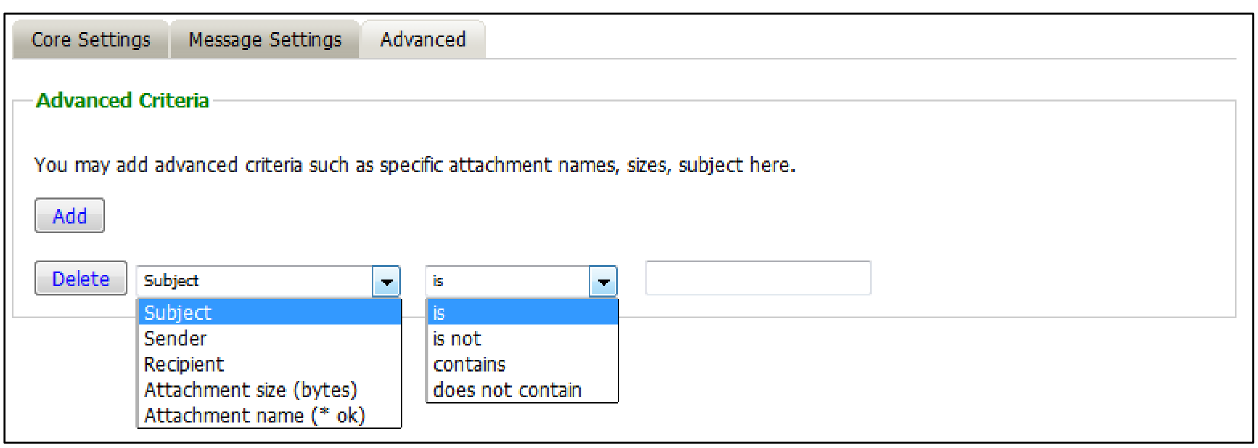
The **Message Settings** tab can be used to exclude or include specific data types for this profile. By default all types of messages will be archived. If left blank, the default will persist.

If only specific data types are to be included in a profile, they can be selected from the Member drop-down list, and added to the inclusion list.

All types of data included in the list will be archived. If the list is blank, all users and data will be archived.



Under the **Advanced** tab, specific criteria can be used to restrict the archived data. Any combination of the variables listed may be used to restrict the data selection. Advanced criteria may be added up to 7 fields.

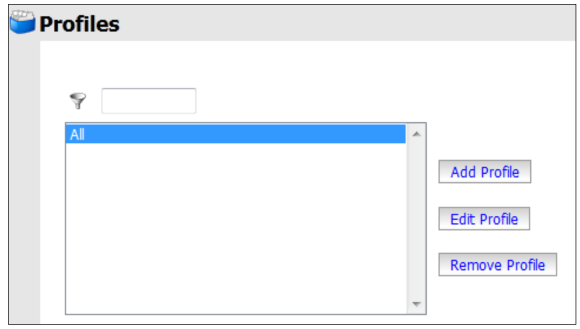


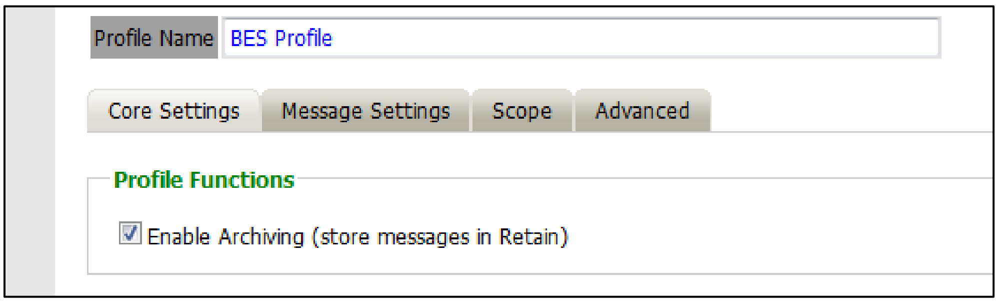
Save changes and the profile is configured.

BlackBerry Profile

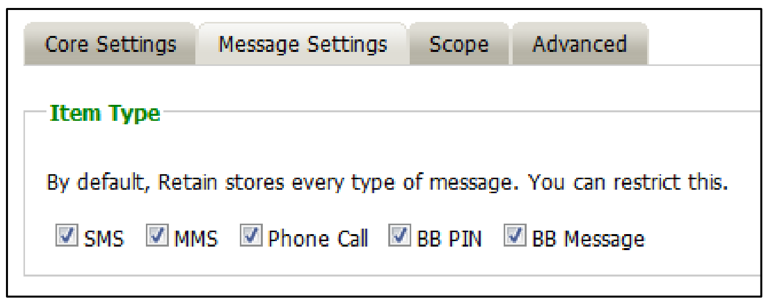
To create a new profile to archive BlackBerry data, first select the 'add profile' button and name the profile. Then continue configuring as desired.

The **Core Settings** tab holds the enabling setting, which allows jobs connected to this profile to run. This must be checked before jobs will run.

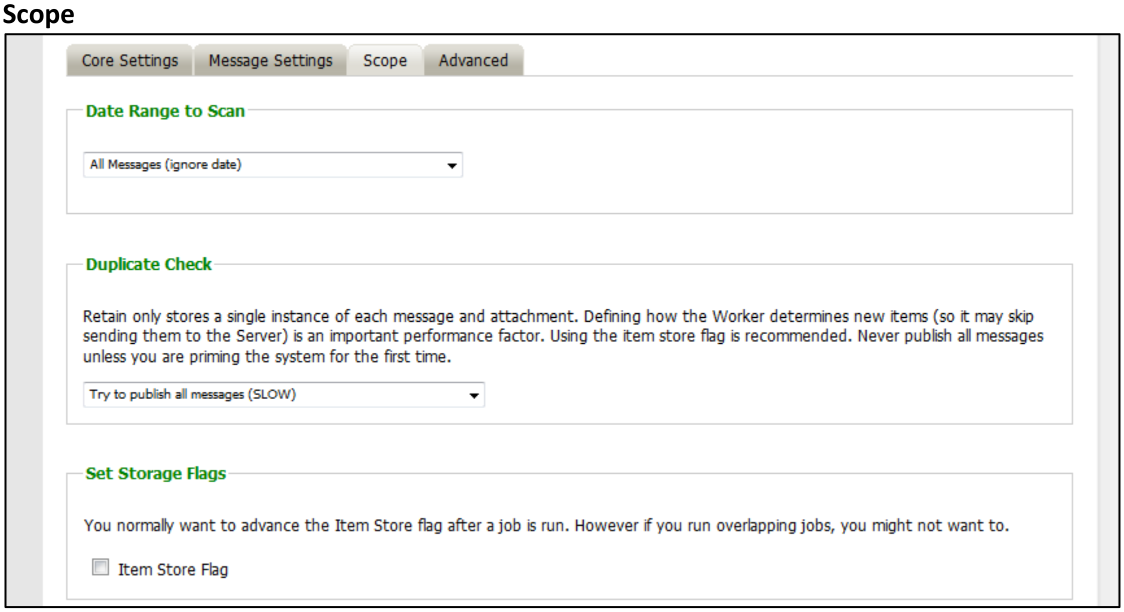




The **Message Settings** tab can be used to exclude or include specific data types for this profile. By default all types of messages will be archived. All BlackBerry data which is selected to be archived MUST be logged in the BlackBerry Enterprise Server or the data will not be available for Retain to archive it.



Scope



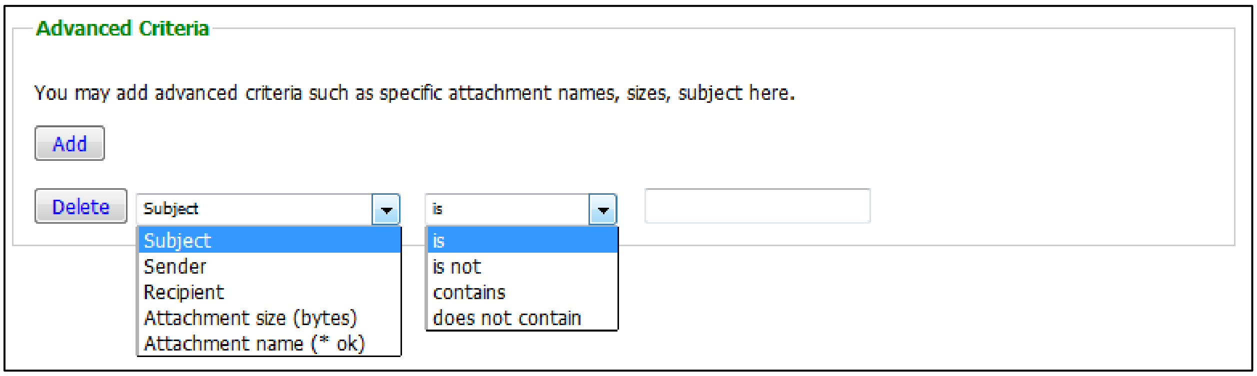
The Scope tab dictates how pervasive the attached archiving jobs are, and what kind of duplicate checking is done, or not done, in the Retain system.

The Date Range instructs Retain to scan for, and archive, messages after, or before, a certain date. This is useful if only specific chunks or areas of mail are to be archived.

The duplicate check either scans for all messages, or instructs Retain to only look for messages which are newer than the Item Store Flag, which is a time-stamp on the system. All messages newer than the time stamp will be archived by Retain if the item store flag is utilized, but Retain will ignore all messages which are older.

It is recommended to have at least the first job archive everything, with the item store flag checked to archive everything possible in the logs, while setting the item store flag. Subsequent jobs should use the duplicate check and the item store flag to only archive new data afterwards.

Advanced



If you want to be more specific as to what to dredge or not to dredge, add the criteria here. Each line will be ***logically AND***-ed together.

Think “Dredge all items where the following is true:”
Criteria A ***and*** Criteria B ***and*** Criteria C etc.

You may select based on:

- Subject
- Sender
- Recipient
- Size
- Attachment Name

Whether they are equal to, not equal to, whether they contain or do not contain the item you specify.

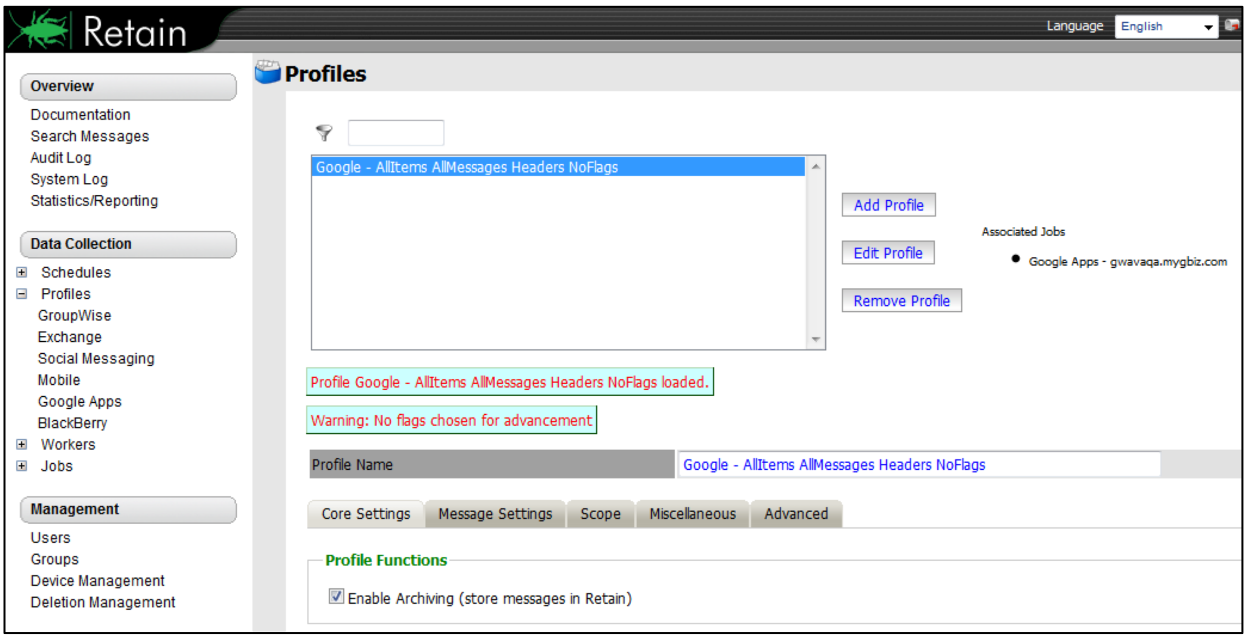
This gives you great flexibility and granularity. It allows you to customize dredges and retention for many different groups, or even individuals.

Google Apps Profile

To create a profile to archive email and data from Google Apps, select the add profiles button and name the profile then continue configuring as desired. The Google Apps profile must be configured and all settings saved before a job can be created and run.

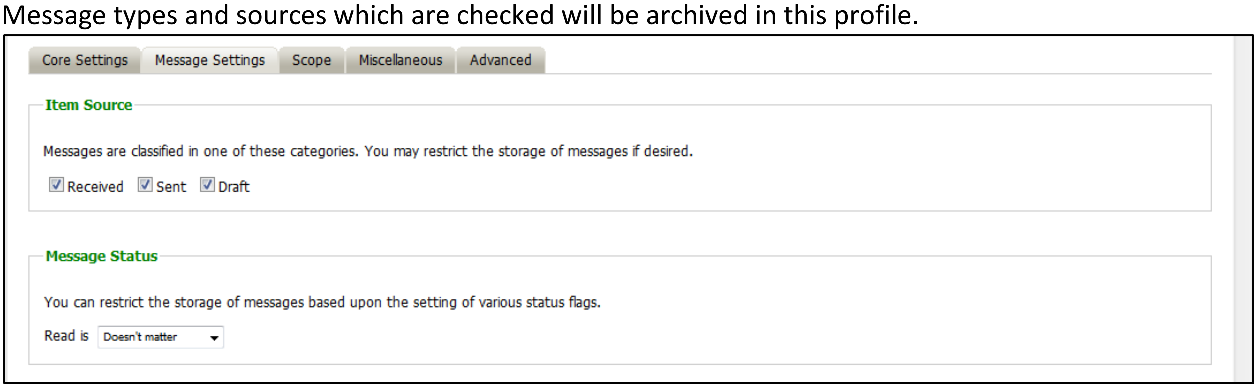
Core Settings

The profile will not become active and will not allow jobs to be run unless the profile is enabled. Enable the profile by placing a checkmark in the 'Enable Archiving' checkbox.



Message Settings

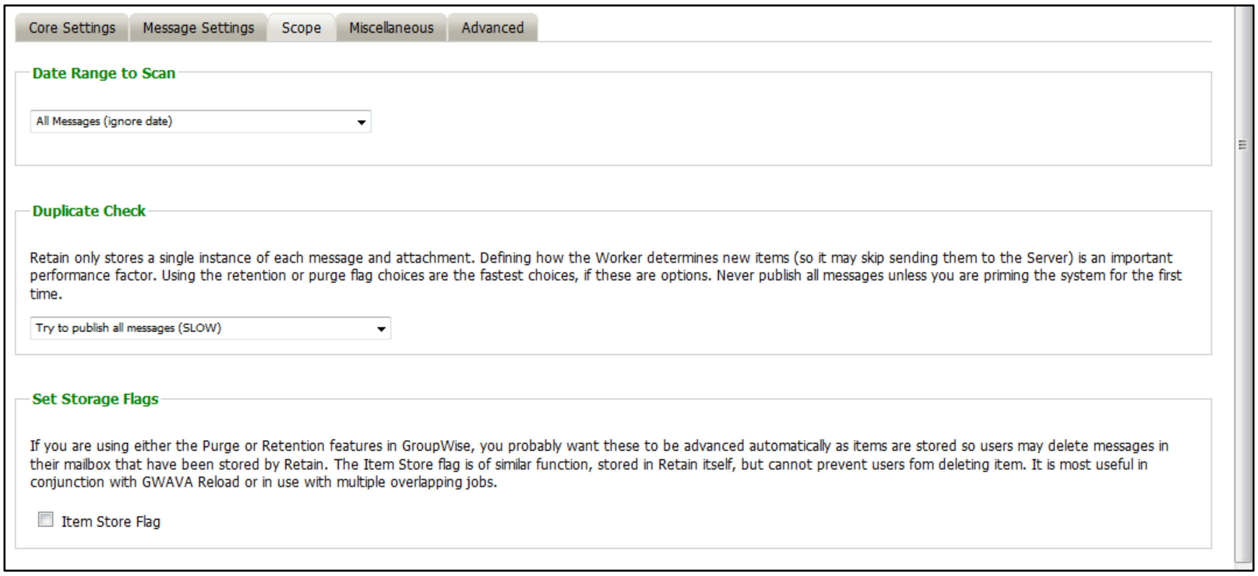
The Message Settings tab contains the source and status settings for the messages to be archived. Message types and sources which are checked will be archived in this profile.



Any item type or status which is not selected or specified will exclude qualifying items from being archived in Retain.

Scope

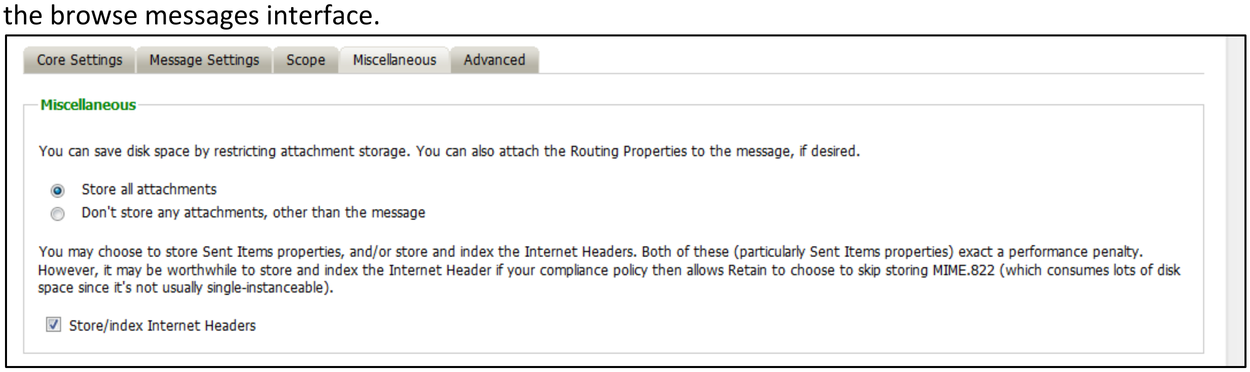
The Scope tab covers the Date Range, Duplicate Check, and Storage Flags. The date range limits the data items archived based on when it was created or sent. The Duplicate check is the method used to eliminate already archived messages from an archival job. Initial jobs should be left to archive all messages, as there are no messages currently archived in the system. Afterwards, the duplicate check should be set to use the storage flag which only attempts to archive messages which are not already in the archive, thus speeding the archival process.



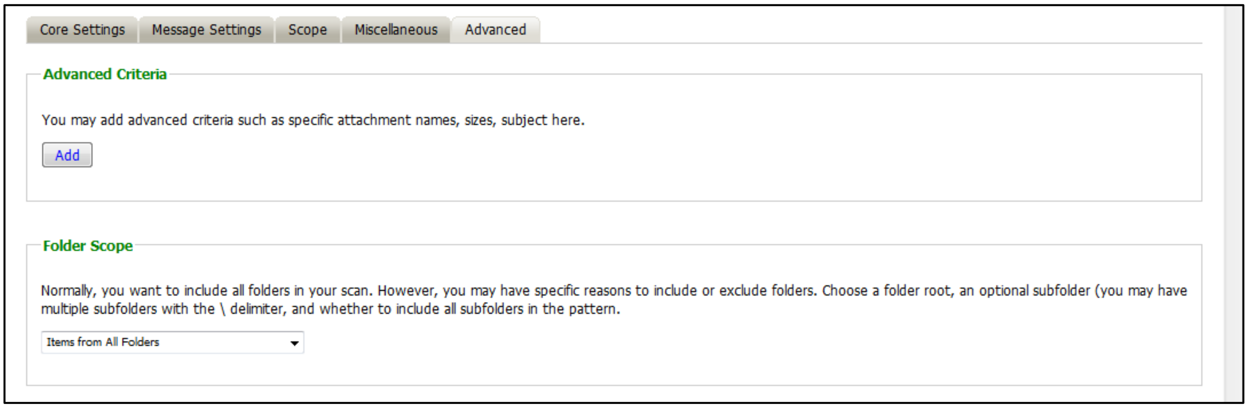
Storage Flags are markers which Retain uses to keep duplicate data items from being added into the archive. This option should be enabled to allow Retain to only archive original data.

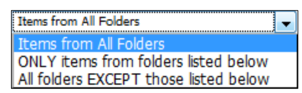
Miscellaneous

The miscellaneous tab allows the configuration to allow or deny archiving and indexing of attachments in Retain. If attachments are to be archived, they may also be indexed to provide searching capability in the browse messages interface.



Advanced
The advanced tab allows the administrator to be even more specific in what to archive and what to exclude. The criteria added under the 'advanced' tab will limit associated jobs to only the items matching the criteria. Up to 6 lines of advanced criteria may be added to each profile. Each additional line will be ***logically AND***-ed together. For example, the system will archive all items where the following is true: Criteria A ***and*** Criteria B ***and*** Criteria C etc.

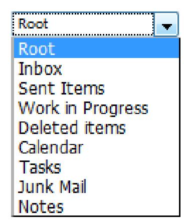




You may select based on:

- Subject
- Sender
- Recipient
- Size
- Attachment Name

Whether they are equal to, not equal to, whether they contain or do not contain the item you specify.



This gives you great flexibility and granularity. It allows you to customize archival jobs and retention for many different groups, or even individuals.

Folder Scope
By default we dredge items from all folders. You can specify one or more inclusions or exclusions. Your choices are:

- Dredge everything
- Dredge only these listed folders
- Dredge everything EXCEPT these listed folders

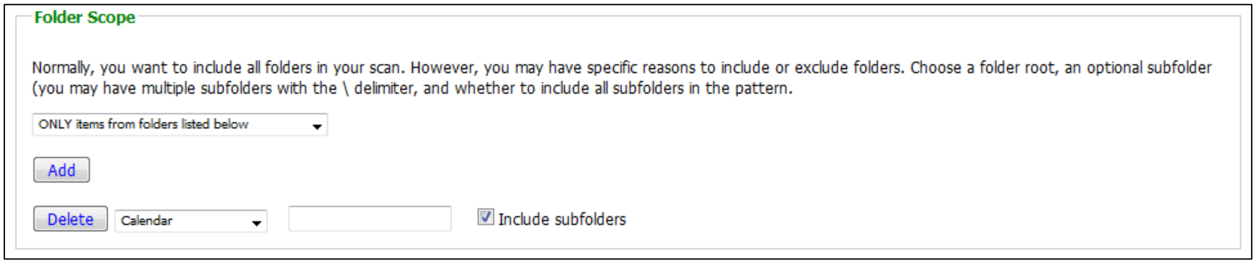
How to specify the list of folders to dredge/exclude:

10) Select 'Add' to open a new selection.

11) Specify a System Folder (mandatory). Example: Calendar.

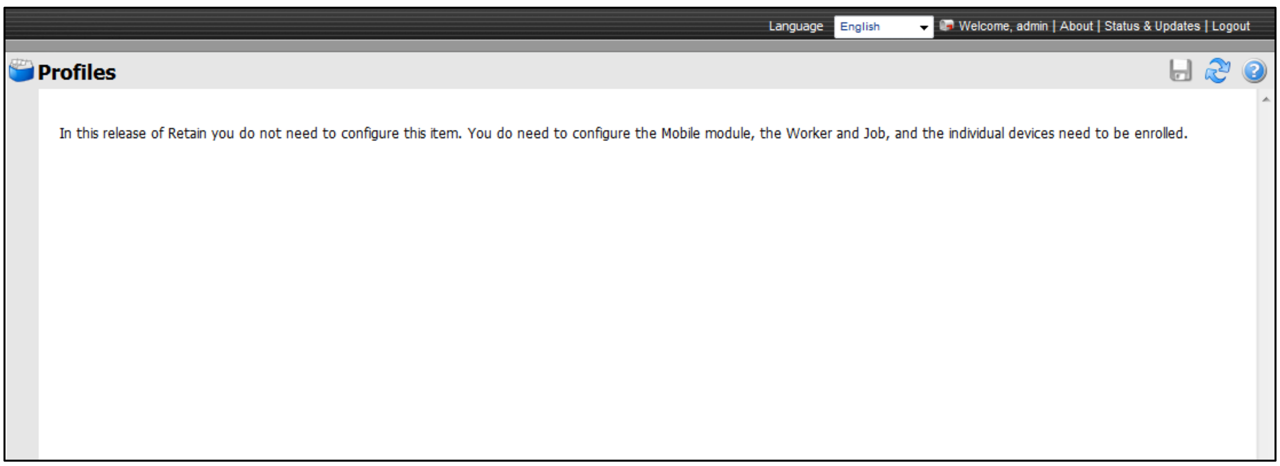
12) You specify a subfolder of that folder (optional).
    Example: entering "old" would mean the folder "old" under "Calendar".
13) You can have multiple hierarchies under that with the / delimiter.
    Example "old/mail" would mean the subfolder "mail" under "old" under "Calendar".

14) You specify if the option includes subfolder.
    Example: If you select “old” and “includes subfolder” is unchecked, “Calendar/mail” is selected. If “includes subfolder” is CHECKED, “Calendar/old/mail” would also be selected.



Mobile Profile

The mobile profile is unnecessary, as all the gathering of data items is performed by the configured router and application installed on individual Android phones.



There is no configuration necessary for the profile, however, as stated in the mobile module configuration section, the mobile module requires the setup and installation of the mobile application on the Android devices, registration of the individual mobile devices, and the Tenant ID created by GWAVA. Contact the appropriate sales representative for your area.

Workers

You will need to set up at least one Retain Worker. The Retain Worker does the actual work of collecting the data from a message system and delivering it to the Retain Server. The Retain Worker component is normally installed local to each GroupWise mail server, or any Exchange server from which you wish to collect data. Although a Worker may be installed on a machine running Retain Server, this is normally not recommended or sufficient, except for very small (100 or fewer users) systems or for evaluation purposes. Ideally, the worker you choose to dredge mail from a desired server is local to the server itself. Using a worker on "Server A" to pull data from a mailbox server on "Server B" is possible, but it will use up network bandwidth and will be slower than simply pulling data locally. For this reason, Retain was designed to allow you as many workers as you need, on Linux or Windows.

Worker Configuration Options

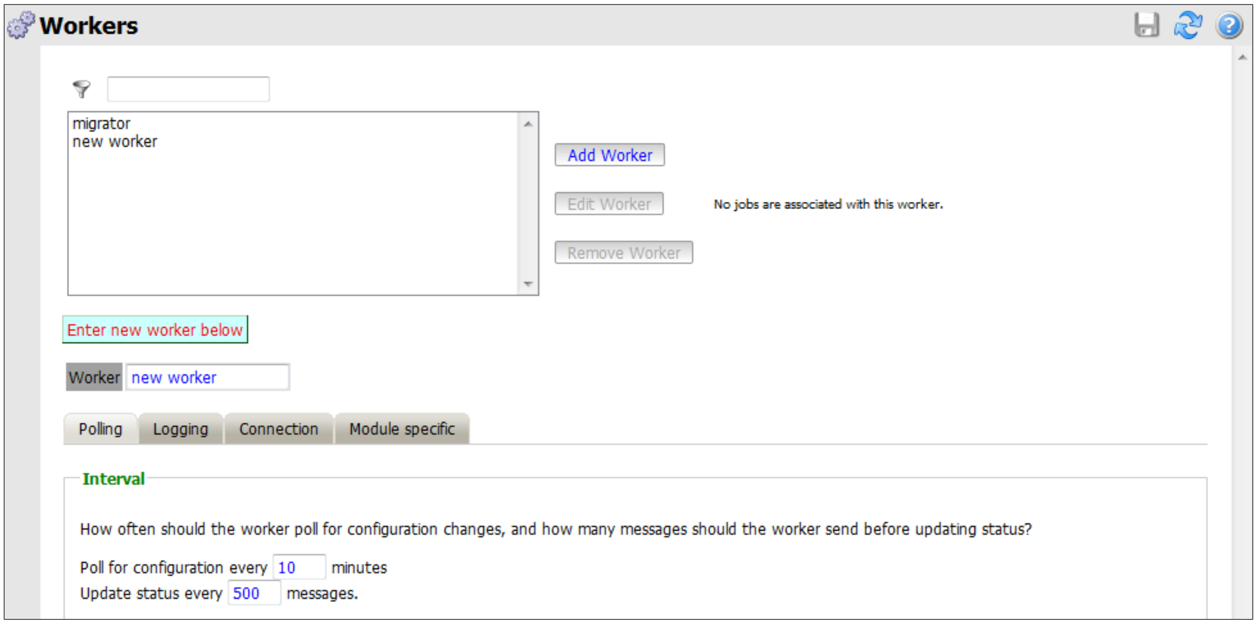
- **Polling:** Defines how often the worker polls for configuration changes. (Jobs, job changes, etc.)
    - Default is 10 minutes.
    - Default is to update the displayed status every 500 messages while running the job.
- **Logging** – Controls logging by the Retain Worker.
    - Default is NORMAL.
- **Connection**. ***Important.*** This is the information the worker needs to connect to the Server. Double check this setting.
    - Protocol
    - URL/host name
    - password
    - If the connection information is changed, you will need to manually copy the Retain Worker.cfg bootstrap file over to the Worker
        - **Correcting the Bootstrap**:
            1) Stop Tomcat.
            2) First delete the Retain Worker.cfg file on the Worker machine. For security reasons, there is no way to do this except by manually deleting the file from the server console itself. The path is: Retain Worker/WEB-INF/cfg. Removing the bootstrap resets the worker to initial configuration.
            3) Restart and re-upload the bootstrap to the worker.
- **Status** – Basic status information on the Worker. This status information is updated while the

worker is running according to the “Update Status” interval described above.

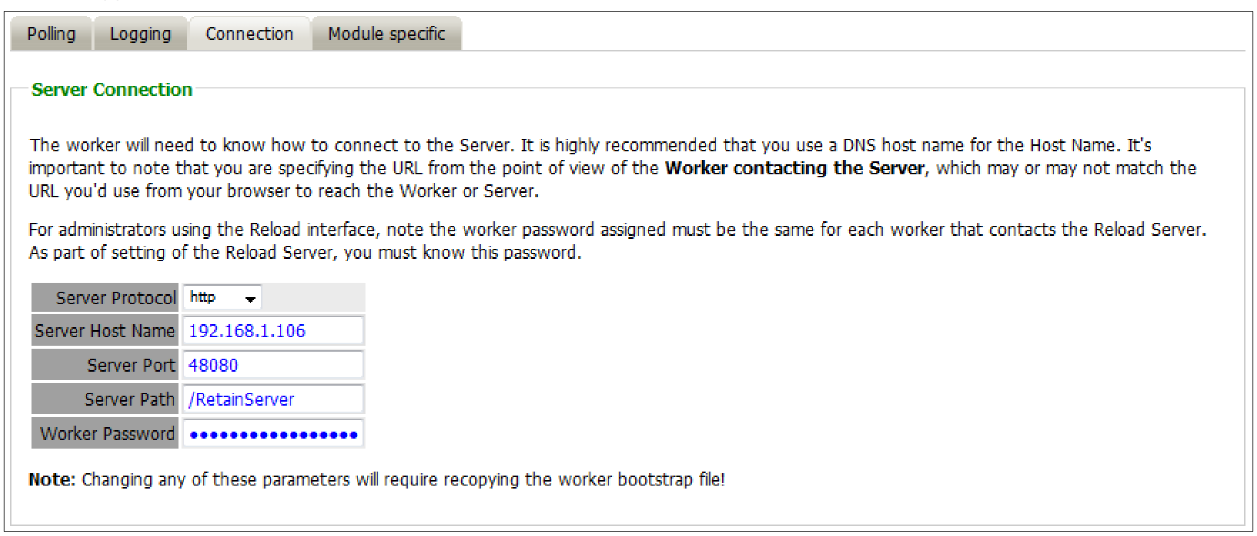
- **Bootstrap** – Indicates the download link and when it was last downloaded.

Worker Configuration

From the Retain home page, click Workers. You will see this screen:



1) Click “Add Worker”.
2) Put the name of the worker in the “Worker” box. *Example:* “Linux Worker 1”.
3) Check the Connections Tab to be sure the Retain Server IP address settings are correct. This tells the Worker where the Retain Server is located. (Server Host Name or IP address must be correct; this should be populated automatically, but double check for accuracy.) The Server Connection setting must be able to resolve to the Retain Server if placed in a browser address bar.



The Connection tab holds very important contact information for the worker's connection to the Retain Server and the Post Office. Make sure that the Retain Server connection address is correct, or the Retain Worker will not be able to talk to the server.

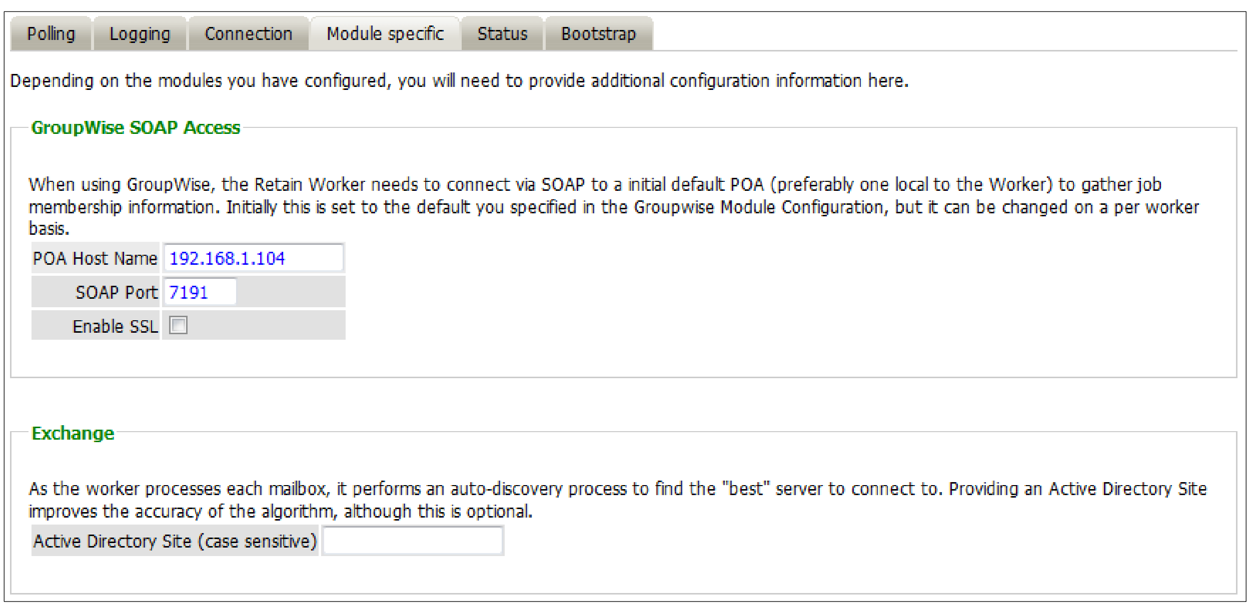
Double check all these settings to ensure that you will have the best performance and connection for your system.

IMPORTANT NOTE!

It is vitally important that the connection information is correct before you save the worker. On a single server system, it is easy enough – it's the same server. However, in an enterprise setting where you might be using different components on different servers, it is extremely important that each component knows how to connect to the Retain Server.

If you do not set this correctly, the Retain Worker will NOT be able to contact the Retain Server and it will not run jobs.

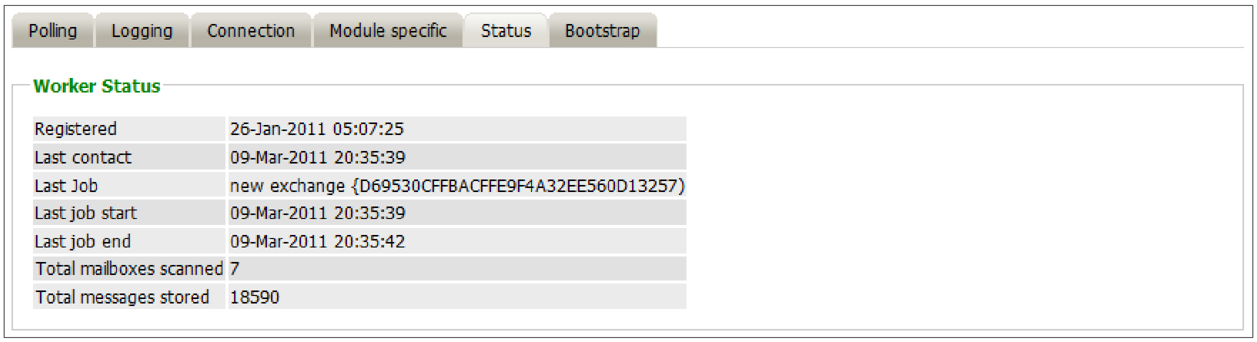
4) The Module Specific tab contains information specific to individually configured modules. With Exchange, you may optionally specify a specific Active Directory Site the worker is located in. That allows Retain to find the "closest" Exchange Server that is appropriate for the user to be archived. The settings specified here are tied only to the specific worker configured, and does not affect the rest of the system. In general this setting may be ignored unless required. If required, input the appropriate information.



5) After you have checked and set your settings, click "**Save Changes**" before browsing to another page to finish creating and to save your worker.

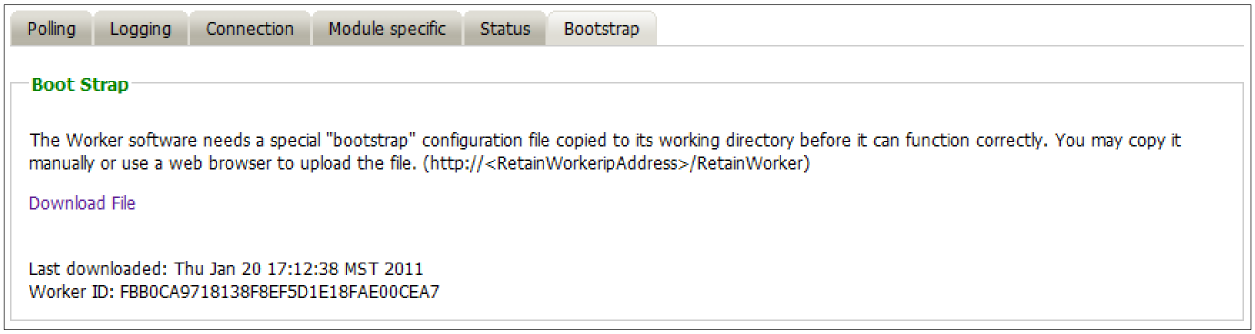
After the worker has been saved, two additional tabs become visible for settings on the worker. You MUST save changes on a newly created worker before the 'Bootstrap' tab is available to be used.

The status tab for the new worker will not hold any pertinent information until a job has been run or the worker has registered to the server and is in communication. Once a job has been completed, information will be displayed on the general status of the selected Worker.

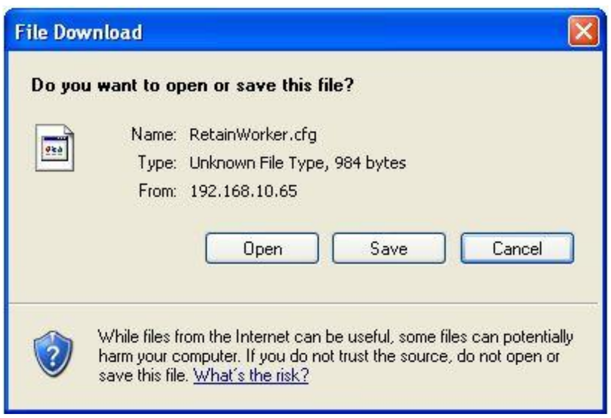


Check this page after the worker has completed connecting to the Server for information and jobs. After a job has been run, or is running, more pertinent information, such as total mailboxes scanned and messages stored, will be displayed.

6) After you have saved the changes, the Bootstrap tab appears (see below). Click “Download File” to save the configuration to a local workstation.



7) Save this file to your hard drive in a place where you can find it. Click “Save”.

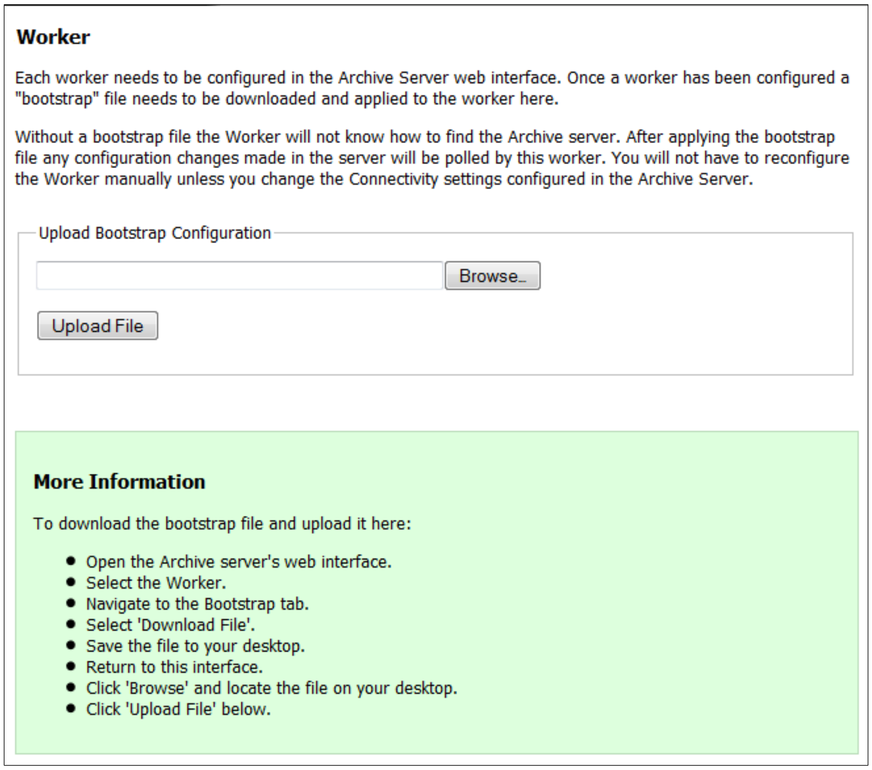


8) Open a new browser window and type:

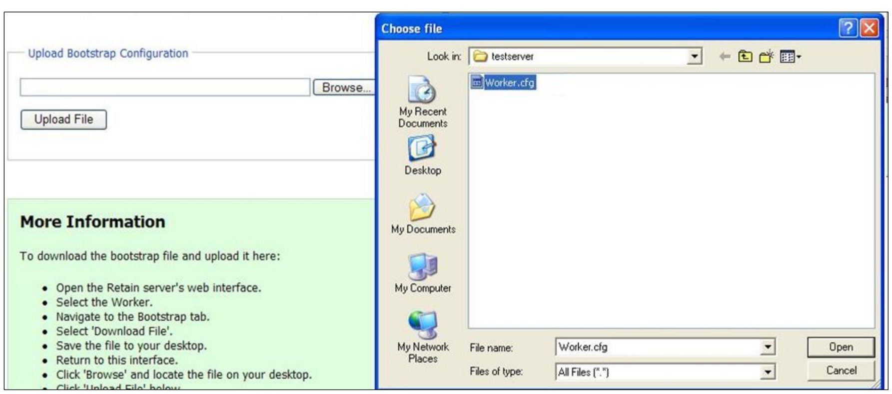
`http://< your-RetainWorker-ip >/RetainWorker`

This screen appears when a worker has not been initialized.

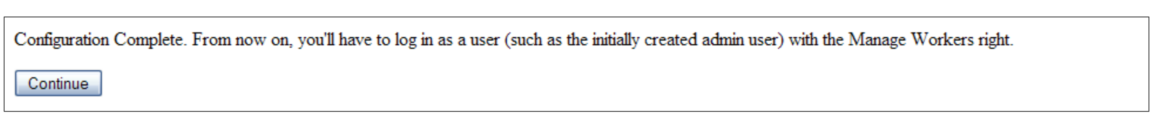
9) Upload the bootstrap file.



- Click "Browse" to find the file you just downloaded to select it.

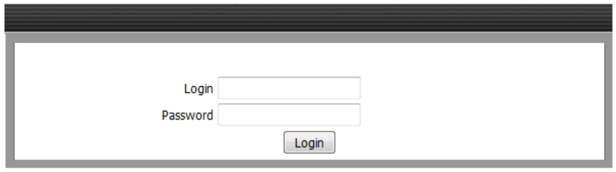


- Click "Open".
- Click "Upload File".
- If the upload went well, you will see this screen:

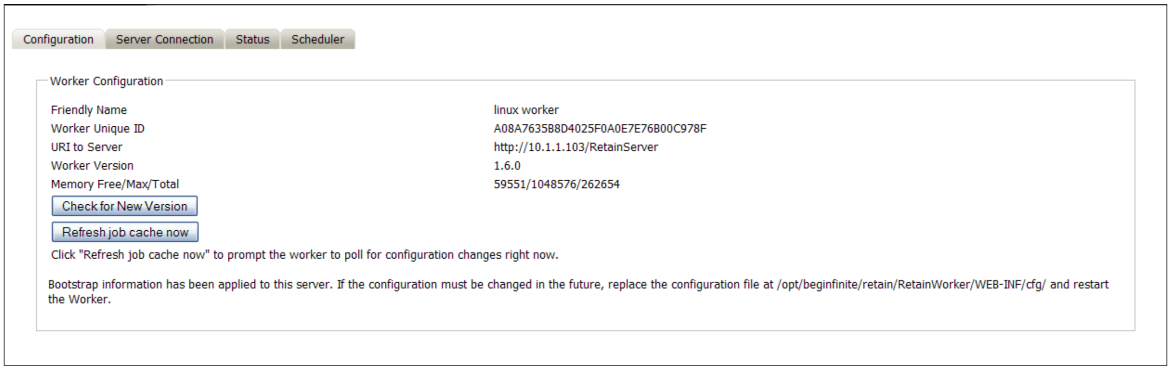


After you click the "Continue" button, you will be returned to the login page.

10) Login as Admin.

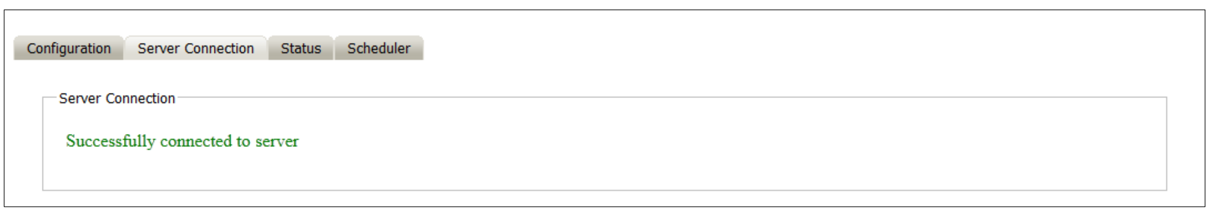


On all subsequent logins, you should be shown the configuration page first.



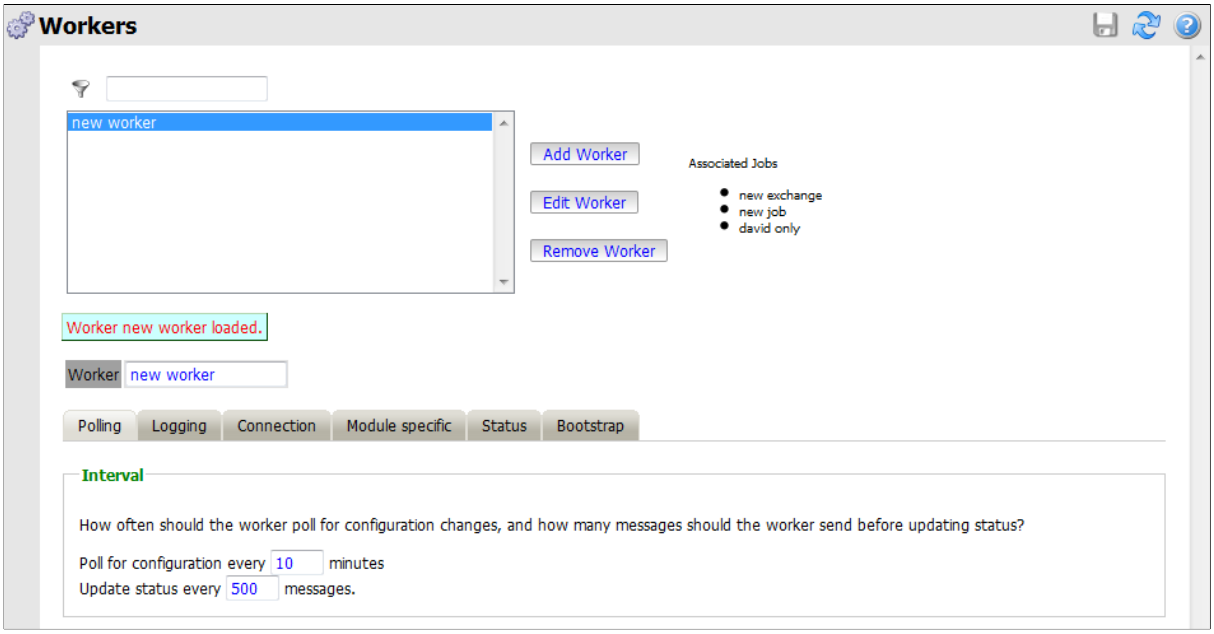
You should be able to see your configuration on the screen, as shown. The “Check for New Version” button checks for updates. The “Refresh job cache now” button tells the worker to poll the server for configuration changes and new jobs. After this button is selected, the Worker page will refresh automatically after the Retain Server has been polled. It takes just a few seconds.

11) Verify the Retain Server connection success by selecting the Server Connection tab.



- Go back to the Retain Server.
- Click “Workers”.
- Click on the worker you just created.

You should see the following:



Pay close attention to “Poll for configuration every ‘n’ minutes. This is how often Retain will check for new jobs.

Also, status updates are displayed on the admin page every ‘n’ messages.

Now, set logging to a level you would like. You may use “Diagnostic” at first, until the system is fully operational and tested. Please be aware, however, that using this setting will write a huge amount of data in the log files.

The **profiles**, **schedules** and **jobs** must be setup, if they already have not been, in order to begin actual data collection.

Jobs

Jobs are separated into different modules. A module, schedule, profile, and worker must be configured before a Job can be created. Module specific job menu's only display when multiple modules are configured. Jobs bring the entire configuration together to archive mail from the mail server, according to the configuration. Jobs are where data collection is achieved.

A job:

- Starts according to the selected **SCHEDULE**.
- Collects data according to the selected **PROFILE**.
- Utilizes the selected **WORKER,** and only the selected worker according to the schedule and profile.
- Collects data from the specified mail source, (messaging server, distribution list, group, and individual user)

Jobs look and act differently depending on which module they are configured under. Select the desired module from the Job menu, (or simply 'Jobs' if only module is configured), and configure according to job needs.

Exchange Jobs

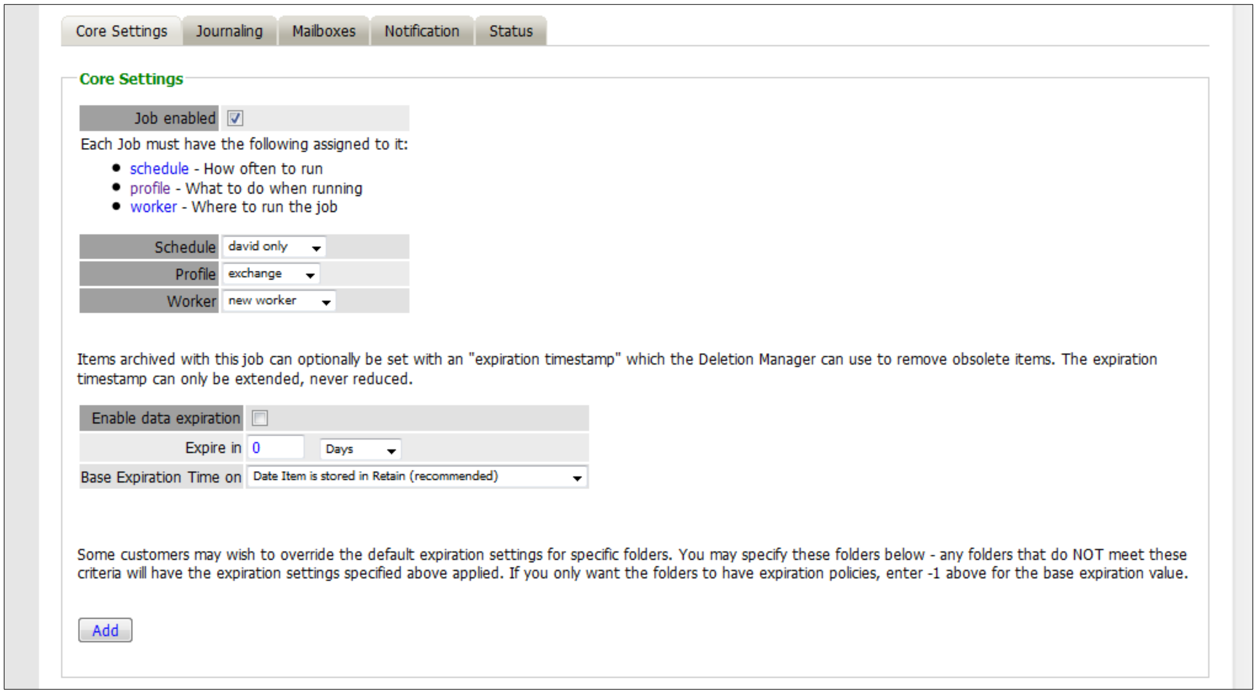
All mail archiving is accomplished through this interface because the methods to interact with the Exchange system are tied into this job interface. Only Exchange profiles will be able to be viewed or selected through this interface, and no other modules profile will be selectable here. However, schedules and workers are universal and can be selected in any modules' job interface.

To create a new job, select the 'Add Job' button and provide a name for the job. To save a job, the job must have a Profile, Worker, Schedule, and a mailbox, distribution list, or server to be archived. In other words, a job must have a time to run, types of things to get, something to get it with, and a target or a place to get it, in order to be saved and run.

A job without an assigned profile, schedule, worker, or mailbox cannot be saved.

Core Settings

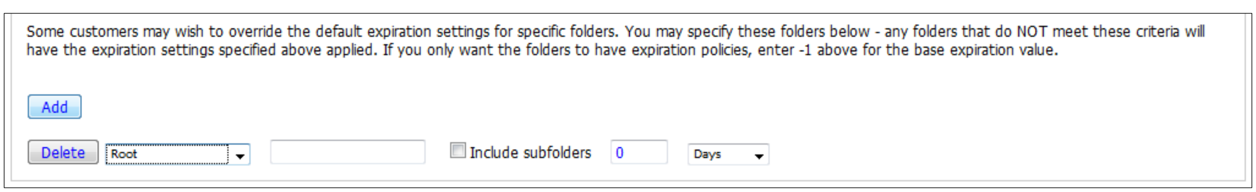
Under ‘Core Settings’ the profile, schedule, and worker are selected. Only existing profiles, workers, and schedules may be selected. The selected schedule will determine when the job is run; the Profile determines what kinds of mail are archived, and the worker is the agent which performs the work.



The data expiration is an option to place a timestamp on the mail in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date.

This time stamp simply puts a date on which the mail is “set to expire” and can be in days, months, or years. Mail that has ‘expired’ due to this time stamp will remain in the database until removed by the deletion manager Job Expiration is not retroactive for mail in the database and only applies to mail archived by the job that it is active for.

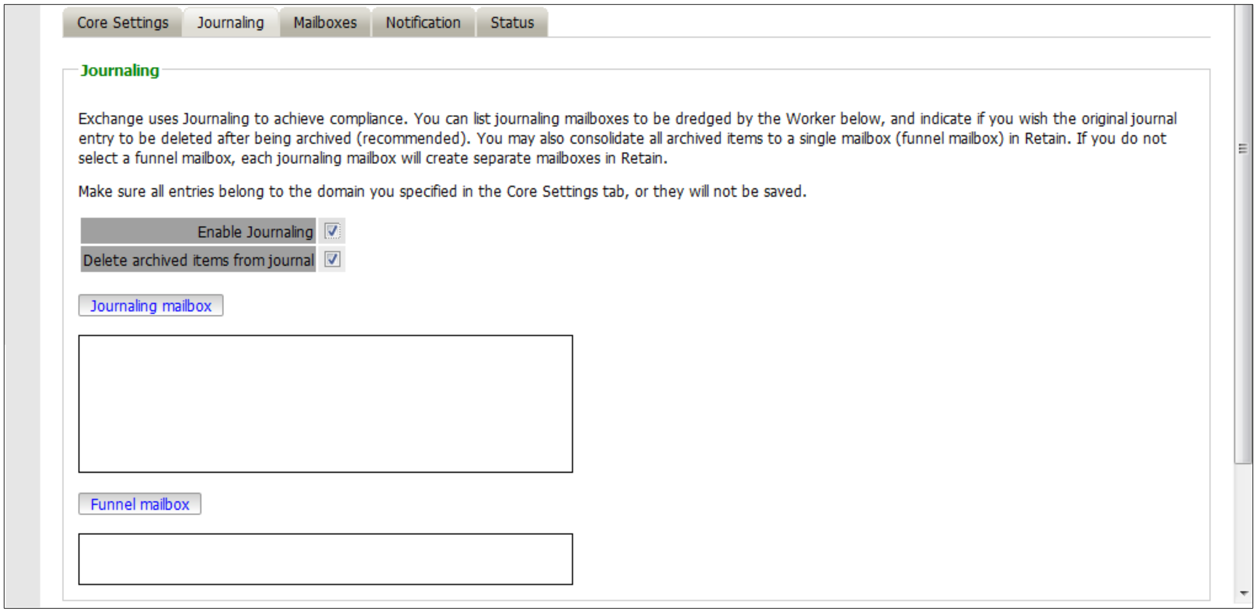
There may be some folders which it may not be desirable to place an expiration time stamp on. Such folders may be specified through the ‘add’ button at the bottom of the page.



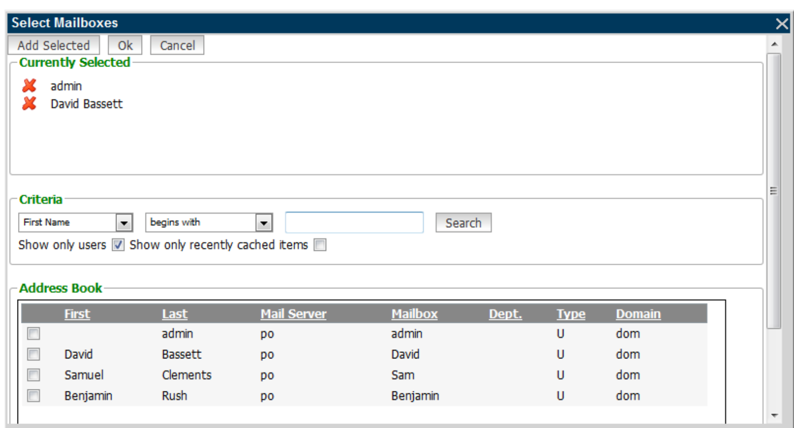
The base folders and criteria are specified here. All messages included in these folders will have a different date, if specified, or exempted from this expiration date. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

Journaling

Journaling MUST be enabled on the Exchange system, and Journaling mailboxes must be provided for legal archive compliance.



To archive messages contained in the Journaling mailbox, specify the Journaling mailbox by selecting it from the user/mailbox list. Open the mailbox selection window by selecting the 'Journaling mailbox' button and searching for the desired mailbox.



After searching for mailboxes and users in the cached address book, the users must be added to the list by selecting the checkbox next to the desired name in the search results box, then selecting the 'Add Selected' button at the top.

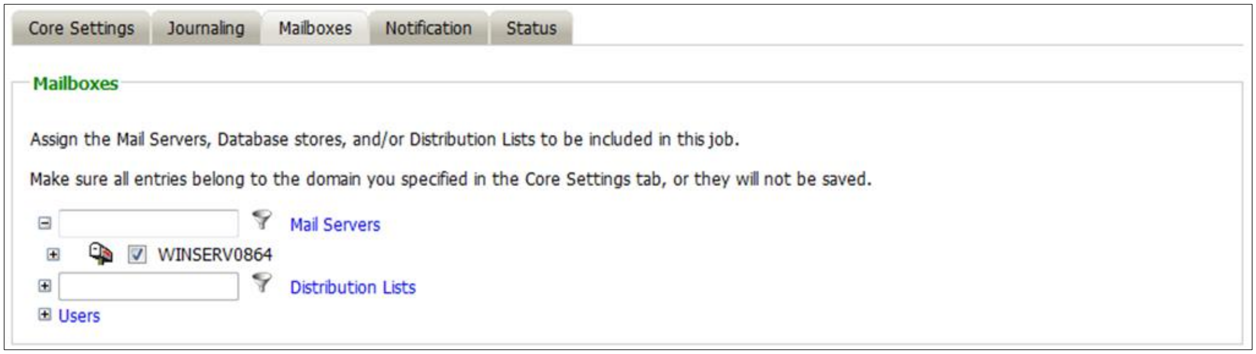
The red 'X' next to the names in the 'Currently Selected' list allows removal of selected items. Once the list has been configured as designed, selecting the 'Ok' button from the top of the window will add the selected names to the list.

A 'Funnel' mailbox creates a single mailbox in Retain that 'funnels' all the mail from all the different journaling mailboxes into one. If this is not specified, then each Journaling mailbox will be created and archived in the Retain system as any normal mailbox would be archived and created.

It is HIGHLY recommended to delete archived items from the journaling mailbox to avoid bloating the existing message system or requiring manual maintenance and management of the Journaling mailboxes.

Mailboxes

The final setting that a Job must have in order to be saved and run, is a target: where to archive mail from. The Mailboxes tab dictates where a Job will look for mail to archive. Only the users or mail server included in a job will be archived by the job when it is run.



Users may be specified separately, whole servers may be selected, and distribution lists spanning different servers may be selected. A job may span all the selected options, or only one of them, but jobs will be faster and more efficient if they are balanced in their scope, for instance, one separate job for each server each with its respective worker, to allow multiple jobs to be run simultaneously without overwhelming one server or worker.

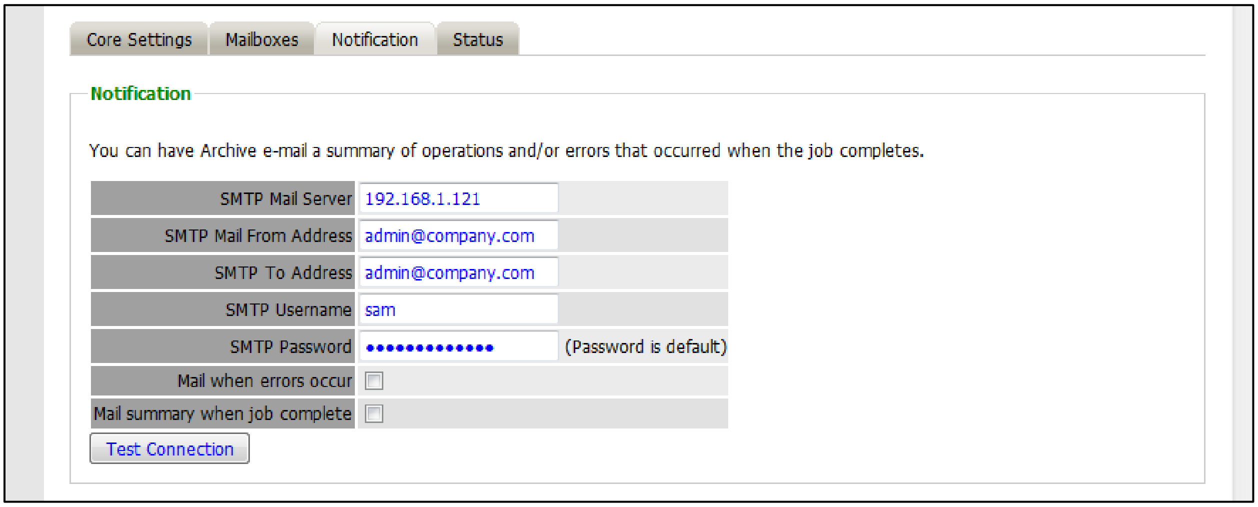
The open text box next to the selection area is a search or filtering interface which allows the administrator to only display distribution lists or mail servers that match the criteria. A blank criteria window will result in all known servers or distribution lists being displayed.

If a user is desired to be included in or excluded from a job, the selection method is identical to that of the Journaling mailbox. Search for the user via the Select Mailbox window and add it to the list.

Mail servers in Exchange may also be expanded into their respective mailbox databases, and individual, or selective mailbox databases may be selected or excluded from any specific job.

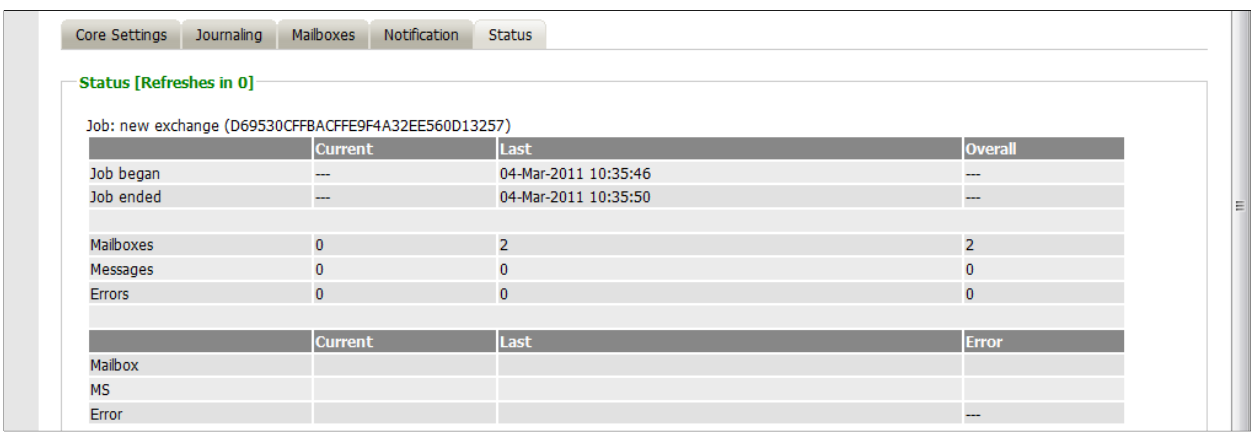
Notification

All errors, summaries, and statistics may be sent in an email notification to a desired address on job completion. If it is desired to be notified, configure the notifications under this tab. At least one of the two notification options must be selected in order for an email notification to be created.



Status

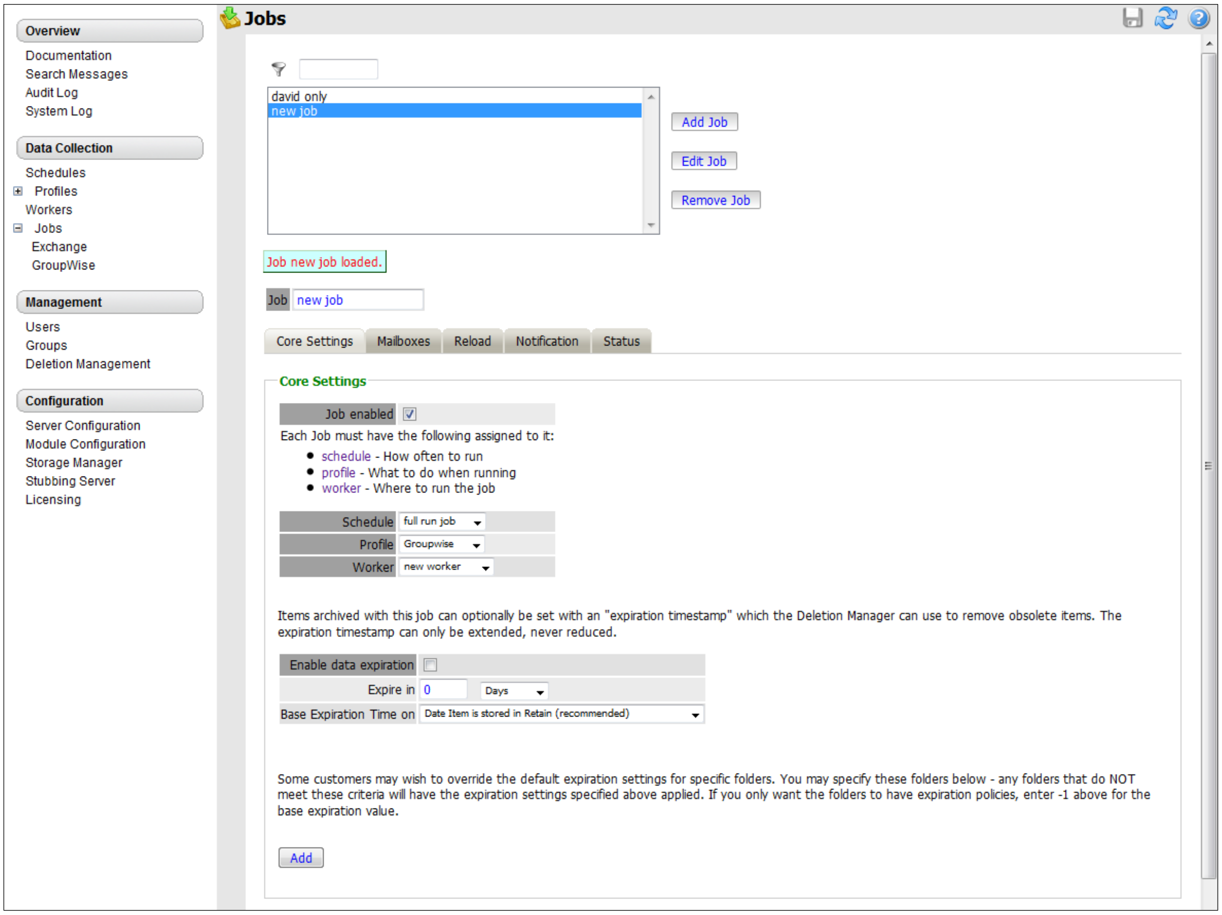
On initial creation, there will be nothing of interest shown under the 'Status' tab, as the job is under creation or has not yet run.
However, after a job has been run, or has begun, the 'Status' tab becomes a monitoring tool to report on exactly how much mail and mailboxes have been archived, along with any errors encountered.



GroupWise Jobs

All data collection for the GroupWise is configured through the GroupWise job interface. The jobs here combine the GroupWise Profile, the Schedule, and a worker together to archive a specified mailbox, distribution list, or domain. A Job must have a Profile, Schedule, Worker, and a target, mailbox, list, or domain, before it can be saved or run.

Core Settings



The Schedule, Profile, and Worker selected here will determine what is archived, when it is archived, and what worker does the actual archival work. The Job MUST be enabled in order to run. Only previously configured Schedules, Profiles, and Workers can be selected.

The **Data Expiration** is an option to place a timestamp on the mail in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date.

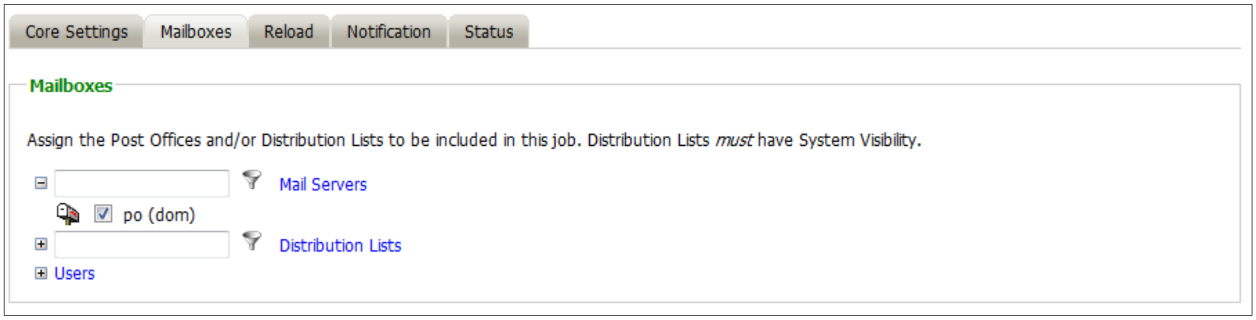
Job Expiration is not retroactive for mail in the database, and only applies to mail archived by the job that it is active for. The base folders and criteria are specified under the custom expiration dates accessed through the 'Add' button at the bottom. All messages included in these folders will have a different date, if specified, or exempted from the standard expiration date. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

Mailboxes

The mailboxes tab is where the administrator specifies which entities (mail server(s) and/or Distribution List(s)) are to be scanned.

Expand the Post Office and/or Distribution List trees, and check off the items you want to be dredged.

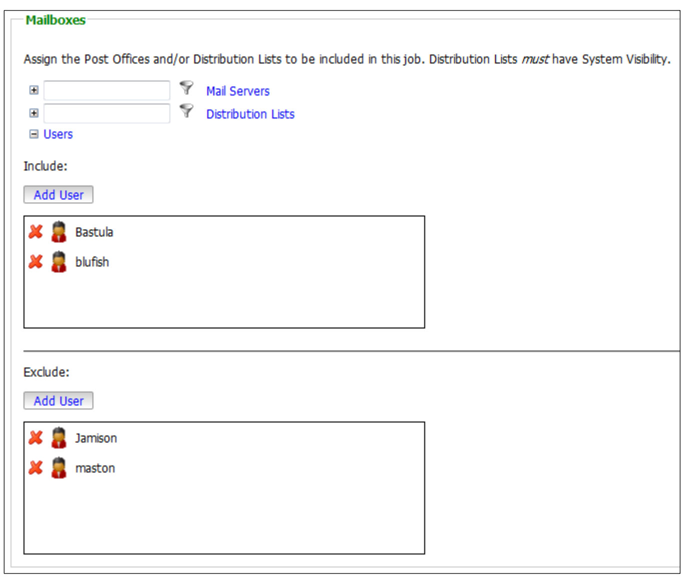
Note: If you desire to have a job backup a single user, or selected group of users, select the Users menu and assign the user(s) desired



The users section allows you to select individual users to include, or exclude them from an archive job.

For example: you can select an entire Post Office to be archived, and then expand the users section to include or exclude users to the job.

This can also be used to select only certain users in the system for an archive job.



To add a user to the Include or Exclude list, select the respective 'Add user' button and search for the user. It can be helpful to unselect the 'only show recently cached items' option.

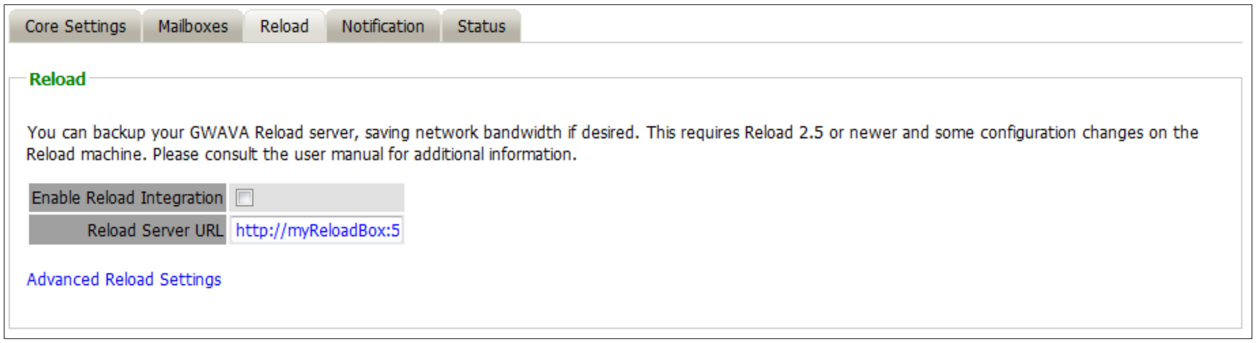
Add the selected users to the list in the search window, then select 'Ok' to add them to the include or exclude list.

NOTE: Retain cannot access certain GroupWise accounts due to GroupWise account limitations. Expired and Disabled accounts are inaccessible to Retain.
Prior to GroupWise 7.0.3, limited license accounts also cannot be accessed by Retain.

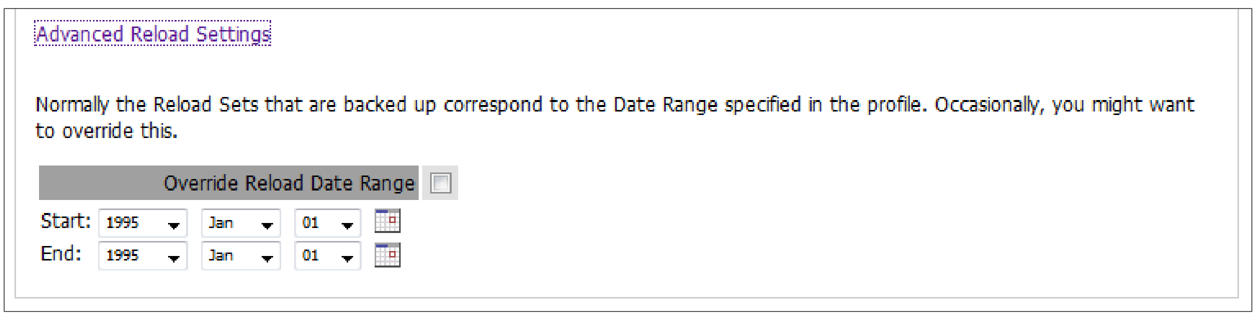
If an expired or disabled user account, (or limited license accounts under GroupWise 7.0.3), is selected for a job, or a post office containing such user accounts is selected, Retain will notify the administrator of a failure to archive those users. This is not an error, it is a limitation imposed by GroupWise. GroupWise and Retain are functioning correctly.

Reload

Selecting this option tells the job to use the Reload integration for systems utilizing Reload. See the Reload integration section for more information. The Server URL must be edited with the correct contact info for the reload server. The default Reload port is 5555.

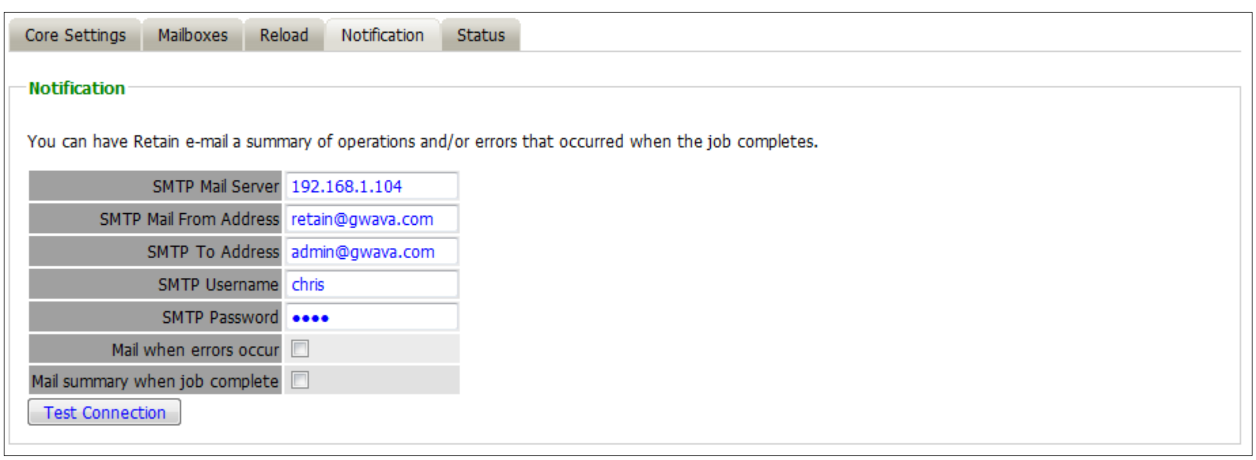


Retain instructs Reload to load the corresponding backup set for each date range in the profile. If a different set needs to be specified, the override setting specifies a date range specifically for Reload, which then will ignore the date range in the profile. Retain will still archive according to the profile date range or settings.



Notification

When a job runs, you can request an error report or job summary to be sent by e-mail.



Job Status

When a job is not running, the status tab displays information about the last time it ran:

Status [Refreshes in 1]

Job: daily (582844007495D6705B173FFE5E4EC23B)

	Current	Last	Overall
Job Began	Not running	12-Oct-2007 12:00:00	---
Job Ended	---	16-Oct-2007 12:42:04	---
Mailboxes	46	46	46
Messages	7596	238896	238896
Errors	0	0	0

	Current	Last	Error
Mailbox	steve	beta	
PO	rlpo	rlpo	
Error			---

When a job is running, you have the option of aborting the job:

Status [Refreshes in 7]

Job: first backup (27318D8551ED008C24B8EABC6CDF8A36)

	Current	Last	Overall
Job Began	19-Feb-2008 13:10:00	never	---
Job Ended	Abort Job	never	---
Completed: 12 / 13 (92%)			
Mailboxes	13	0	0
Messages	3568	0	0
Errors	0	0	0

	Current	Last	Error
Mailbox	lindy	craig	
PO	po-702	po-702	
Error			---

This window will refresh every ten seconds to keep you up to date as to the status of the selected job. Is it running, did it run and when, how long did it take, what did it accomplish?

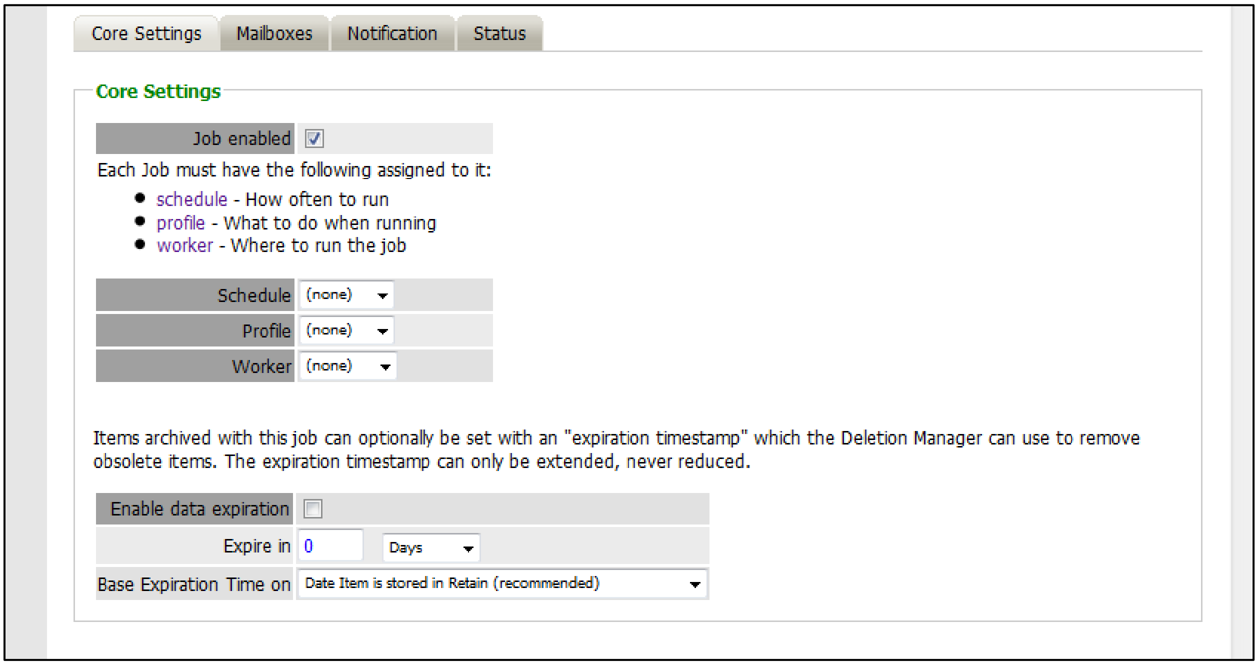
In the title, it displays a refresh countdown in seconds.

The completed line is displayed during an active job. The completed status is a display of how many mailboxes have been completed, the job mailbox total, and gives an incrementing percentage for the amount completed. This amount is based entirely on the number of mailboxes, not the amount of mail. Because the last mailbox could be larger than the rest of the system, this percentage may not be accurate according to time.

Social Messaging Jobs

All data collection for the Social Messaging module is configured through the Social Messaging job interface. The jobs here combine the Profile, the Schedule, and a Worker together to archive a specified mailbox, distribution list, or domain. A Job must have a Profile, Schedule, Worker, and a target, mailbox, list, or domain, before it can be saved or run.

Core Settings



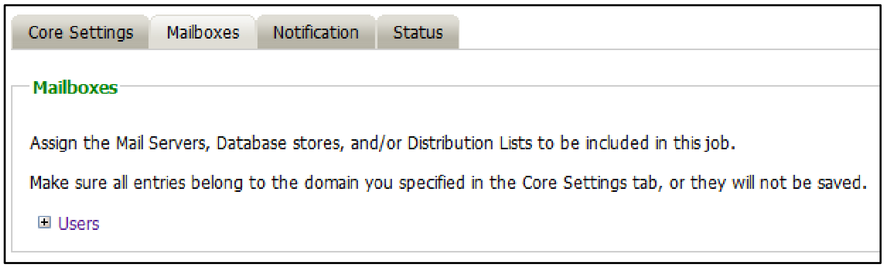
The Schedule, Profile, and Worker selected here will determine what is archived, when it is archived, and what worker does the actual archival work. The Job MUST be enabled in order to run. Only previously configured Schedules, Profiles, and Workers can be selected.

The **Job Expiration** is an option to place a timestamp on the data in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date.

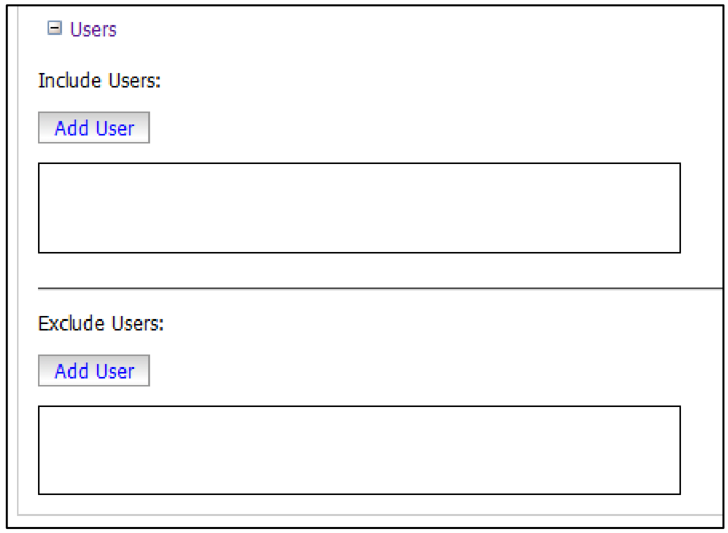
Job Expiration is not retroactive for mail in the database, and only applies to mail archived by the job that it is active for. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

Mailboxes

The mailboxes tab contains the target users, distribution lists or groups to be archived by the job. By default, all users are included.



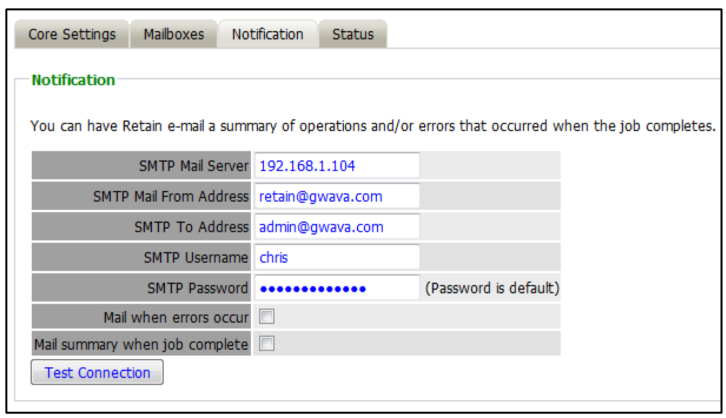
The job may be restricted to specific users, either on the 'Include Users' list. To add users, expand the User's option box and select the users to be archived. For users to be available for this dialog box, the RSM must have been configured with users. Users may be selected through the user search interface, spawned through selecting the 'add user' button.



If there are users listed, then the users listed in the 'Include Users' box are the ONLY included users, while those listed in the 'Exclude' window are excluded from the jobs.

Notification

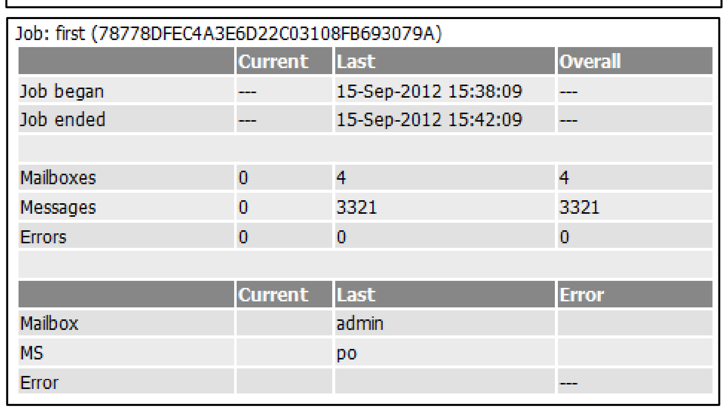
All errors, summaries, and statistics may be sent in an email notification to a desired address on job completion. If it is desired to be notified, configure the notifications under this tab. At least one of the two notification options must be selected in order for an email notification to be created.



Status

On initial creation, there will be nothing of interest shown under the 'Status' tab, as the job is under creation or has not yet run.

However, after a job has been run, or has begun, the 'Status' tab becomes a monitoring tool to report on exactly how much mail and mailboxes have been archived, along with any errors encountered.


Job: first (78778DFEC4A3E6D22C03108FB693079A)

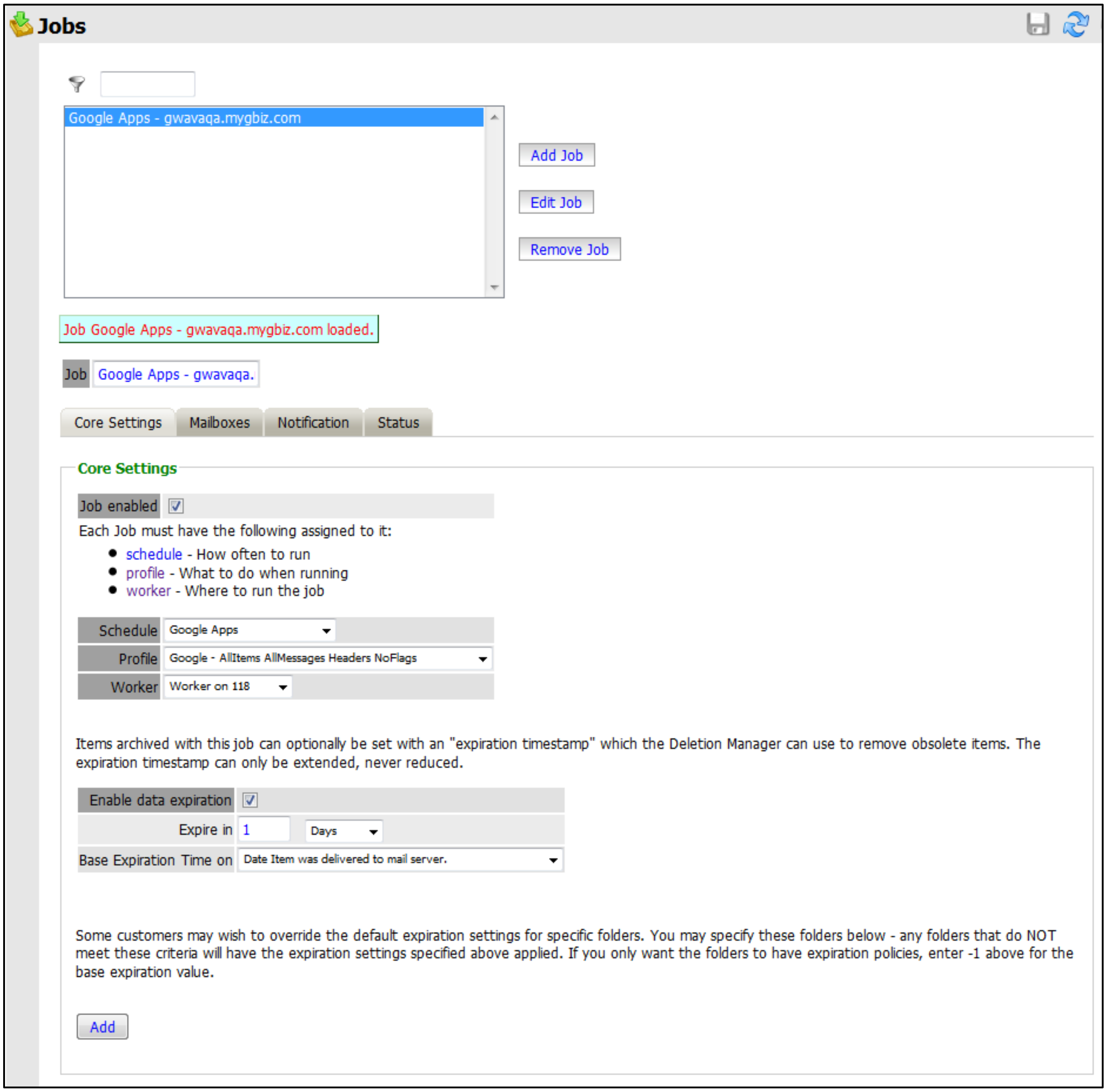
	Current	Last	Overall
Job began	---	15-Sep-2012 15:38:09	---
Job ended	---	15-Sep-2012 15:42:09	---
Mailboxes	0	4	4
Messages	0	3321	3321
Errors	0	0	0

	Current	Last	Error
Mailbox		admin	
MS		po	
Error			---

Google Apps Jobs

All data collection for Google Apps is configured through the Google Apps job interface. The jobs here combine the Profile, the Schedule, and a Worker together to archive a specified mailbox, distribution list, or domain. A Job must have a Profile, Schedule, Worker, and a target, mailbox, list, or domain, before it can be saved or run.

The Schedule, Profile, and Worker selected here will determine what is archived, when it is archived, and what worker does the actual archival work. The Job MUST be enabled in order to run. Only previously configured Schedules, Profiles, and Workers can be selected.



The **Data Expiration** is an option to place a timestamp on the mail in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date.

Job Expiration is not retroactive for mail in the database, and only applies to mail archived by the job that it is active for. The base folders and criteria are specified under the custom expiration dates accessed through the '**Add**' button at the bottom. All messages included in any specified folders will have a different date or be exempted from the standard expiration date. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

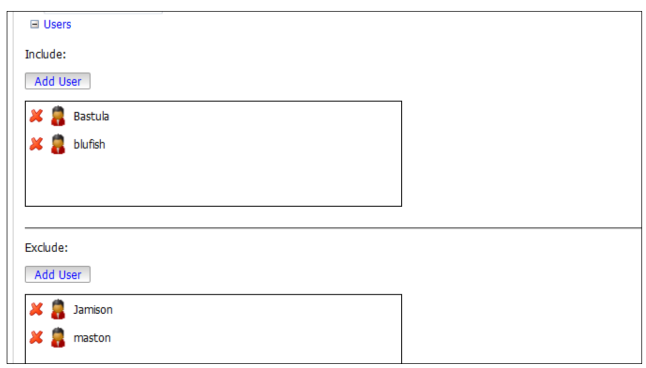
Mailboxes

The mailboxes tab is where the administrator specifies which entities (mail server(s) and/or Distribution List(s)) are to be scanned.

Expand the Post Office and/or Distribution List trees, and check off the items you want to be dredged.

Note: If you desire to have a job backup a single user, or selected group of users, select the Users menu and assign the user(s) desired

The users section allows you to select individual users to include, or exclude them from an archive job. For example: you can select an entire Mail Server to be archived, and then expand the users section to include or exclude users to the job.



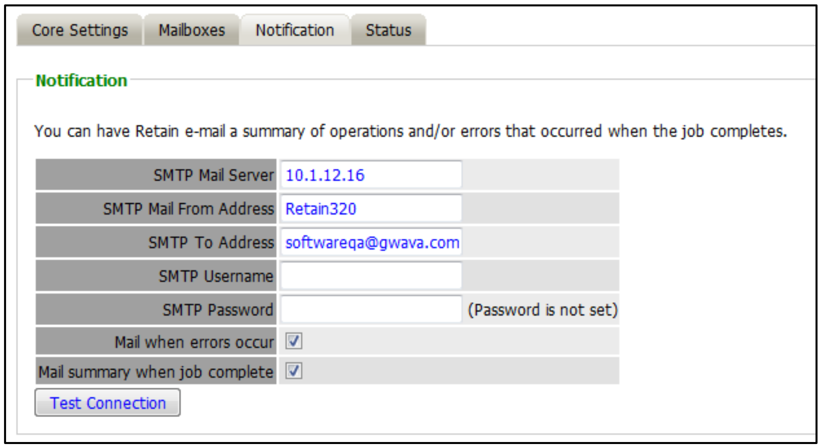
This can also be used to select only certain users in the system for an archive job.

To add a user to the Include or Exclude list, select the respective 'Add user' button and search for the user. It can be helpful to unselect the 'only show recently cached items' option.

Add the selected users to the list in the search window, then select 'Ok' to add them to the include or exclude list.

Notification

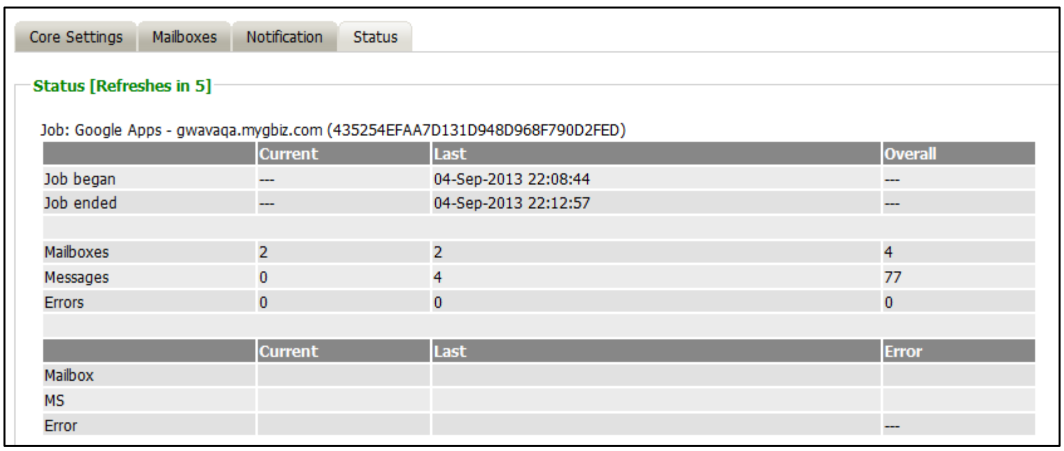
When a job is run, the notification option allows the administrator to be emailed a summary of each running job if desired.



For notification to function correctly, the SMTP information for the desired SMTP server must be fully filled-out. How much information is required varied depending on the mail system used.

Status

The Status tab displays the status of any currently running jobs, as well as the stats of the last completed job.

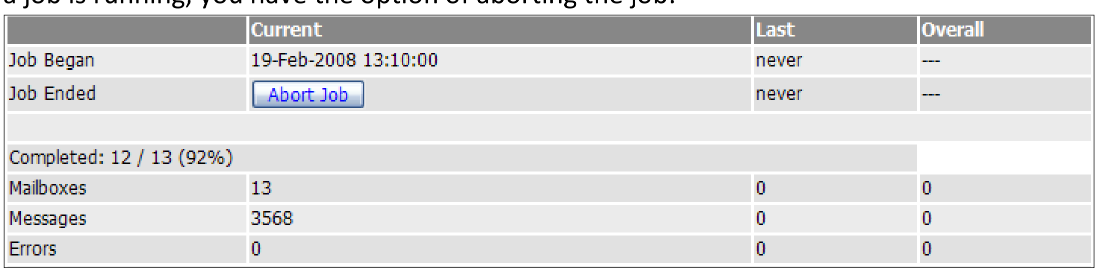


	Current	Last	Overall
Job began	---	04-Sep-2013 22:08:44	---
Job ended	---	04-Sep-2013 22:12:57	---
Mailboxes	2	2	4
Messages	0	4	77
Errors	0	0	0

	Current	Last	Error
Mailbox			
MS			
Error			---

This tab is informational only unless a job is currently running, an option to abort the currently running job is displayed.

When a job is running, you have the option of aborting the job:



	Current	Last	Overall
Job Began	19-Feb-2008 13:10:00	never	---
Job Ended	Abort Job	never	---
Completed: 12 / 13 (92%)			
Mailboxes	13	0	0
Messages	3568	0	0
Errors	0	0	0

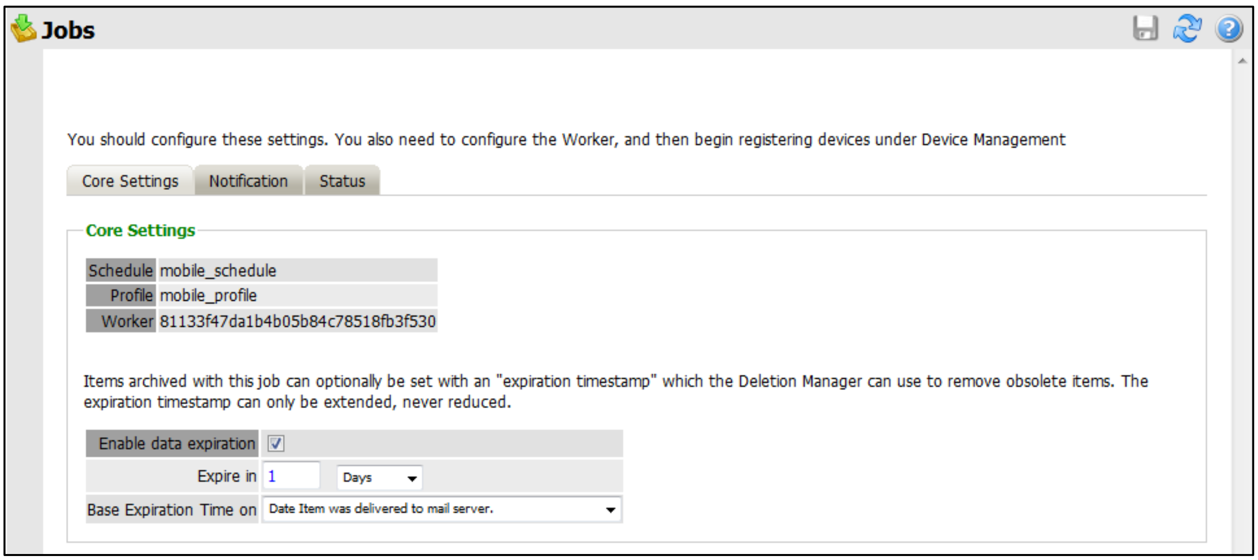
This window will refresh every ten seconds to keep you up to date as to the status of the selected job. The completed line is displayed during an active job. The completed status is a display of how many mailboxes have been completed, the job mailbox total, and gives an incrementing percentage for the amount completed. This amount is based entirely on the number of mailboxes, not the amount of mail. Because the last mailbox could be larger than the rest of the system, this percentage may not be accurate according to time.

Mobile Jobs

Usually, the Job interface combines the worker, profile, and schedule configurations into a workable format for data collection. However, due to the particular nature of archiving from Mobile devices and the setup of the Mobile module, the profile, schedule, and worker are already dictated. The Job's interface for the Mobile module contains the Data Expiration, Notification, and Status functions for message data gathering. Enabling of Mobile data archiving is achieved in configureing the Mobile module, acquiring a tenant ID, and registering mobile devices.

Core Settings

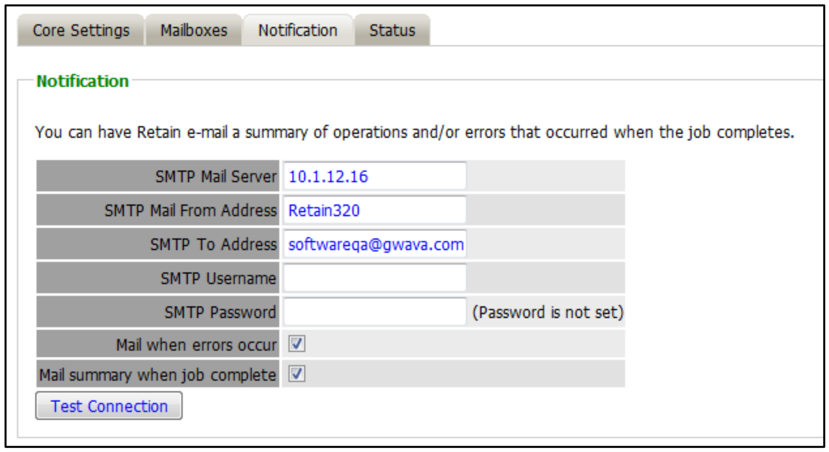
The core settings tab contains information on the schedule, profile, and worker utilized for the mobile module, as well as the data expiration date.



The **Job Expiration** is an option to place a timestamp on data in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date. Job Expiration is not retroactive for mail in the database, and only applies to mail archived by the job that it is active for. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

Notification

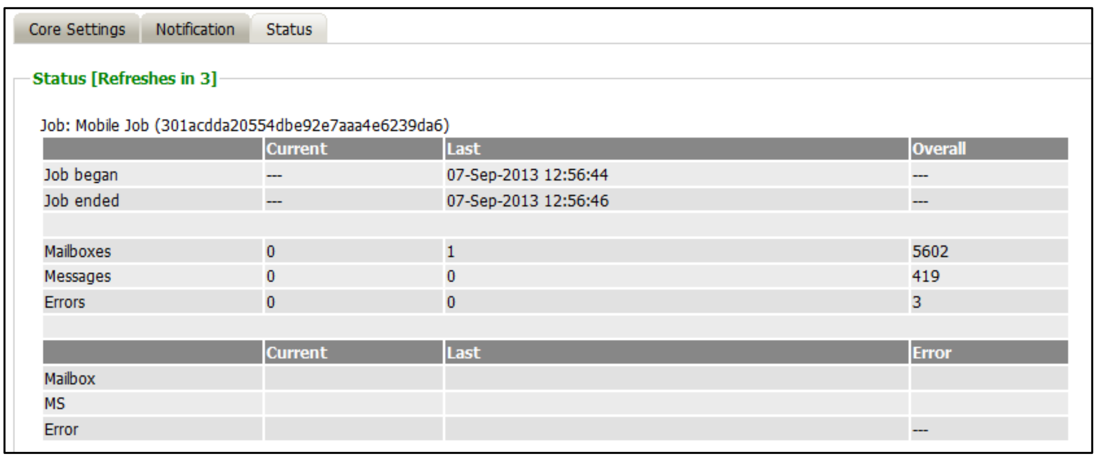
When a job is run, the notification option allows the administrator to be emailed a summary of each running job if desired.



For notification to function correctly, the SMTP information for the desired SMTP server must be fully filled-out. How much information is required varied depending on the mail system used.

Status

The Status tab displays the status of any currently running jobs, as well as the stats of the last completed job.



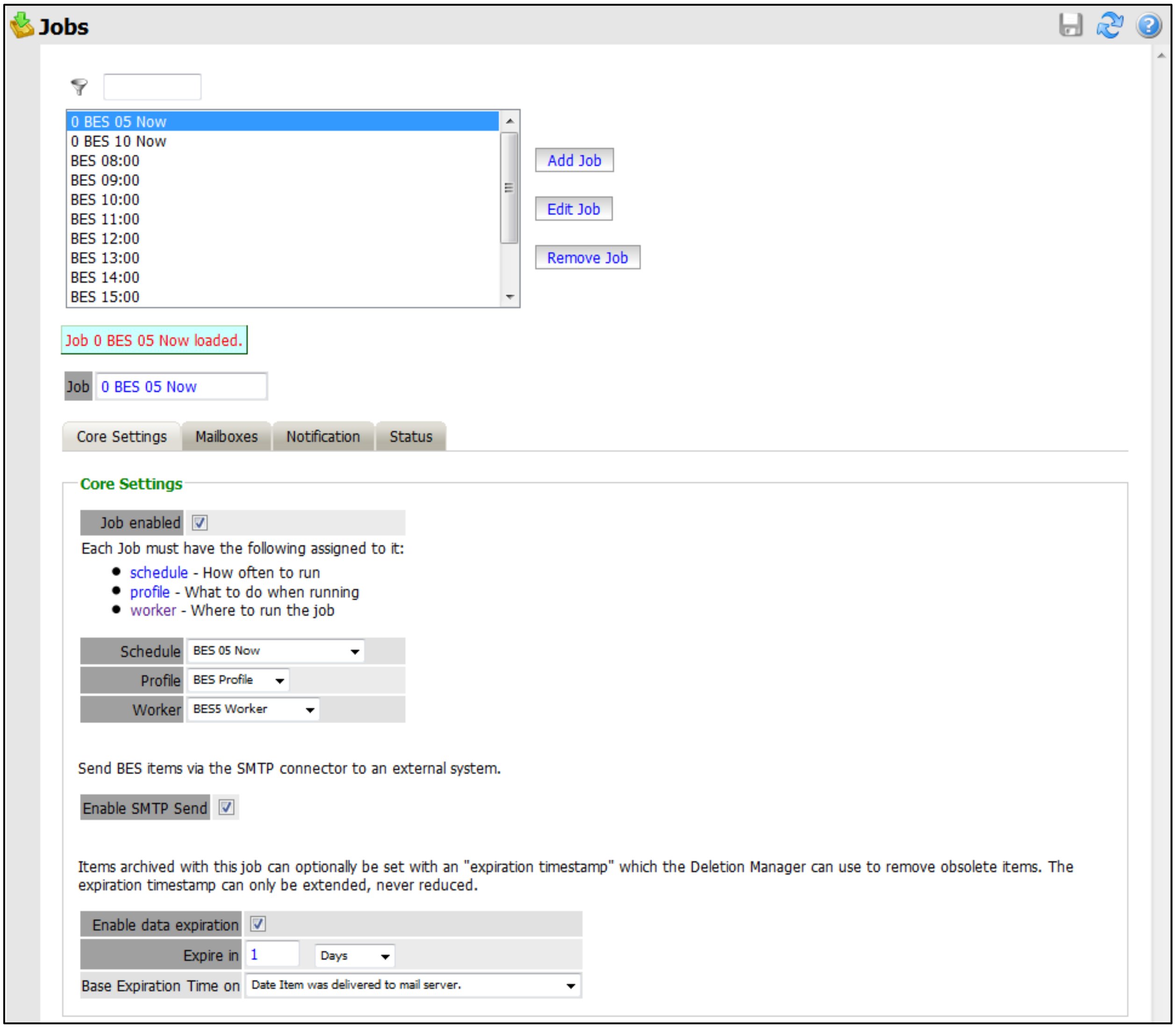
This tab is informational only for the Mobile module.

Blackberry Jobs

All data collection for the Blackberry module is configured through the Blackberry job interface. The jobs here combine the Profile, the Schedule, and a Worker together to archive the specified server logs. A Job must have a Profile, Schedule, Worker, and a selected server, before it can be saved or run. To create a new job, click, 'Add Job', and configure and save.

Core Settings

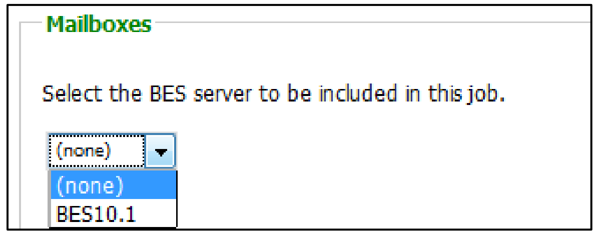
The core settings tab contains the basic configuration. Select the 'Job enabled' option to enable archiving. Also select a Schedule, Profile, and Worker to complete the job. If the SMTP Send is enabled, the worker will forward BES message data.



The **Data Expiration** is an option to place a timestamp on the data in the Retain database, which allows for ease of automation for the deletion manager. In addition, devices such as NetApp, Centera, Caringo, and Hitachi HCAP may use this number to enforce hardware level protection of the stored item so that no one (including Retain) may delete the item before its expiration date. Job Expiration is not retroactive for mail in the database, and only applies to mail archived by the job that it is active for. The base folders and criteria are specified under the custom expiration dates accessed through the '**Add**' button at the bottom. All messages included in any specified folders will have a different date or be exempted from the standard expiration date. **In order to have messages with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete messages with an Expiration Date older than 1 day.**

Mailboxes

The mailboxes tab contains the target users, and BES servers to be archived by the selected job.



Under the Mailbox tab, select the BES server to be included in the Job. The list of available BES servers is configured from the Modules page. Once selected, all users associated or present on the BES server are included.

Once a job has been run, the user list will be populated and further configuration is possible. The job may also be restricted to specific users, specified on the 'Include Users' list, or restricted to exclude users listed on the 'Exclude' list. To add users, expand the User's option box and select the users to be archived. Users may be selected through the user search interface, spawned through selecting the 'add user' button.

If there are users listed, then the users listed in the 'Include Users' box are the ONLY included users, while those listed in the 'Exclude' window are excluded from the jobs.

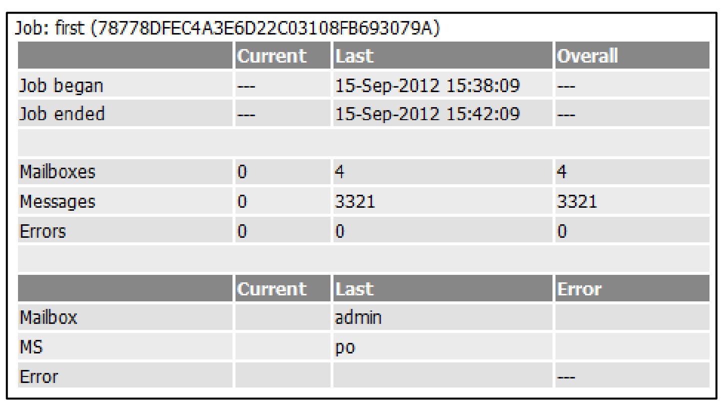
Notification

All errors, summaries, and statistics may be sent in an email notification to a desired address on job completion. If it is desired to be notified, configure the notifications under this tab. At least one of the two notification options must be selected in order for an email notification to be created.

Status

On initial creation, there will be nothing of interest shown under the 'Status' tab, as the job is under creation or has not yet run.

However, after a job has been run, or has begun, the 'Status' tab becomes a monitoring tool to report on exactly how much mail and mailboxes have been archived, along with any errors encountered.



Job: first (78778DFEC4A3E6D22C03108FB693079A)

	Current	Last	Overall
Job began	---	15-Sep-2012 15:38:09	---
Job ended	---	15-Sep-2012 15:42:09	---
Mailboxes	0	4	4
Messages	0	3321	3321
Errors	0	0	0
	Current	Last	Error
Mailbox		admin	
MS		po	
Error			---

Management

Users

User and Rights Management in Retain include:

- Creating, deleting, and editing users.
- Allowing new user accounts, and restricting specific ones from being created.
- User expiration.
- Assigning users to groups, to conveniently grant rights or set initial settings on a multiple user basis.
- Granting access to mailboxes others than the user's personal mailbox.
- Changing the specific functions the user can perform.

To access User and Groups Management, the user logging in needs the “Manage users and groups” administrative right.

Creating Users

The primary purpose of a user account is to store their preferences, rights, mailboxes to which they have access, and authentication information.

Users come from one of two places

- They may be valid message system users logging in with their credentials
  - These users use SOAP authentication for GroupWise and Active Directory authentication for Exchange.
    - Retain checks their login credentials with GroupWise or Exchange
  - These users initially belong to the group *default.* You may change this later.
  - You may restrict users (prevent them from logging in) in **Server Configuration**.
- They may be specially created in Retain independently of any message system
  - Users created in Retain do not need to have a message system account.
  - Users who don’t exist in the message system will use the *offline password*.

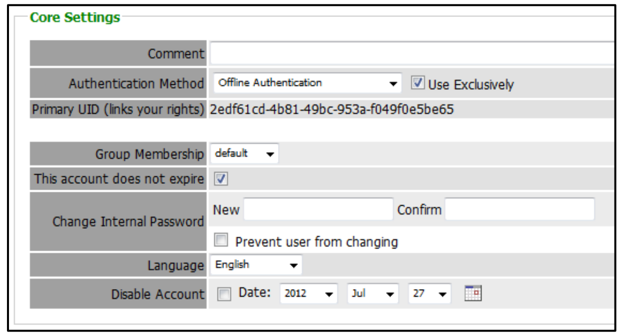
Offline Password

There are, however, occasions when you might want someone to search through the Retain archives, but who is not part of the mail system. Such a person might be an independent auditor, a lawyer, a user deleted from the live system, etc.

For this reason, Retain has an *offline password* system. These passwords are stored in Retain’s control database. Retain does not care how a user authenticates: whether offline, via SOAP for GroupWise, Exchange, or LDAP, the same rights can be assigned. An administrator who possesses the Manage Users and Groups' administrative right can assign all the rights they contain.

Users may also be assigned access to more than one mailbox. Offline users will need to be given access to at least one mailbox to perform searches. Users who are assigned “Search All Mailboxes” rights have access to all users’ mailboxes.

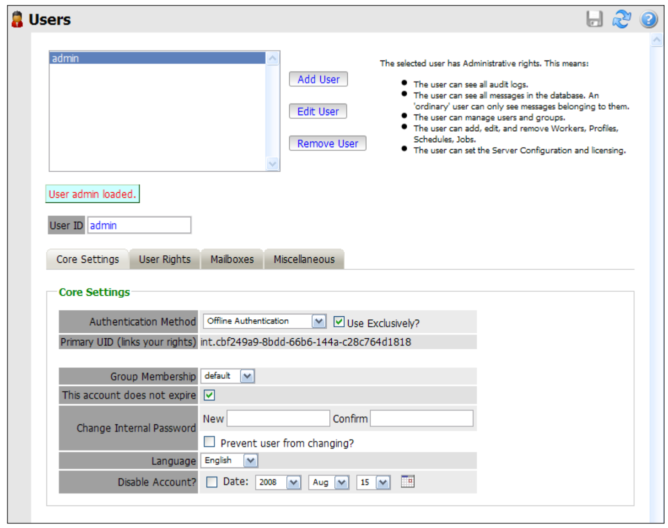
GroupWise Proxy support only works for users who authenticate via GroupWise SOAP protocol.



Creating a new user

1) Begin by clicking on the *Add User* button.
2) Enter a new user name and then fill out the options under each tab.
3) When you are done, click the **SAVE CHANGES** disk icon at the upper right.

All previously created users are listed and can be edited or removed, by clicking on the *Edit User* or *Remove User* buttons.

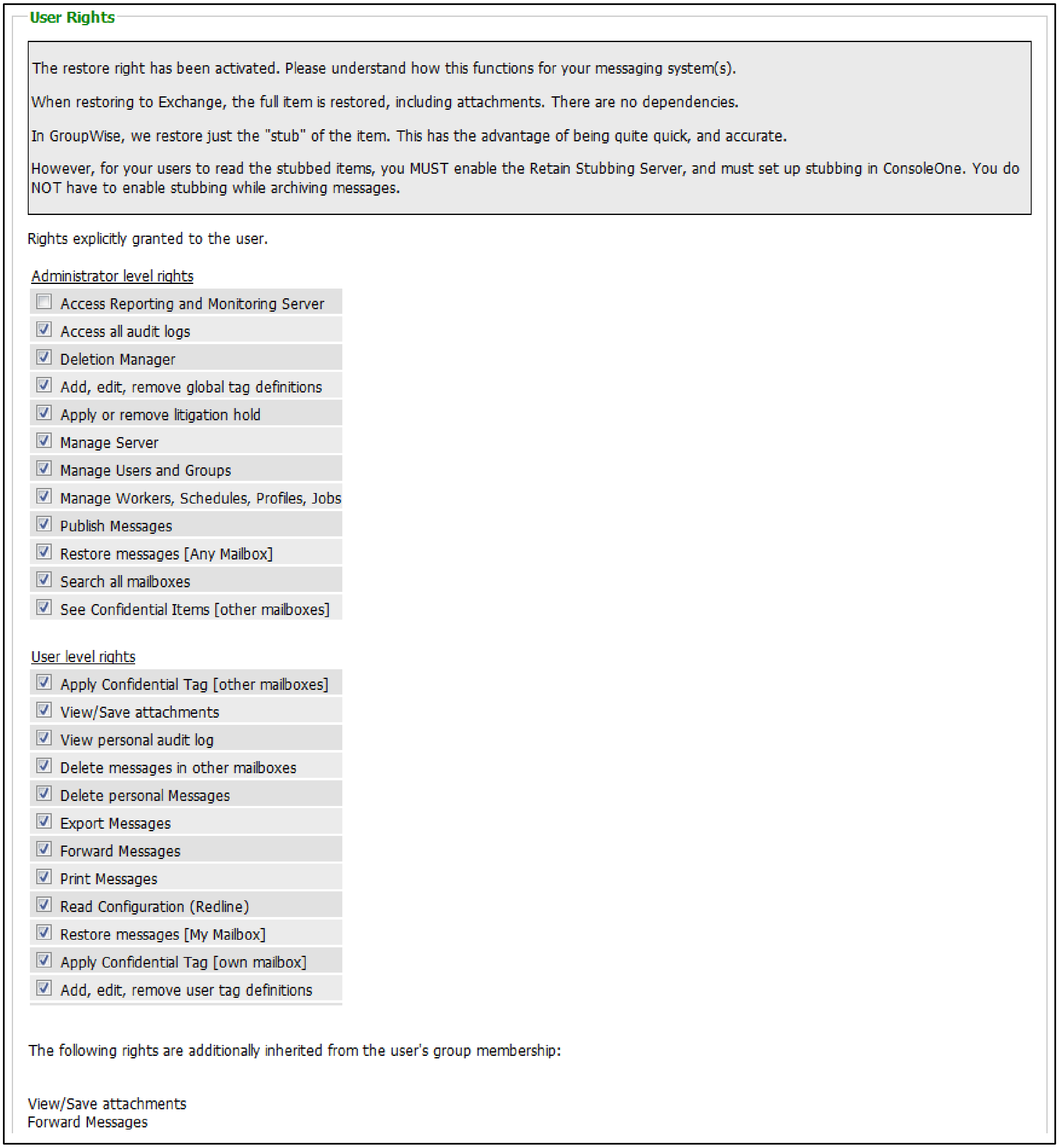


Core Settings

- Authentication method
  - SOAP (for GroupWise users)
    - GroupWise users logging in are authenticated using SOAP.
    - These users are automatically entered into Retain's user list.
  - Exchange (SOAP for Exchange). Exchange users are authenticated via SOAP for Exchange and users are added into Retain's user list.
  - Offline Password (credentials stored within Retain)(any type of user)
  - LDAP authentication – The LDAP authentication must be setup under Server Configuration, accounts tab.
  - You may lock a user account so it can only use one type of authentication.
    - If "exclusive" is not checked, it will try one, then the other.
- Primary UID
  - *Offline* only accounts usually won't have one.
  - The initial Admin account is set to use *OFFLINE* exclusively, so it never has one.
- Group Membership.
  - Default is "*default*"
  - Create groups under "Groups" and they will appear as choices here.
  - Users may belong to one and only one group. From an assigned group, additional rights, mailboxes, and initial settings may be inherited.
- Account Expiration.
  - Check this box if this user's account should not expire.
  - Useful for administrator accounts.
  - By default, accounts never expire, (0=never), but can be changed in **Server Configuration**.
- Offline Password.
  - If you use this authentication method, store the password here.
  - May be changed as needed.
  - You can prevent the user from changing it themselves.

  - Passwords are always stored in an encrypted format – <u>never in clear text</u>.
- Default Language.
  - Choose which language will be used in the Search Interface for this user.
- Disable account
  - This allows the admin to pick a date when the account will no longer be allowed to login, but the account will not be deleted.

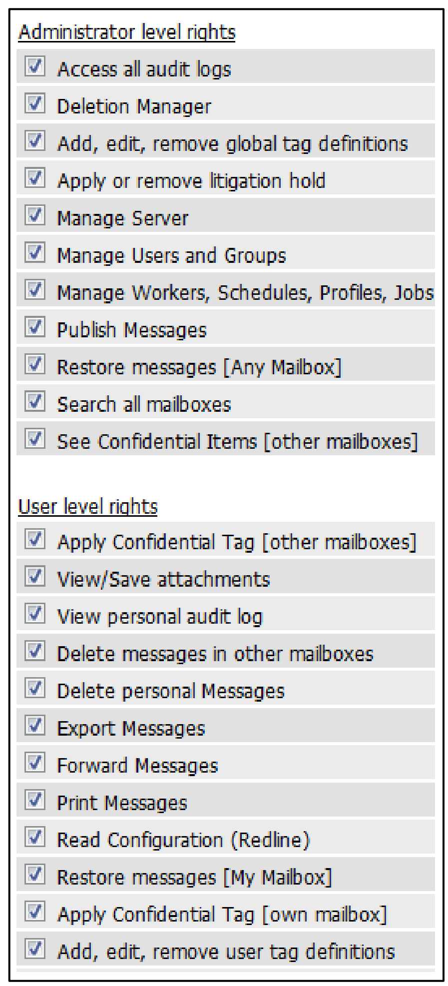
User Rights



When an administrator level right is granted a user, that user will see that right in the management console when they log into Retain. If a right that the full Administrator can view is missing from the menu of that user, they are missing that right. To view and have access to that option, they must have the missing right granted to that user. **If you have performed an upgrade and are missing options, check for a missing administrator right.**

- Control what rights you grant to the user here. Check the box to enable the right.
- These are extra rights.
  - You don't need ANY of them for the user to access their mailboxes.
  - You do need them to do “special things”. The first admin account gets them all.

- Retain first checks your assigned group and you start with the group rights.
- The rights you explicitly set here are ADDED to the group rights for the user’s effective rights.
- This way, you can control users as a group and give different rights to different groups.
- If you don’t have rights to an administrative option, it won’t appear on the left.
- It should be clear from this screen that there is no such thing as an “Administrator” per se in Retain. Instead, some users simply have more rights to do more things than others. A distinction is made between Administrator level rights (which allow a user global system wide power) and User level rights, but any user can have zero or more rights in either category. The “administrator” you created in the setup wizard was simply a user account with all of the Administrator level rights granted by default.



User Rights Summary

Administrator-level rights

- Access Audit Logs
  - The Audit Logs become visible.
    - Main menu audit log
    - Message properties audit log
  - You can see user activity on two levels
    - Globally
    - On an individual message basis
- Deletion Manager
  - Allows management of Deletion jobs.
- Add, Edit, Remove global tag definitions.
  - Allows manipulation of global tags in the view messages interface.
- Litigation hold
  - Allows excluding mail from Deletion
- Manage Server
  - Access Server Configuration and Licensing
  - Access diagnostic utilities
- Manage Users and Groups
  - Access Users and Groups
- Manage Workers, Profiles, Jobs, Schedules
  - Access data collection system.
  - Login to Worker web interface
- Allows use of Publisher
- Allows messages to be restored to all mailboxes

- Search All Mailboxes
  - Grants access to all mailboxes in the system
  - Allows the user to search and browse them.
- See Confidential Items [Other Mailboxes]
  - Allows users to view items which others have tagged as confidential.

Note: Only users with administrative rights will see the administrator's screen on login. Non-admin users are simply forwarded to the Search Interface.

User-level rights

All user level rights are strictly optional, and add additional functionality.

- **None are needed** to <u>access</u> your own mailbox and other mailboxes assigned to you.
- You may wish to grant Forwarding, View Attachment, and Printing rights.
  - The initial "default" group created upon installation does this.

Note: There is no way to perfectly block printing in a web browser, so using this feature should not be taken as a 100% guarantee that users won't be able to print. Nonetheless, for most users, it is effective.

These rights are self-explanatory:

- View/Save Attachments
- View own audit log
- Forward Messages
- Restore Messages (My mailbox only)
- Print Messages

Other rights:

- Delete messages in other mailboxes
  - Allows access to delete items from mailboxes that the user is granted access to, but is not their personal account
- Delete personal Messages
  - Allows deletion of items from the user's personal account
- Export Messages
  - Grants the right to use the export option which sends groups of messages or items as a single PDF document.
- Add, Edit, remove user tag definitions
  - This allows the user to create, remove, and edit the user's tags in the search messages interface.

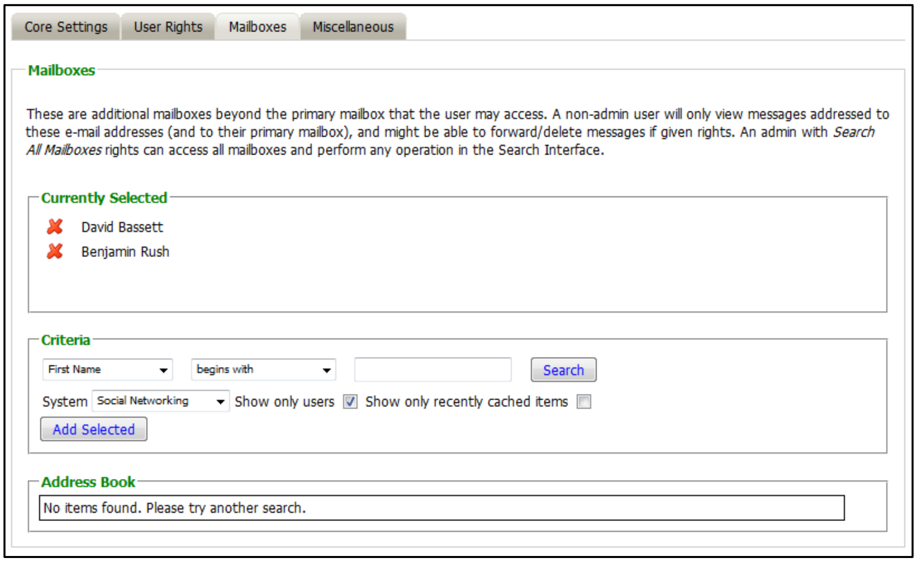
The Read Configuration right (Redline Integration)

If you are integrating with GWAVA's **Redline** monitoring product, you will need to create a user account so that Redline can log in and retrieve monitoring information. We recommend the following settings:

- Account Never Expires
- Offline Password Authentication is required. (use exclusively) (be sure to set the password)
- Read Configuration (Redline) right.

Mailboxes

Select the mailboxes this user will be able to access in addition to their own.



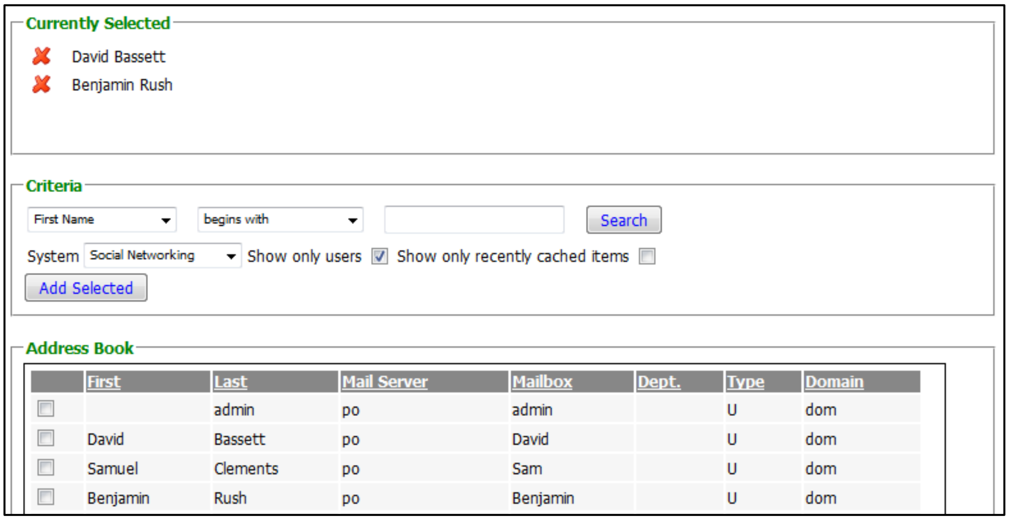
Often, you will want some users to be able to search through more than just their own mailbox. Administrators can have “Search All Mailboxes” as a right which gives them access to EVERYTHING. This section allows you to give a far more selective range of mailboxes to a user for searching.

In the example above, the user has explicit rights to two mailboxes. These mailboxes can be taken away from the user simply by clicking on the red ‘X’.

Adding users to the list is done using the Address Book selector. In the criteria section, you may enter information to search for a mailbox or a set of mailboxes. The search results will appear in the Address Book section. Each listed entry has a check box you can use to select that mailbox for addition to the list. Once you are done selecting, click **Add Selected Items** to add those mailboxes to your list of searchable mailboxes.

Address Book Selector

This interface is utilized in various other areas, but is described here.



It shows the currently selected items at the top, and lets you delete an item by clicking the red X.

(The New Mailbox selector in the Search Interface is an exception; just choose another item)

Adding Mailboxes

1) Choose between the configured module systems
2) Fill out basic criteria to narrow your search results (or no criteria for the first 100)
3) Click **Search**.
4) The results up to a maximum of 100 are displayed. The user can then page back and forth among the first 5 pages of results.
5) Choose which of the results you want to add to the selected list
6) Click **Add Selected Items**

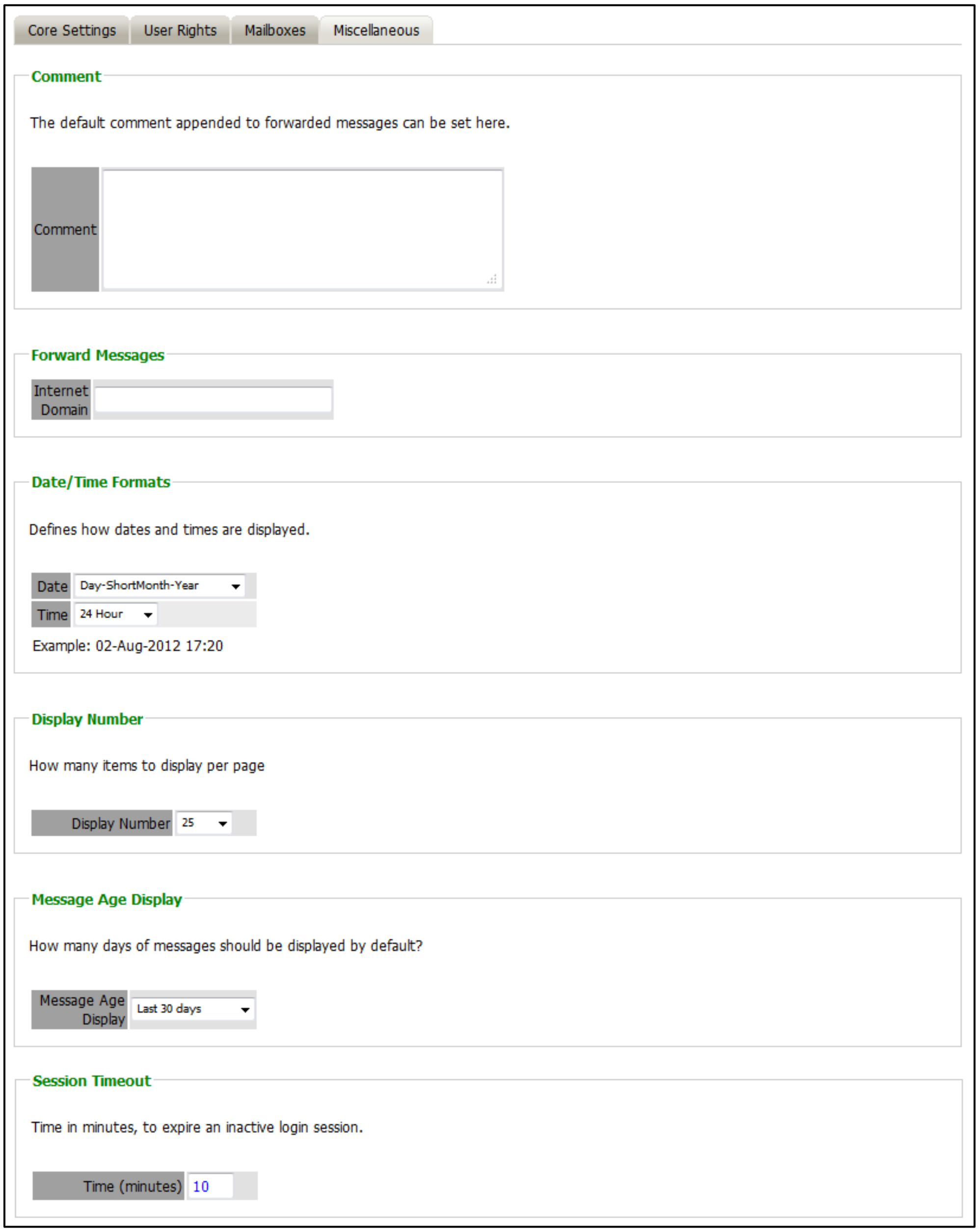
Notes: You can restrict to just Users (skipping Resources)
You can show only recently cached items (last 10 days)
The search is not case sensitive.

About “Show only recently cached items”

This option restricts the list of items shown in the selector to those with items stored within the last 10 days. In user/group management, it restricts the list to users who have logged in to the live Mail system within the last 10 days. The idea is to show only current items. If you DO want to see all items regardless of whether they’ve shown activity within the last 10 days, just uncheck this option.

Miscellaneous Tab

This tab contains settings that mainly govern the way the Search Interface works for the selected user. Note that the user can change any of these settings by using the User Options tab in the Search Interface.



- Comment — Default comment for forwarding messages.
- Date/Time Format — How you want your dates and times to be displayed.
- Display Number — How many items to display per page.
- Message Age Display — Default date filter for searching. May be changed on the fly.
- Session Timeout — Inactive session timeout. Can be between 5 and 60 minutes.

GroupWise Proxy Support

Retain supports the GroupWise proxy function. To enable it, check the box in the Module Configuration section. (NOTE: using proxy is useless if the user you wish to enable this function for is set to use offline authentication – found under the core settings of the user.)

NOTE: The 'All User Rights Access' in GroupWise is NOT supported.

This function is used to enable a user to access the mailbox of another user. For example, if user B grants the right to user A to access their mailbox in the GroupWise client, then user A can "proxy" in to user B's mailbox.

Much the same way, if user A has proxy rights into user B's mailbox in GroupWise, and the function is enabled in Retain, then user A may select user B's mailbox for browsing or may search through user B's mailbox in the Search Screen.

In Retain, it is the MAIL READ right which grants access.

Retain uses the list of available mailboxes shown in the GroupWise client to determine which mailboxes will be made available to the logged in user (user A in our example). Thus, it is important that user A has logged into user B's mailbox as proxy using the GroupWise client before doing this in Retain. While user B might have granted the rights to user A, if user A has not yet logged in as proxy to user B's mailbox with GroupWise, then user B will not appear in user A's list of available accounts to proxy into.

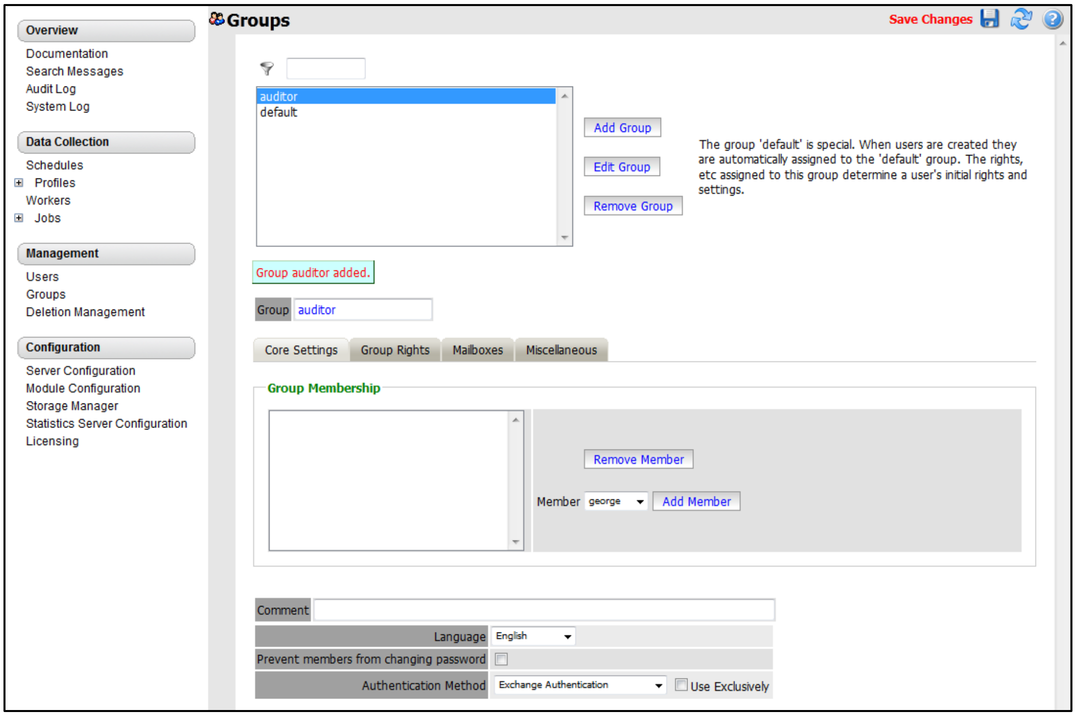
Retain checks these proxy rights the first time you access a proxy users mailbox, then caches the information for 7 days as configured in the server Configuration – Miscellaneous tab. (Default is 7 days.)

If you have access to another mailbox by virtue of GroupWise proxy, then you will see that mailbox appear in the mailbox selector in the search screen or you may search through that mailbox as well.

Groups

Once you have created users, you can group them and give them common rights. For instance, you can make a group called “Auditors” and this group will have rights to certain specific functions. If you then add users to this group, these users will get those specific rights in addition to the rights you have explicitly given them.

This is a great way to save time in managing the rights of a large number of users.



This is the main Groups administration screen. It’s laid out just like the Users screen and rights are assigned the same way, for the most part.

In the Groups screen, you will see all defined groups .The group *default* is created when you install Retain. Users are automatically assigned to this group. If you want users to be part of another group, you must first create that group and then add users to it.

You will notice the drop-down list that allows you to select a member. If it says “(no users)”, it means that all users are part of the currently selected group and that there are no more users available to add.

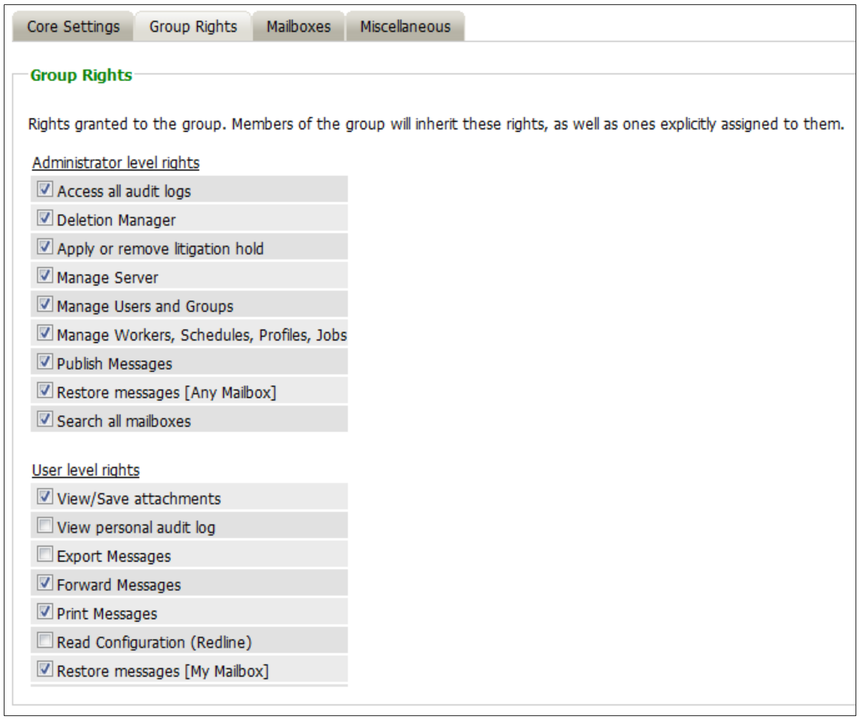
You may specify the default language used in the Search Interface for this group of users.

Creating a New Group

If you want to create a new group, simply

1) Click “Add Group”
2) Type the name in “Group”
3) Click “Save Changes”.
4) Change the properties of the group in the tabs below.

Group Rights



In this tab, you define all the rights that will be common to all members of the group. These rights are ADDITIVE and will be in ADDITION to the rights you have explicitly given to the individual user.

For this reason, if you want to manage users as a group, you would typically not assign any individual rights. Rather, you would assign rights to their group. These rights have all the same meanings and function as the users' rights.

To log into and manage or monitor Workers, a User or Group must have the manage workers, Schedules, Profiles, Jobs right. To set or work with the Deletion Manager, the user must likewise have the Deletion Manager right, or they will not be able to modify those settings.

TIPS
Typically, you will not want to grant Redline rights to a group, but in a situation where you have more than one Redline control center and you want to see which one is monitoring, group-level Redline rights would be appropriate.

Typically, you will want to make the default group's rights rather restrictive, granting very limited access by default. If you wanted a user to have more rights, you would simply assign them to another group or you could assign additional explicit rights.

By using groups, you can have groups of individuals with rights to totally different sets of archives. Users only get rights to the mailboxes you allow them.

"Redline" is a trade mark of GWAVA Inc., 100 Alexis Nihon, Suite 500, Saint Laurent, Quebec H4M 2P1

Mailboxes

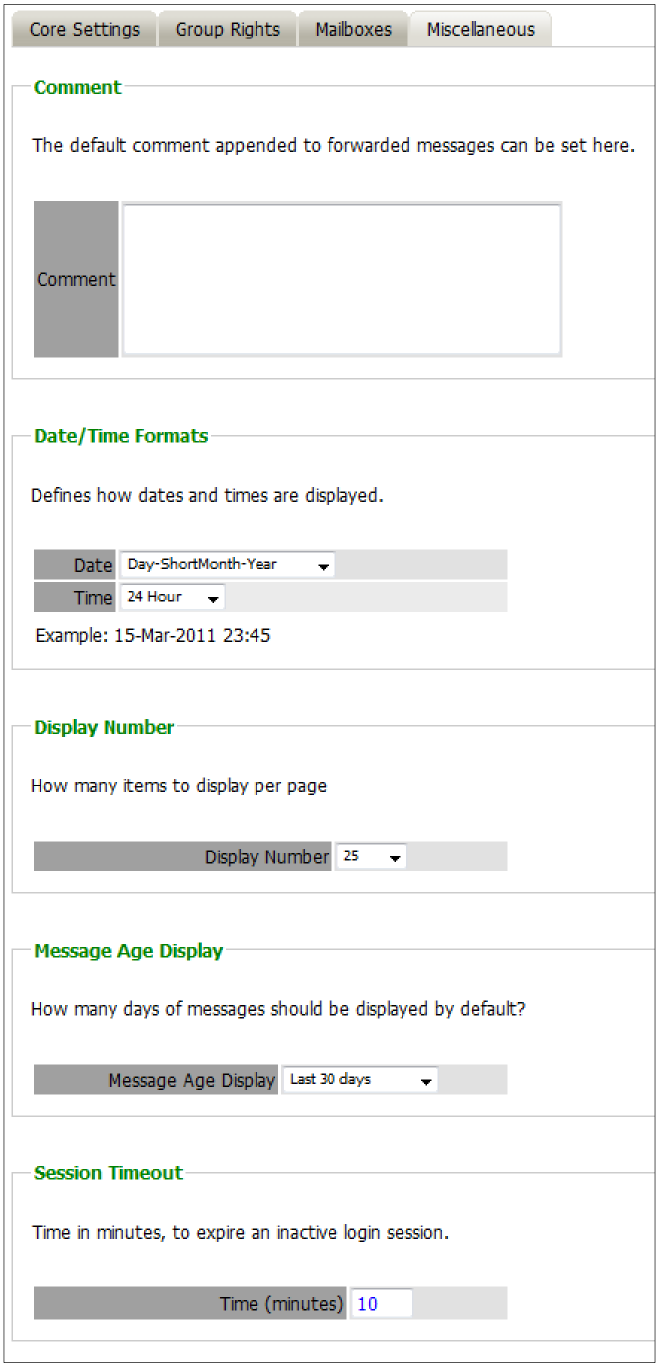
This screen works exactly like the user's access to mailboxes. Please see that section on details on how to select which mailbox or mailboxes to assign to the group.

You use the address book selector to choose which mailbox or mailboxes to give the group access to.

By default, groups have access to NO mailboxes; users may only access their own mailboxes. If the user exists only in Retain (no GroupWise account) and their group has access to no mailboxes, then they will have access to no mailbox either.

Typically, you'll give group access to mailboxes only when you want all members of the group to be able to access a particular mailbox. Some examples could include a general sales account or accounts being audited by a group of auditors, a workgroup needing to access each other's archives, and so on.

Groups – Miscellaneous



This is exactly like the users' miscellaneous configuration screen. It applies to all users in the group and users' explicit settings will override the group settings.

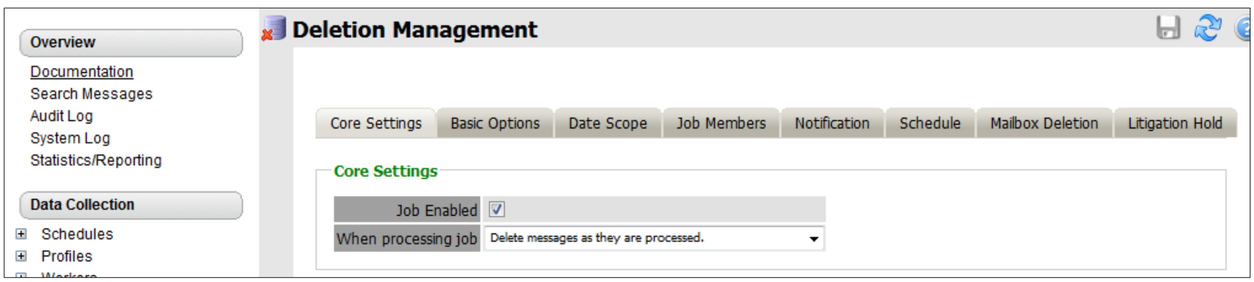
These settings govern the way the search interface works for the selected group. See more information about these settings in the users' miscellaneous section.

Deletion Management

The Deletion Manager provides for the removal of items from the archive according to the specified criteria. The Deletion Manager runs as a scheduled job in the archive, looking for, and processing or deleting items that match the search terms. Mail removed from the archive is permanently deleted. Use this option with care. The Deletion Manager will not show up in your system menu if you have not granted the logged-in user the Deletion Management right, or have the litigation hold right. See User Rights. The Litigation Hold right allows users to go to the deletion management section and add or remove the Litigation Hold right for other users. They cannot modify other settings. Users with the deletion management right can view the litigation hold tab, but they cannot grant rights; it is read only.

Core Settings

Here you enable and disable deletion jobs, and detail which actions they will take. When setting up a deletion job, you have the option to tell the job delete and report on the messages deleted, or to simply generate a report on the mail that will be removed from the database. The report function can be very handy to ensure that a job will not remove any mail that is needed, before the messages are actually deleted.

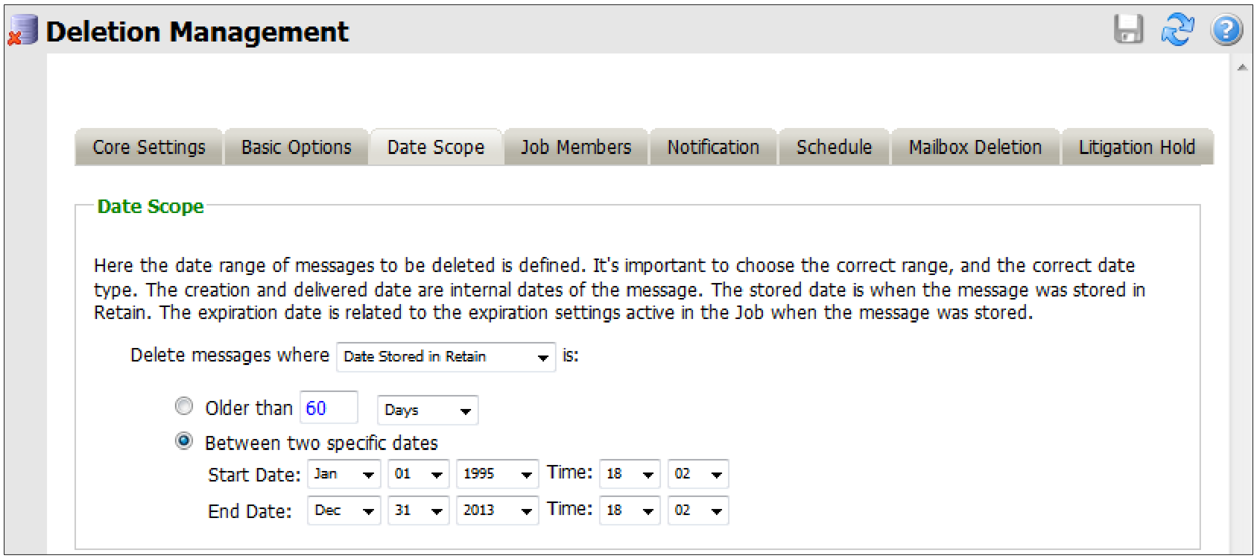


Basic Options

This tab provides the criteria that the deletion job will use to identify messages to be deleted. This should look nearly identical to the profile of an archive job. The functions are the same. The item type, source, and status determine which messages are flagged for deletion.

Date Scope

There are many dates that are contained in a mail system, and the deletion manager allows you to select different date ranges to identify the scope of the deletion manager. The setup is simple; the date range between the “Begin” and “End” dates will be targeted by the delete job.



The dates can be identified by the date filter. The Date filter allows you to specify the mail system or Retain message dates. The creation and delivered date are mail system dates. The date archived and expiration dates are set in Retain. The expiration date is tied to the job, and is set under the job section.

In order to have data with custom job or folder expiration dates properly expire, the deletion management date scope must be set to delete data with an Expiration Date older than 1 day.

The Job Expiration option allows you to set an ‘expiration date’ that the mail no longer needs to be archived after. (Different States have different laws and requirements. Usually it is between 5 and 10 years.) The Deletion Management interface can utilize this expiration date to identify messages that are due for removal.

Job Members

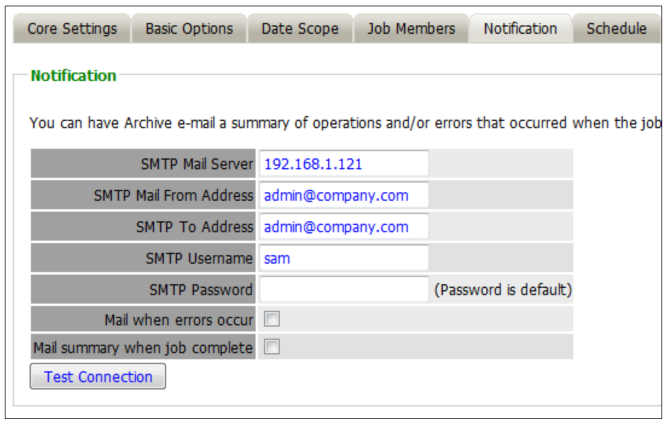
A delete job will only be active for selected users or a selected mail server. The Job Members tab allows you to include an entire mail server or group of users, while excluding specific users from the delete job.

Use this in conjunction with the Generate Report option under Core Settings to pinpoint the mail that will be included in the delete job.

Select the options as desired.

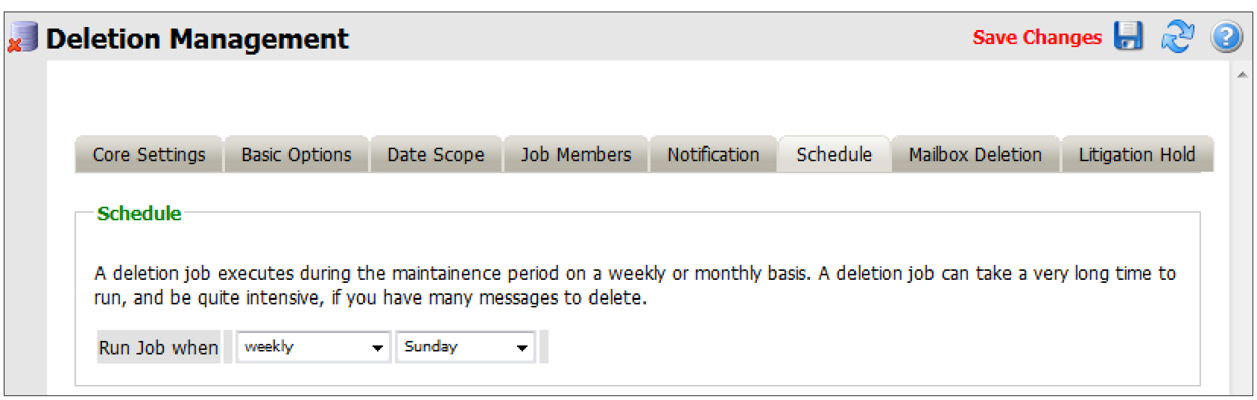
Notification

The reports, errors, and summaries of delete jobs can be sent to the listed address in the notification tab. Using the Generate Report option in Core Settings is useless unless you set this variable.



Schedule

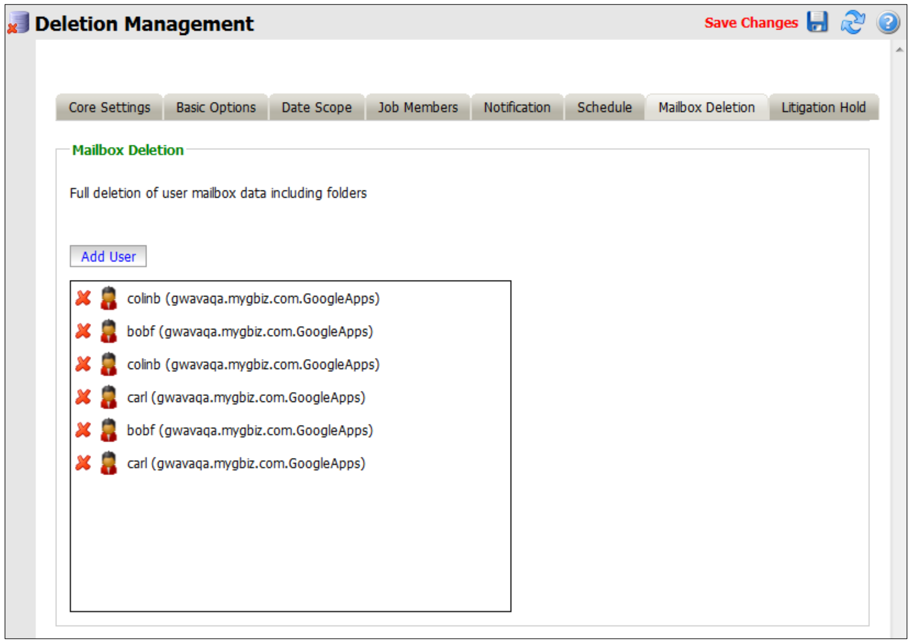
The Schedule allows you to automate and run a deletion job automatically on mail that has passed its required archive duration. The options are to run this weekly or on a specific day of the month. The Deletion job is set to run at the same time as the rest of your scheduled maintenance. (Scheduled Maintenance is found under Server Configuration – Maintenance tab. Manual starting of a job is not currently supported.)



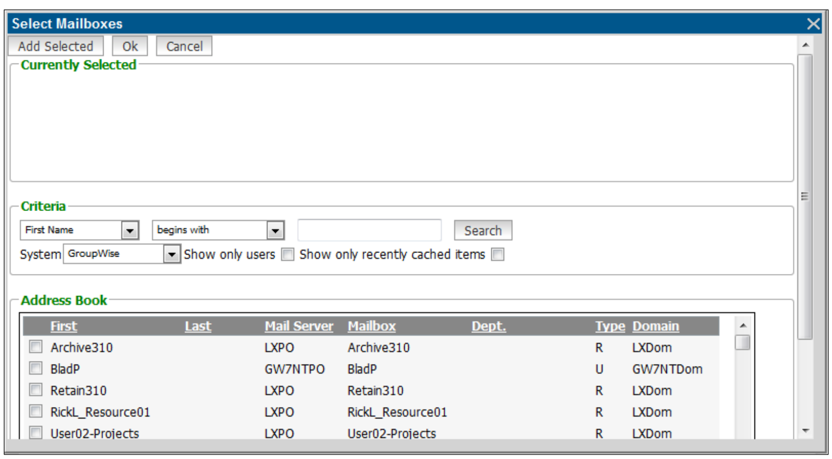
Mailbox Deletion

Deletion Management also has the ability to clean out mailboxes which no longer need to be archived. Mailbox Deletion will not remove the mailbox itself, but will remove everything in a mailbox; messages, items, and folder structures. Any mailbox which has a litigation hold applied to the whole mailbox will be skipped if placed on this list. Likewise, and any item or message with a litigation hold applied will remain with the dependent folder structure. Everything not protected by a litigation hold will be deleted from the mailbox, archive, and index.

Mailbox Deletion may be performed with a standard deletion job, but it is not something usually left with a scheduled, recurring job, because there is no need to re-delete an empty mailbox. It is recommended to use the Mailbox Deletion option on single instance jobs.



To set a mailbox for deletion, select the 'Add User' button to open the 'Select Mailboxes' dialog.



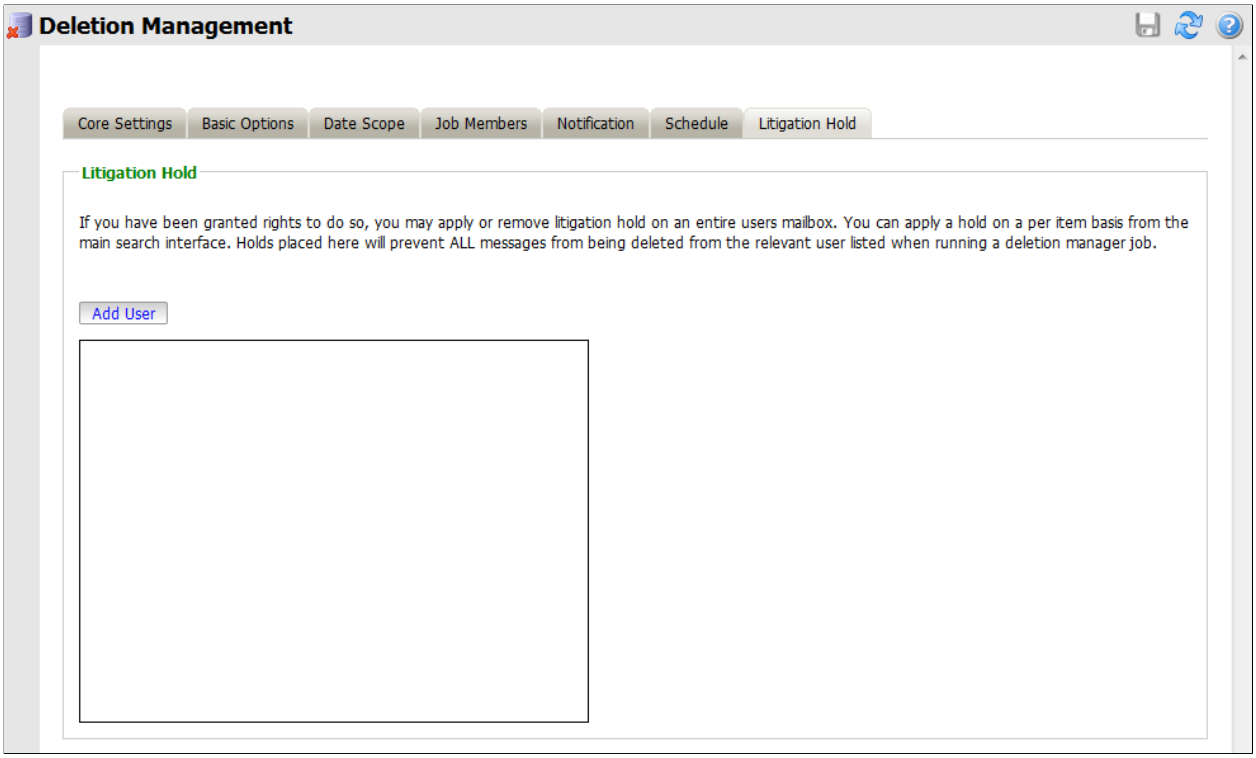
Search for and select the desired user, or users' mailboxes.

Select the 'Add Selected' button to add the selected users to the selected user list. Additional searches may be performed after selected users are added to the currently selected list. Repeat until all desired users are selected, then select 'OK' to add the user mailboxes to the deletion list.

Save the changes on the page. There is no other work to be completed. Once the deletion job executes, the mailbox is cleaned out and all items not subject to a litigation hold are deleted.

Litigation Hold

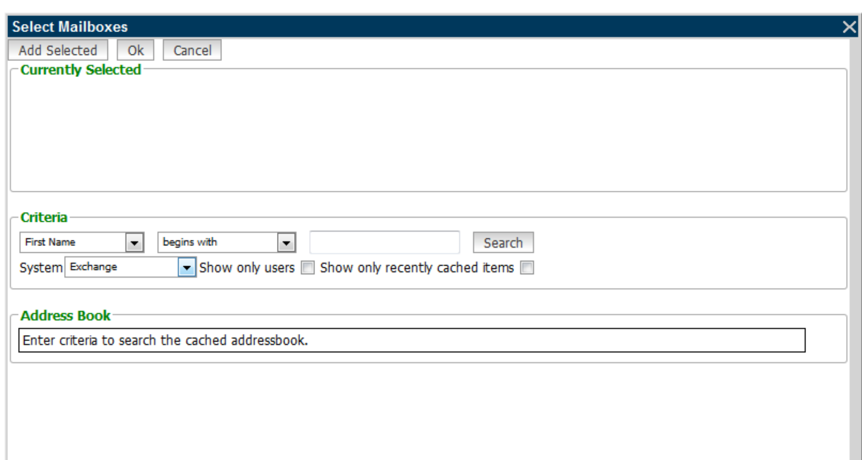
The Litigation Hold tab provides the ability to exclude any specified user's data from any deletion job, preventing any of their data from being deleted when the job runs.



Any official auditors, legal representatives, system administrators, or users may be added to this list. These accounts will be able to set and lift any legislative hold in the system, and therefore this is not a generally granted right and should be restricted to only specified users. Because of the power of this right it is granted separately from the usual rights for users.

To add a user to the legislative hold list, select the 'Add User' button to open the 'Select Mailbox' window.

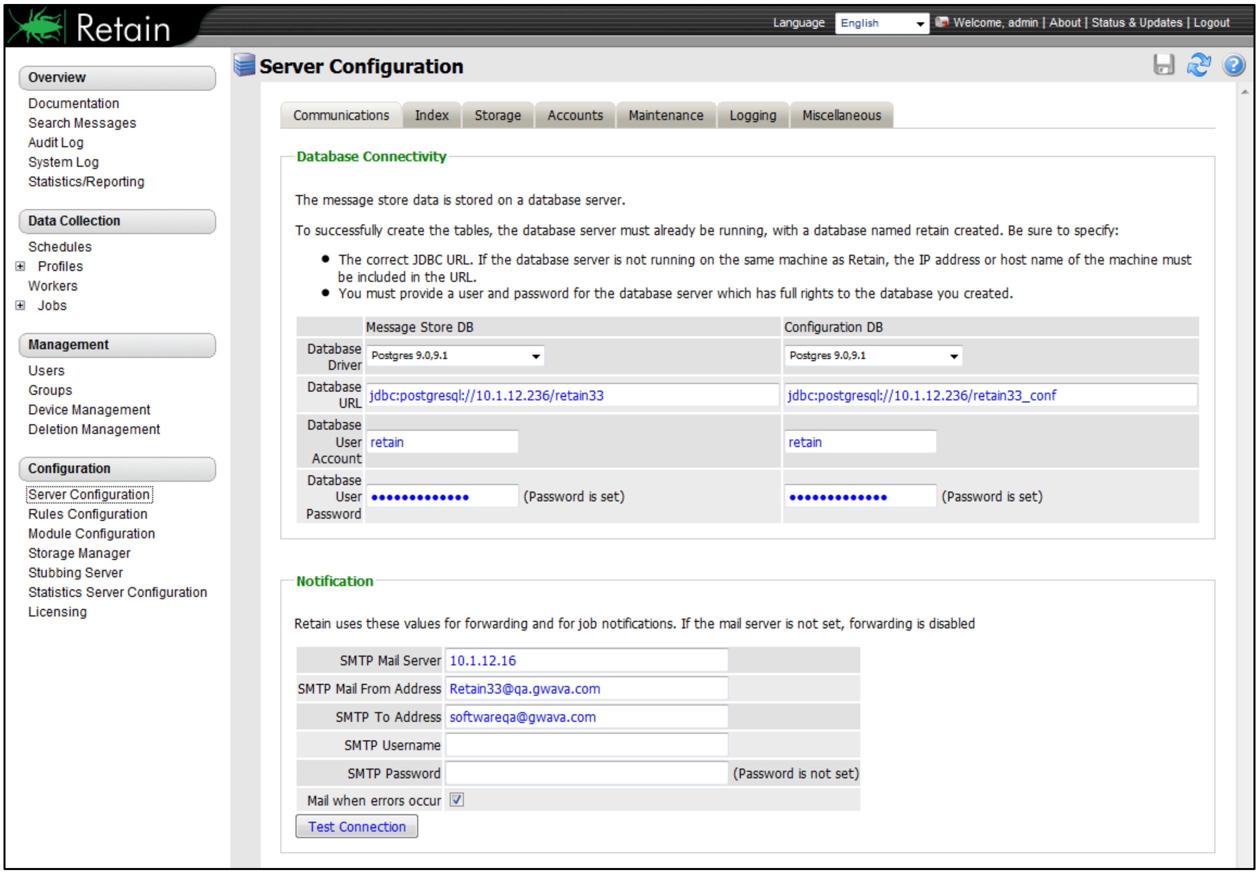
Select the source system for the user and enter search criteria. After searching, select the desired user or users and select the 'Ok' button to add them to the list. Save all changes.



Configuration

Server Configuration

The overall operation of Retain is configured in this section.



Each tab will be explained below.

Along the top, you will see configuration options for the Retain server and workers known to this server.

The most important topic is communications. These are the settings you have set when you initially installed Retain. You may make changes here.

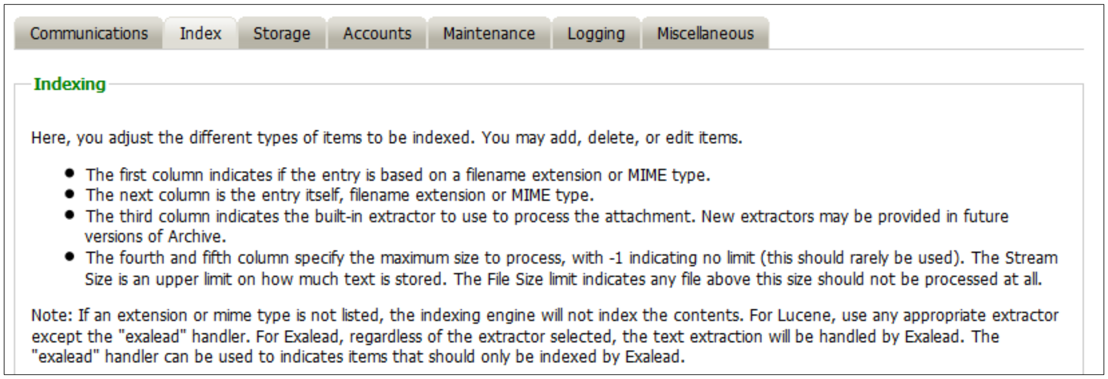
After changing any communications options, it is strongly recommended that Tomcat be restarted immediately.

Communications

The settings for the Communications tab are set in the initial setup of Retain. These include the connection to the SQL Database server, the Retain database, and the notification, SMTP information. If any changes in the system or corrections are needed, they should be configured here.

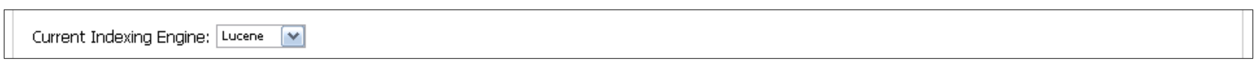
Index

The Index tab allows the management of the indexing engine as well as the ability to decide what kinds of attachments are indexed, and what size.



Because Exalead is a much more robust indexing engine it requires its own server and resources. As such, when Exalead is selected as the indexing engine, a connection address and starting base port are required. The default BASEPORT is 10000. To ensure that the connection to the Exalead server is working, the 'Test Connection' button may be selected, which triggers Retain to contact the Exalead server. The results should shortly appear as a small notification window in your browser.

Lucene is hosted locally on the same machine as the Retain Server, and requires no further configuration, but does not have the same options or the extent of the capabilities as the Exalead engine does.

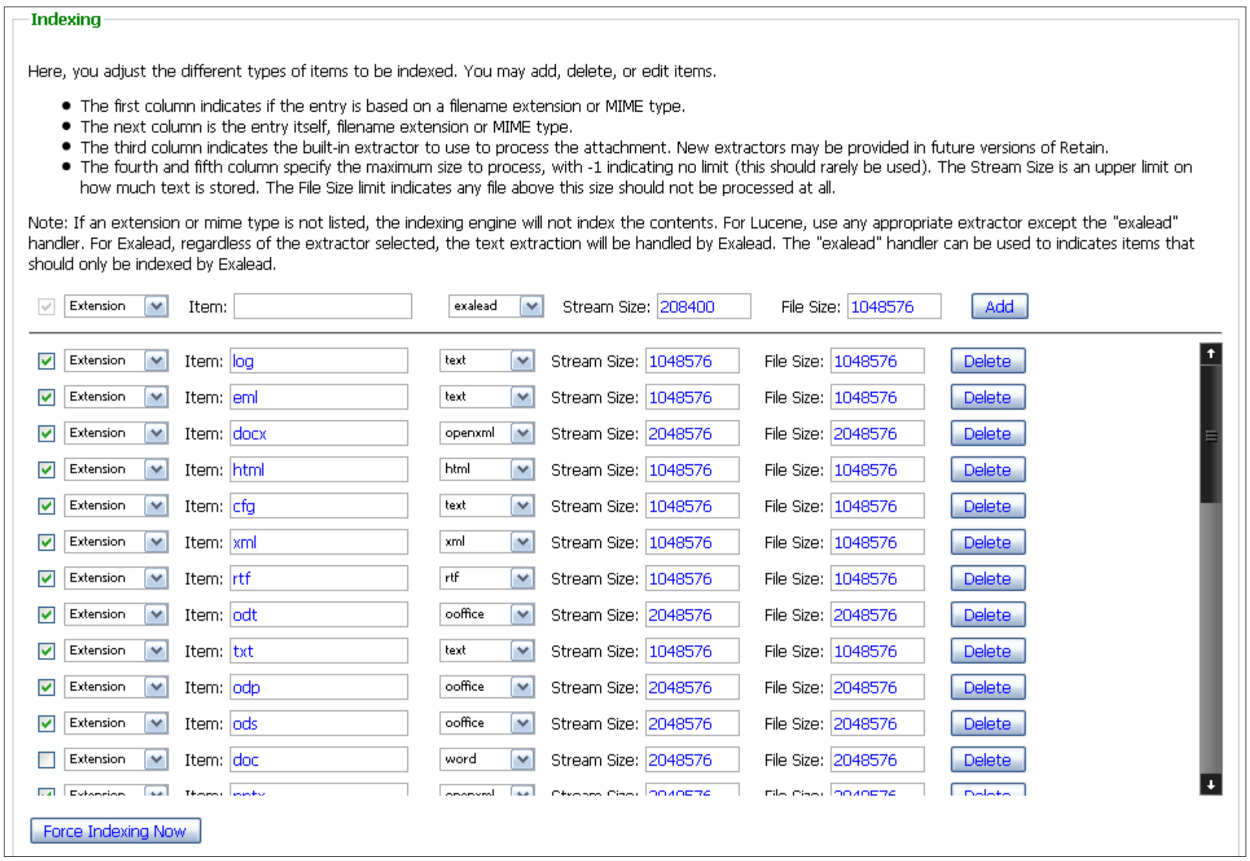


The indexing engine can be changed between the two engines, but requires the index to be re-created. Recreating the indexes is a time consuming process and should not be done unless required. Searches of the Retain Archive during the index re-creation or migration process may not contain all results.

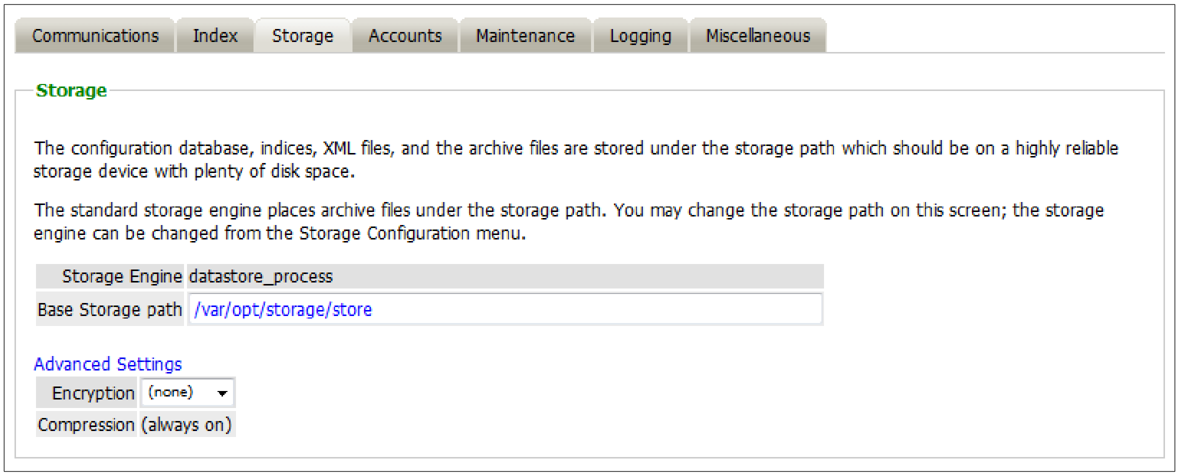
For details on how to change from one index to another, see the appendix section on switching the index engine.

You can control what Retain indexes here. You may add as many items as you wish to the list of attachment types to index. **Note the explanation at the top of the table.** The items are listed (in order) by type, extension, archived form (extractor used), and maximum stream size and file size. You choose whether to index the attachment based on its filename extension or its MIME type (the content itself). You also choose which extractor to use to index the attachment. Retain supports HTML, RTF, TEXT, XML, OpenXML – (MS Office 2007 .docx), OpenOffice2, Word Perfect documents, Excel files, .DOC, and .PDF under the Lucene indexing engine, while Retain supports many more under Exalead. (Because of high CPU, memory, and performance requirements, MS Word and Adobe PDF are not indexed by default and must be enabled to be indexed. If you need to index these items, the allotted memory should be increased. Indexing these items will slow down the indexing process.) Select as many as you need. If an attachment type common in the system which needs to be indexed, but which does not already exist in the system, it may be added by using the 'add' row.

Force Indexing tells the server to index items that are not currently indexed. This queries the system for the top 500,000 items that are not currently indexed, and starts the indexer working if it is not currently working.



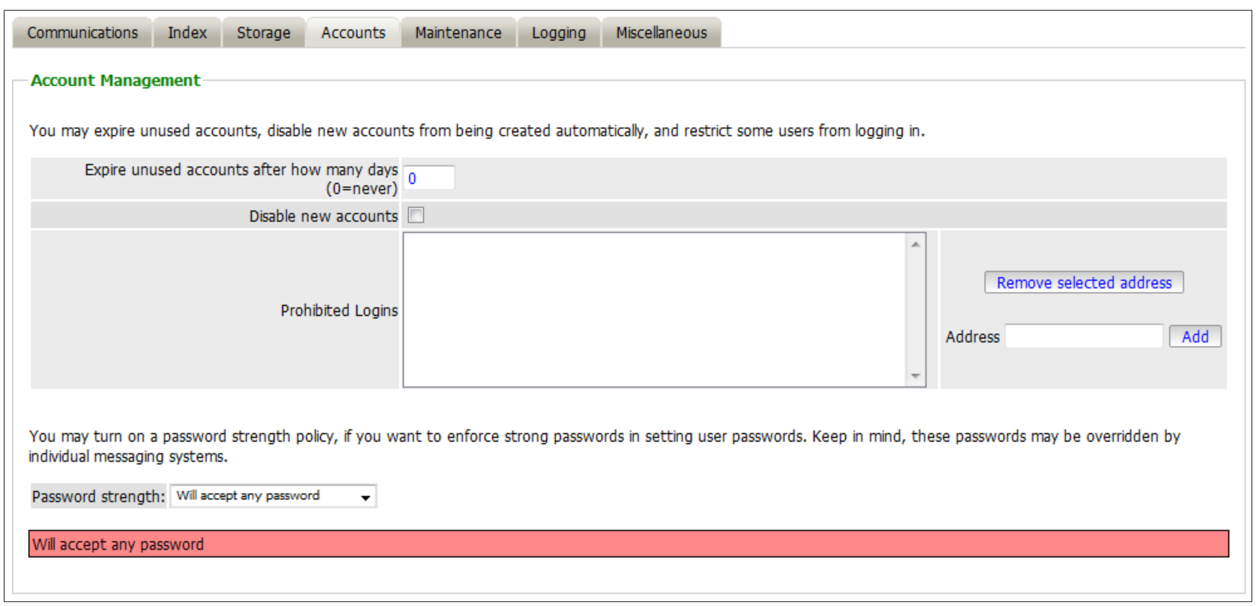
Storage



The default storage path for your Retain archives is listed here. (See About Storage Paths and Storage manager sections.)

Retain uses a **hybrid storage system**. All message headers and metadata is stored in the database but all message text and attachments are stored as files on the file system in the location listed here (and subdirectories). This is done a little like GroupWise, where the OFFILES directory stores Binary Large Objects (anything larger than 2KB). In the case of Retain, this is transparent to the user and you may choose whether to encrypt this data. If it is stored in a location accessible ONLY to the Retain Server, then encryption is not strictly necessary.

Accounts



Open System vs. Closed System

Normally, Retain lets all mail system users log in. This is considered to be an "open" system. When that happens, Retain will check to see if a Retain account already exists and if not, it will create a new account for them and assign them to the group *default.*

Sometimes, you don't want certain users to have access to the Retain archives. In this case, you may add these users to the list of **Prohibited Logins**. You do so by entering their name in the Address field and click "Add".

To make a "closed" Retain system, simply click on "Disable New Accounts". If you use this option, it means that you will have to manually create accounts in Retain for authorized users. In other words, the only people who can access your system will be people who you specifically create an account for.

In Retain, user accounts expire after 30 days of inactivity by default. You may choose the number of days or choose 0 for "accounts never expire".
See "User Rights" for more information.

Password Strength

User-created passwords may be controlled for strength. By default, Retain accepts any password set by users. To require a higher security password, select the higher level desired. Requirements for the low, medium, and high settings are defined as:

Low

Must be between 5 and 15 characters in length, with at least 0 lower case characters, at least 0 upper case characters, at least 0 numerical characters, and at least 0 special characters.

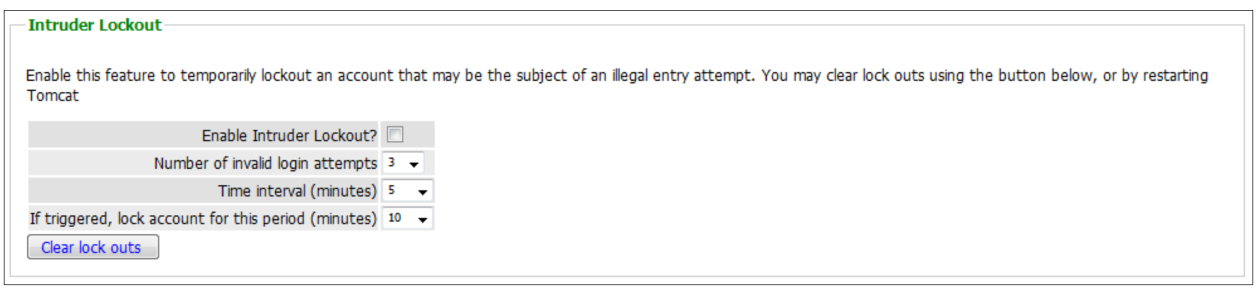
Medium

Must be between 5 and 20 characters in length, with at least 1 lower case characters, at least 1 upper case characters, at least 1 numerical characters, and at least 0 special characters.

High

Must be between 8 and 20 characters in length, with at least 2 lower case characters, at least 2 upper case characters, at least 2 numerical characters, and at least 2 special characters. . In addition the password will be checked against a dictionary.

Intruder Lockout



Accounts may be locked if multiple failed attempts are detected, according to the specified time window. This is useful to deny password cracking attempts on the server.

To enable Intruder Lockout, select the checkbox next to the 'Enable Intruder Lockout' option and save the changes. All changes will be immediate as soon as the save button is selected.

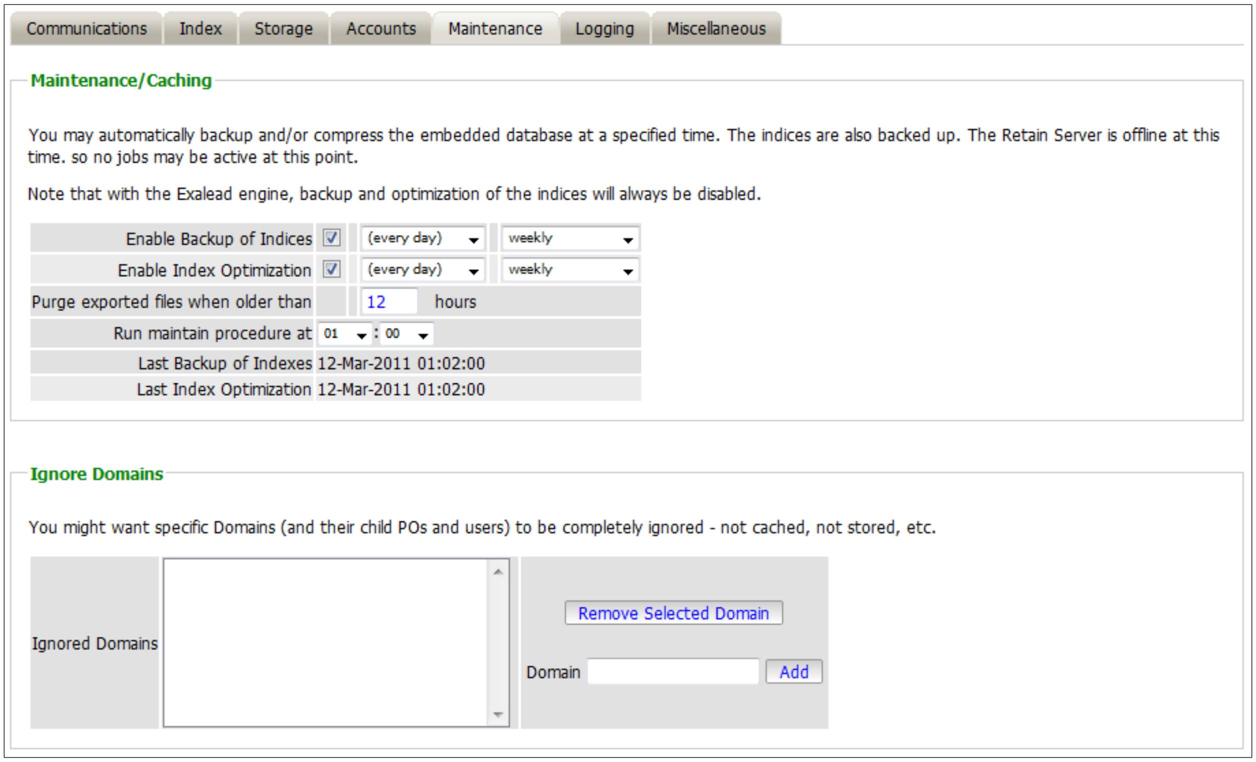
If a user has locked their account and requires immediate access to the system, all lockouts may be cleared. To clear any locked accounts, select the 'clear lock outs' button at the bottom of the page. There is no need to save changes; the clear command is immediate.

Maintenance

Maintaining a Retain system involves many tasks:

- Backup Configuration (Embedded) Database
- Compress Configuration Database
- indexing (All Indexes)

These items are all controlled here.



This configuration database – the "Embedded" database:

- should be backed up regularly
- contains your system address book
- also contains key information used by Retain

Configure how often it gets backed up here.

You can also configure how often indexes get backed up and how often the indexes are optimized for speed.

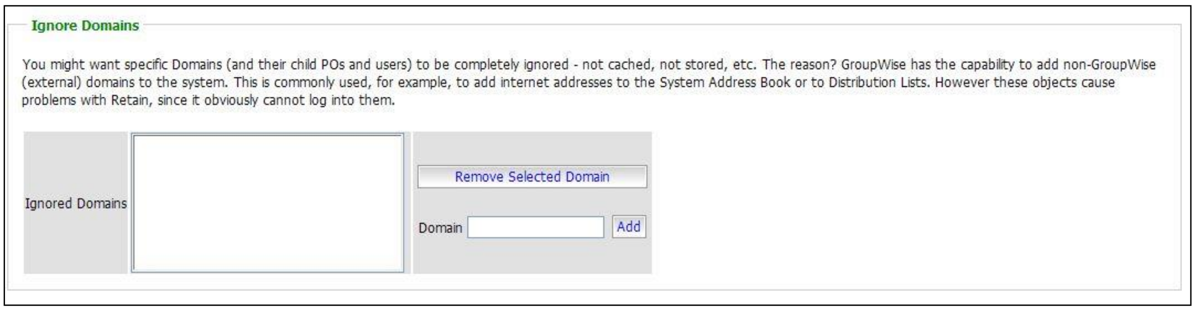
Retain also lists a history of backups and maintenance here.

Note: This maintenance section does NOT involve backup or maintenance of the data store. You must back that up yourself with your normal backup tools.

You must backup:

- SQL Database
- File System where your data is stored. (see index/storage for location)

Ignore Domains

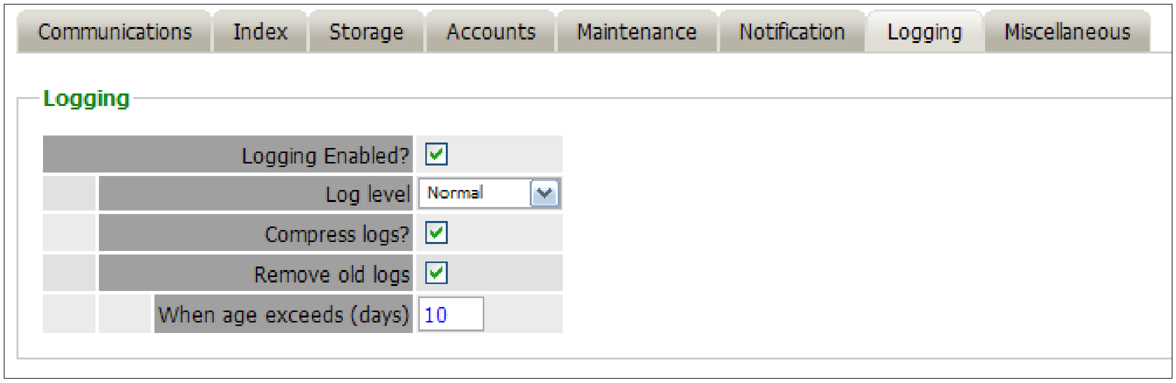


Some mail systems allow for the addition of non-system, or external domains. Sometimes, you might do this to add external domains to the mail system address book. However, the mail system cannot pull up e-mail from these domains and you may want to tell Retain to ignore references to these external domains to avoid wasting time during data collection.

Specify these domains in this window.

Logging

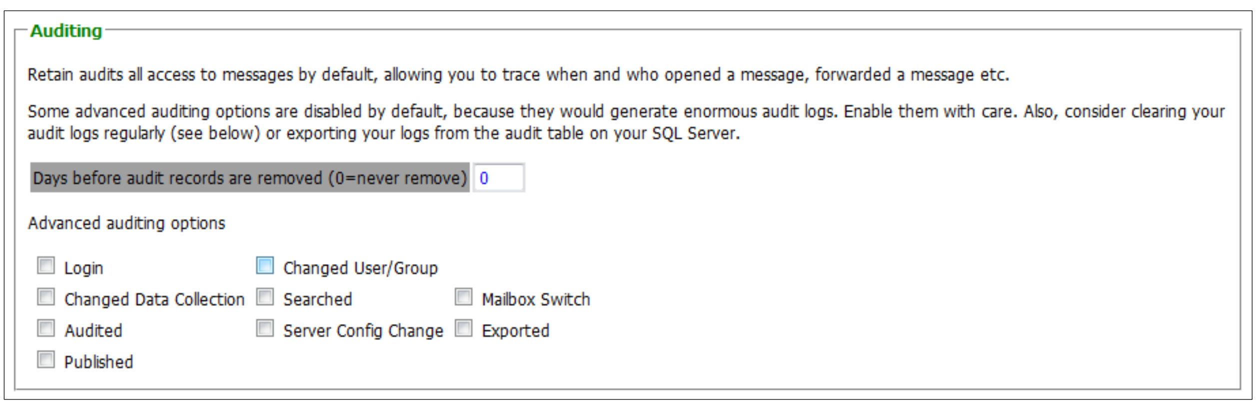
Configure the system logging here. Normally, you want verbose logging. Diagnostic is ordinarily done just for troubleshooting purposes.



You also specify how long to keep logs here. By default, logs are deleted after 10 days. Logs may be compressed to save disk space.

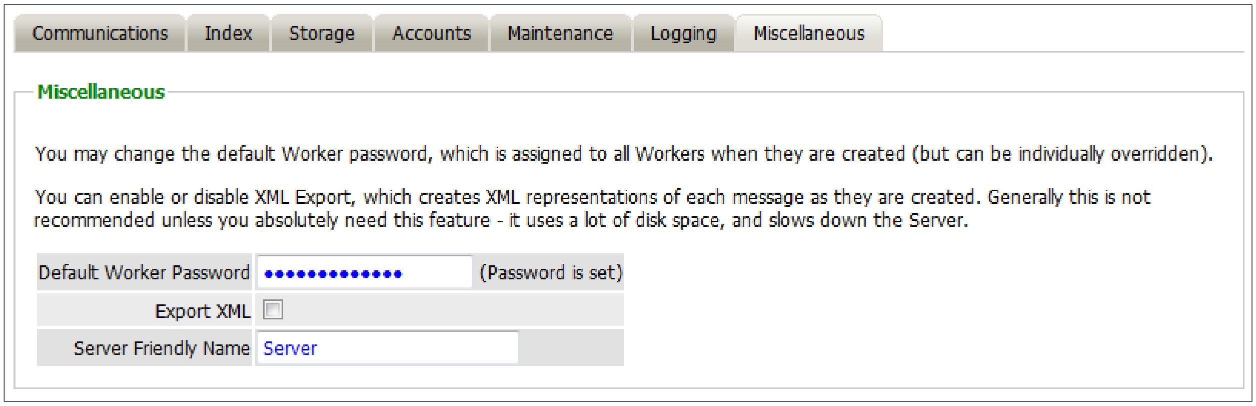
Auditing Records

Retain now will create an auditing record of all actions, specified by the user, which are taken on a specific piece of mail. Auditing records can be removed automatically after a specified length of time. The variable is set in days. All of the options associated with this feature are found under the Server Configuration page, Logging tab.



This logging option creates very detailed logs for the options selected, and it is very important to know that if every option is turned on, the logs can become extremely large. It is highly recommended that an expiration date is set for the logs, so that they are automatically removed from the system to avoid filling up your disk space. Selecting all options for logging will also adversely affect performance. Do not select all the options at one time unless requested by Support.

Miscellaneous



You may choose the default worker password here. One is automatically generated for you when you create a worker but you may change the password here if you like.

Export XML

This XML Export function is included in Retain in case you have an XML compliance mandate. You enable it here.

When selected, each attachment will have an XML export file of its parent message. In other words, an XML representation of the metadata is created and linked to the blobs as the messages are stored. There's nothing more done.

Ordinarily, you would not want to do this because it consumes enormous quantities of disk space, loads up your file system and degrades performance.

When you do NOT use the XML export function, you will benefit from Retain’s single-instance message storage and data compression to save disk space and improve performance.

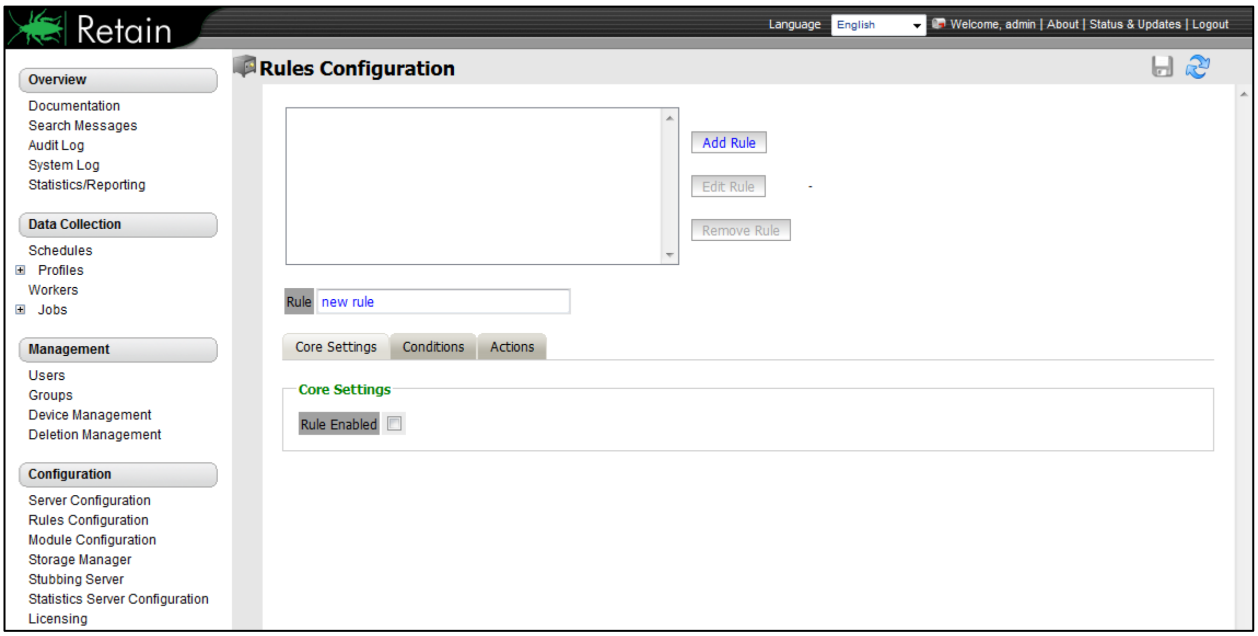
Module Configuration

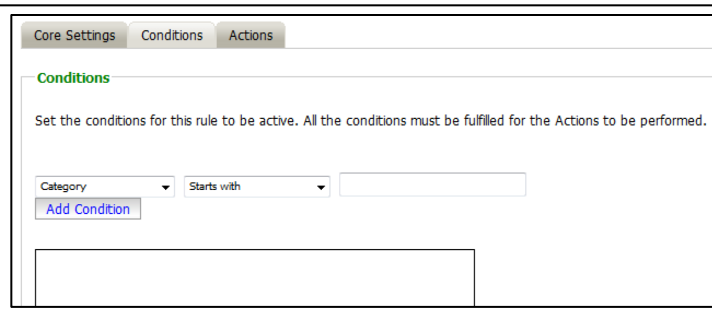
Please see the module configuration section in the initial setup section of the manual.

Rules Configuration

Rules for Retain is a way for administrators to automate tasks and administration based on criteria. This means that any message containing items or information specified in the criteria to have the described action applied automatically. A rule must be enabled, have at least one condition, and one action defined before a rule comes into effect.

To create a rule, select the 'add rule' button and name the rule. To make the rule active, select 'Rule Enabled".

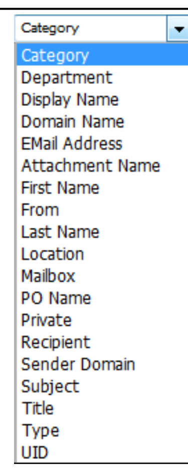


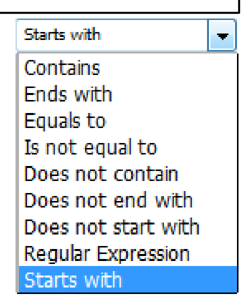


Conditions

The conditions are the criteria which determine whether the action is applied to message data or not.

Criteria is entered in plain text or in regular expression, and are separated into categories. Select the category that the criteria is to be restricted to, from the menu.



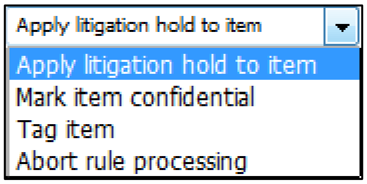


Once a category has been selected, the criteria to be applied to that needs to be specified. The 'Starts with' menu further defines the critieria. The 'Starts with' menu also allows the administrator to either relax some constraints by selecting a vague entry like 'Contains' or 'Starts with', or specify the criteria with 'Regular Expression'. Select the appropriate limiter and then select the 'Add Condition' button. Multiple conditions may be added. Make sure to save changes before leaving the page.

Actions

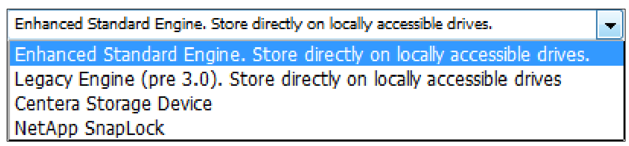
The actions tab defines which actions are to be taken. There are four different options to choose from.

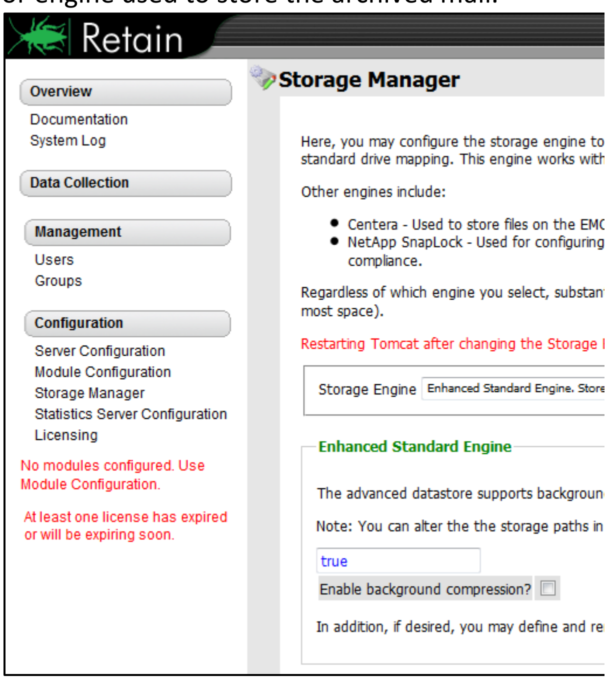
All four actions may be applied to any one rule. Once the desired actions are applied to a rule, save changes before leaving the page.



Storage Manager / Storage Engine

Retain Supports the ability to change the location or engine used to store the archived mail.





To change the storage option settings which were created during the initial setup of Retain, simply select the different storage engine of your choice.

If the Standard Engine is selected, then the Standard Engine window is displayed. This details the setting location for the default storage location, under Server Configuration, Storage tab.

The other three options are:

Legacy Engine
Centera Storage Device
NetApp SnapLock

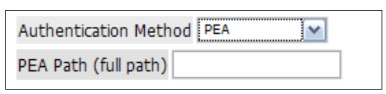
Enhanced Standard Engine
The Enhanced standard storage engine is the standard storage option which should be selected for all new installations of Retain. The storage engine utilizes locally accessible drives and media. When selecting this option, make sure that storage requirements will be easily met, size or capacity increased, and managed.

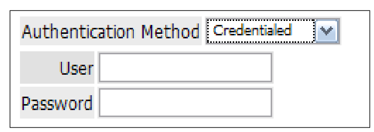
The enhanced engine also allows for background compression to be used. Background compression is recommended for social media and mobile modules, to help keep the size of the data store down.

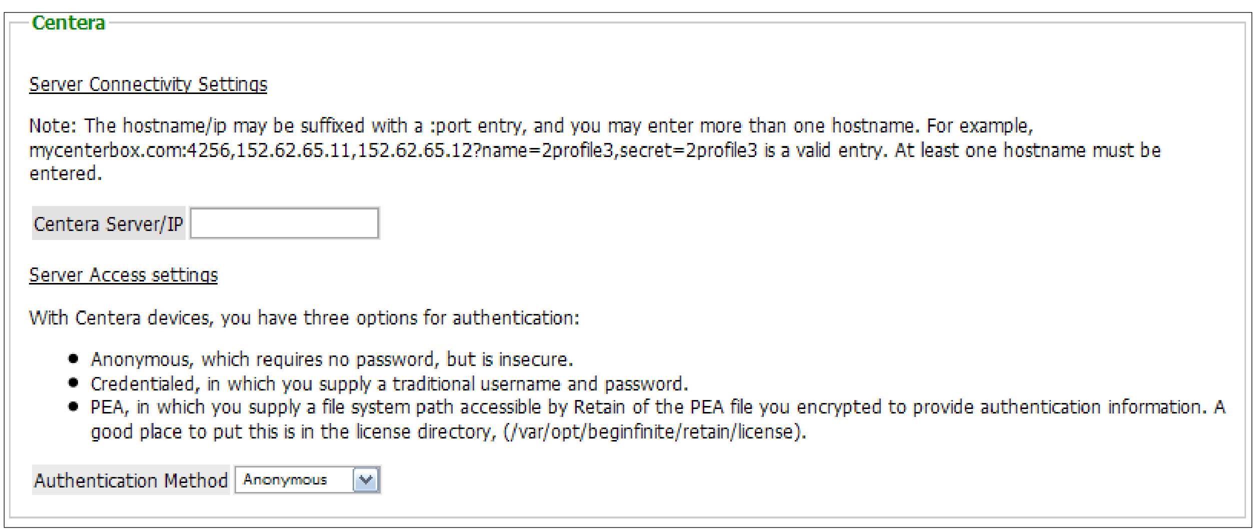
Legacy Engine
The legacy engine works as a seamless connection to the 2.x line of Retain, and is available as a bridge for upgraded devices and legacy support systems.

Centera Storage Device

The Centera Storage option simply requires you to put the storage server IP address or DNS name, and the authentication method.



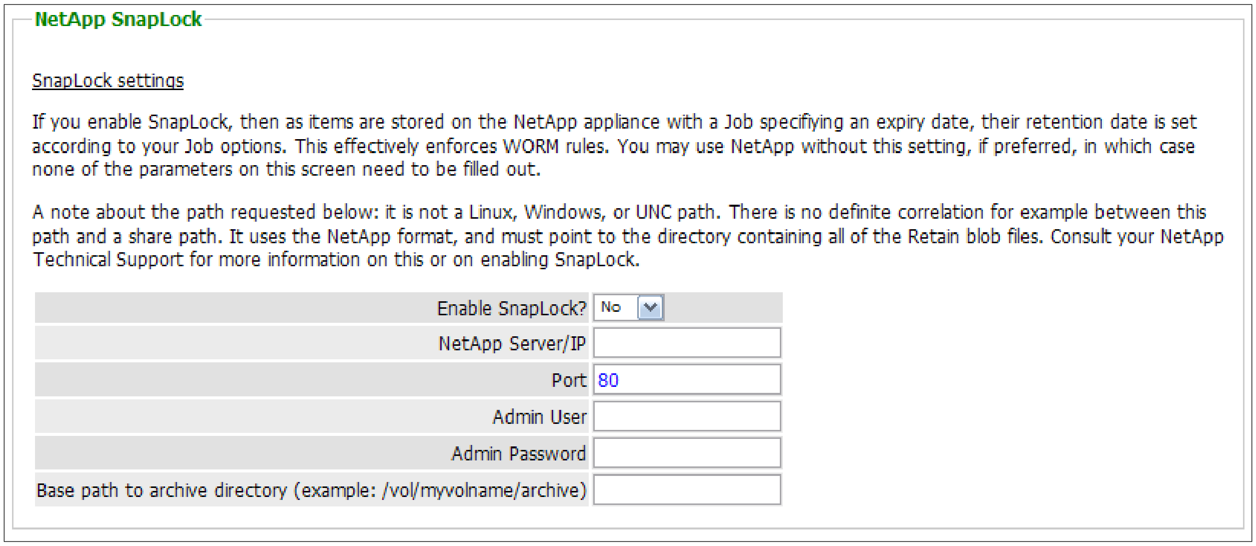




The different Authentication options are PEA and Credentialed. The PEA requires the full path to the PEA file. For a credentialed authentication, simply input the username and the password for the Centera server.

NetApp SnapLock

NetApp is fully supported with SnapLock for storage. Note the information in the option. To enforce WORM rules you MUST set the Job Expiration feature. Also set the IP address, username, password, and the correct path to the server. THE PATH MUST BE SET IN NETAPP FORMAT.



Partitions

Retain also supports the ability to define a different storage location, through the partitioning option. **Partitioning is only available when Storage is set to the 'local' drive.** To access the partitions option click on "partitions" in the Enhanced or Standard Engine window. Ideally, this option would **only** be used to archive to a new, larger, location when the current storage path has been filled, or to separate mail storage between years. (I.e. /archive/2008; /archive/2009)

A Retain system without a specified partition location will store all mail in the default storage location. This is defined in the Server Configuration menu, under the Storage tab mentioned previously. The default location is set during the initial install.

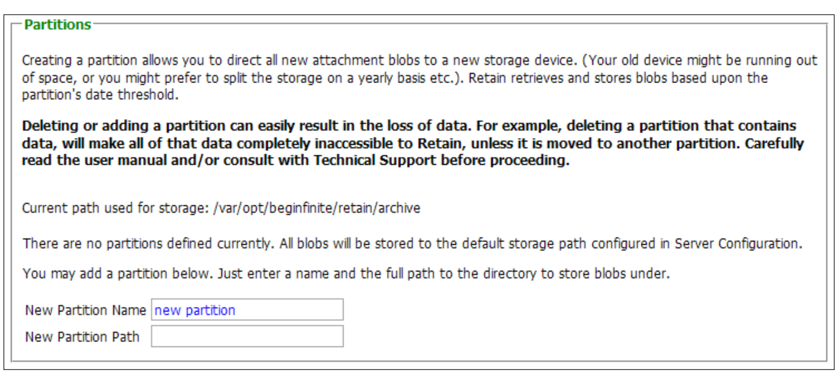
READ THE BOLD WARNING ON CHANGING PARTITIONS!
You may only specify one new partition at a time. After you have entered the new partition information, click 'save changes'. *Creation or changes to a partition requires Tomcat to be restarted.* When adding a Partition on Linux, the path needs to be created manually on the Linux Server before specifying the path within Retain. Ensure that the permissions for the new path are given to Tomcat.

Once Tomcat has been restarted, the new partition can be viewed, edited, or deleted from this window.

Partitions are listed with their Begin Date, Name, and Path. The Begin Date is the creation date. A partition is used to store all archived mail from the moment it is created

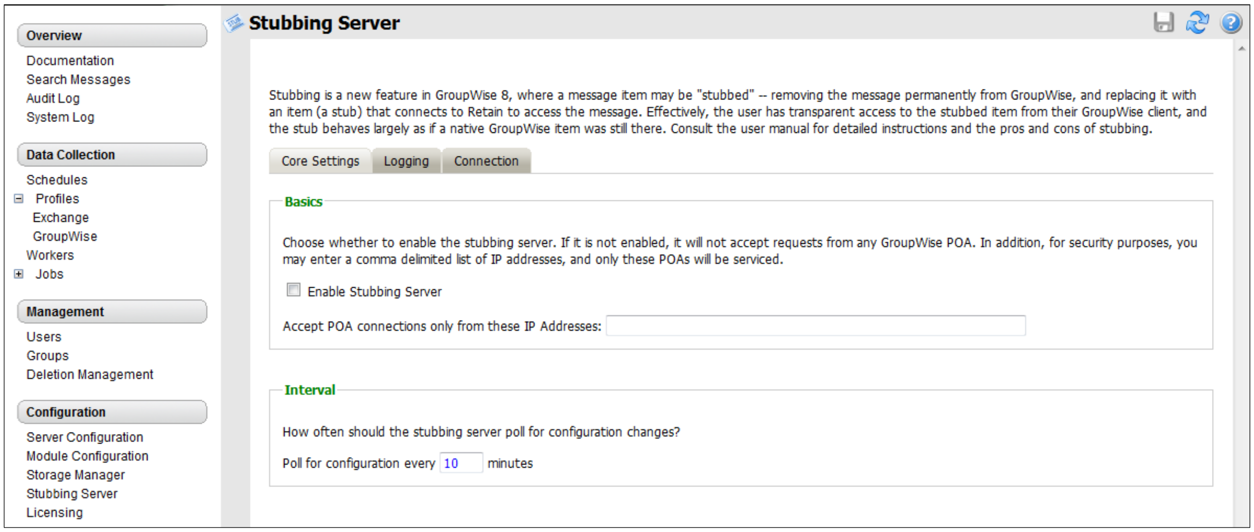
Because of how Retain indexes and tracks messages that are archived, deleting a partition can lead to catastrophic data loss. Do not delete an active storage partition or location without first consulting support.

If a partition is deleted Retain will look for the archived mail that was stored in the deleted partition to be stored in the default storage location. (This is defined in Server Configuration, under the Storage tab.) Removing a designated partition in the management console does not delete the storage directories or data on the hard drive or SAN, but it does disconnect Retain from the storage location.



All partition changes are logged in the partition.log file, located in the backup directory specified in Server Configuration. (By default this is located in <your storage location>/backup)

Stubbing Server



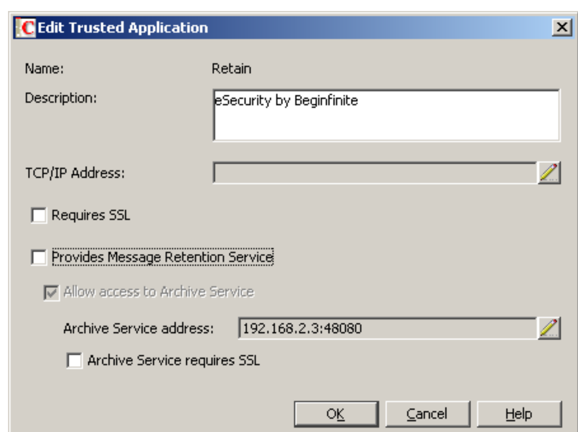
To set up stubbing, you must perform the following tasks:

1. You **must** be running GroupWise 8.0HP1 Post Office Agent(s). **Once enabled, the stubbing process cannot be reversed. Stubbing requires GroupWise 8.0HP1. Previous versions of GroupWise do not contain critical stability fixes.**
2. ConsoleOne must be configured as discussed below.
3. Retain job profiles must have Stubbing turned on. (see the Profiles section)
4. Stubbing server must be installed and setup as discussed below. (For install see your platform install guide.)

ConsoleOne GroupWise settings

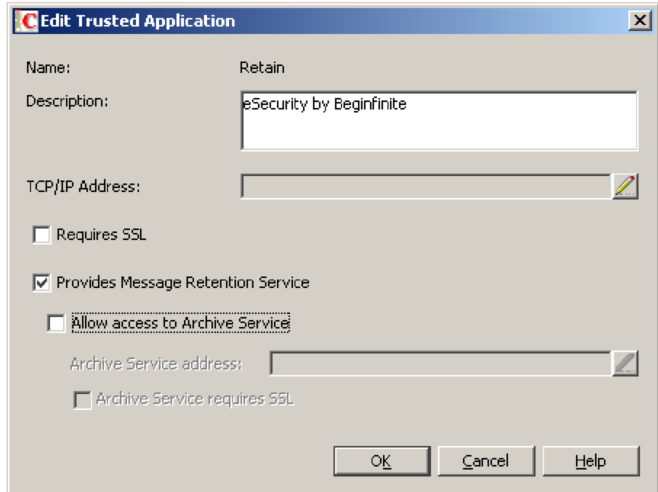
For the Retain Server to function, GroupWise must be told where the Stub Server is located.
In ConsoleOne;

- Connect to the domain and highlight the domain or GroupWise system.
- Select Tools | GroupWise System Operations | Trusted Applications
- Select Retain and click Edit.
- Select “Allow Access to Archive Server”



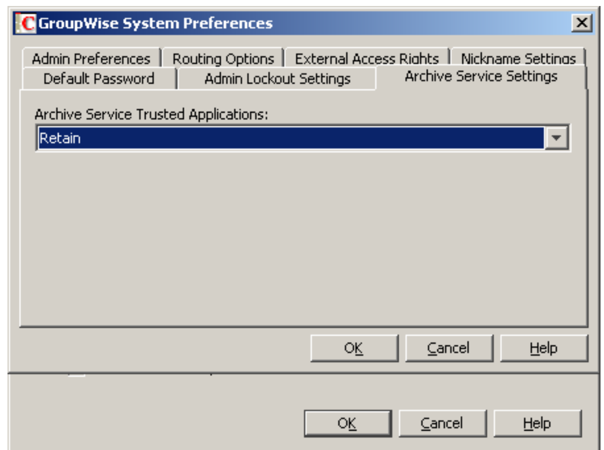
- Put the address or DNS name of the Stub Server and the correct port as shown. (48080)
- Click OK and exit the rest of the windows.

Your settings should look the same as the settings pictured here with your specific DNS or IP address for the Stub Server.

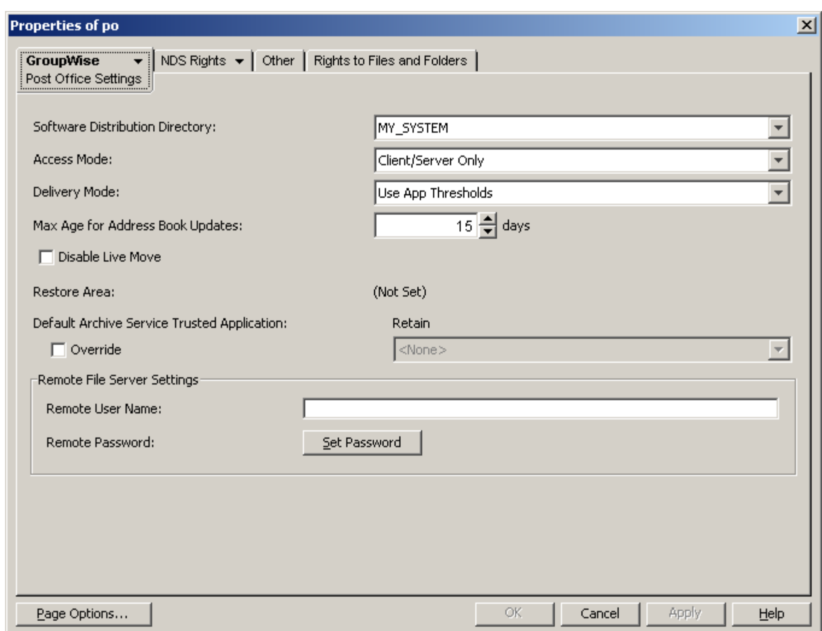


We also need to change the settings in the preferences menu:

- Connect to the domain and highlight the domain or GroupWise system.
- Select Tools | GroupWise System Operations | System Preferences…
- Ensure that Retain is set under the Archive Service Settings as a trusted Application. Select it if it is not already selected.

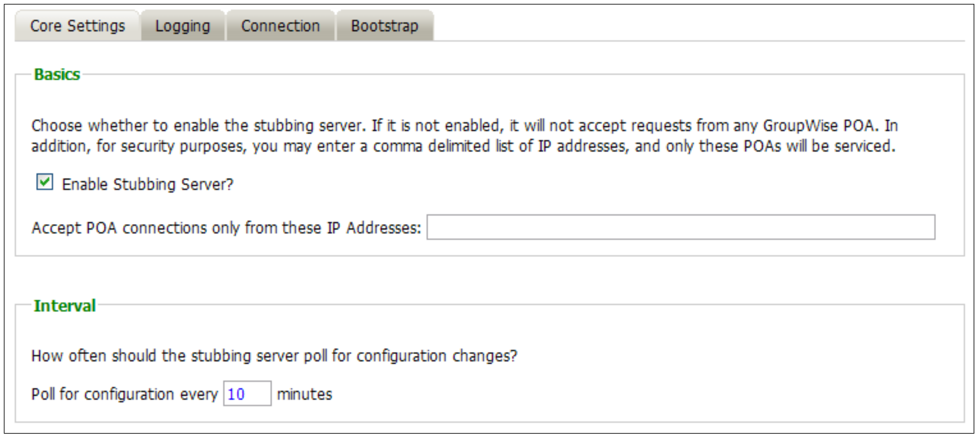


Set the Post Office Remote File Server Settings.
Enter the properties of the Post office. The settings should look as they do here.
Retain should be listed as the Default Archive Service Trusted Application. If it is not set as the default, override and select Retain.



Retain Stubbing Settings

Job profiles must have Stubbing enabled for the Server to function. See the Profiles section for details. The Stub Server must first be enabled in order to allow access to the bootstrap file required for communications. Set the interval as desired. (10 min. is lowest recommended setting. Anything lower may be unnecessary.)

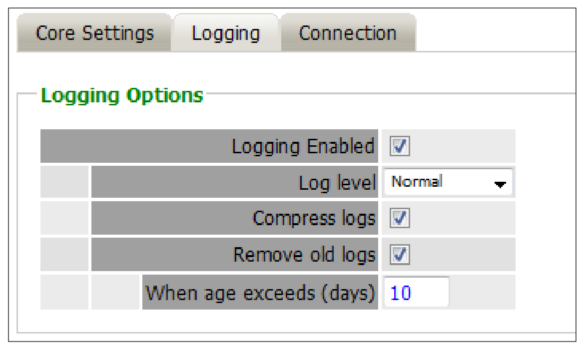


If you wish to restrict connections to the Stub Server, input the IP address(es) of all the Post Offices that the Stub Server will service. Use commas to separate multiple addresses.

Save changes before continuing.

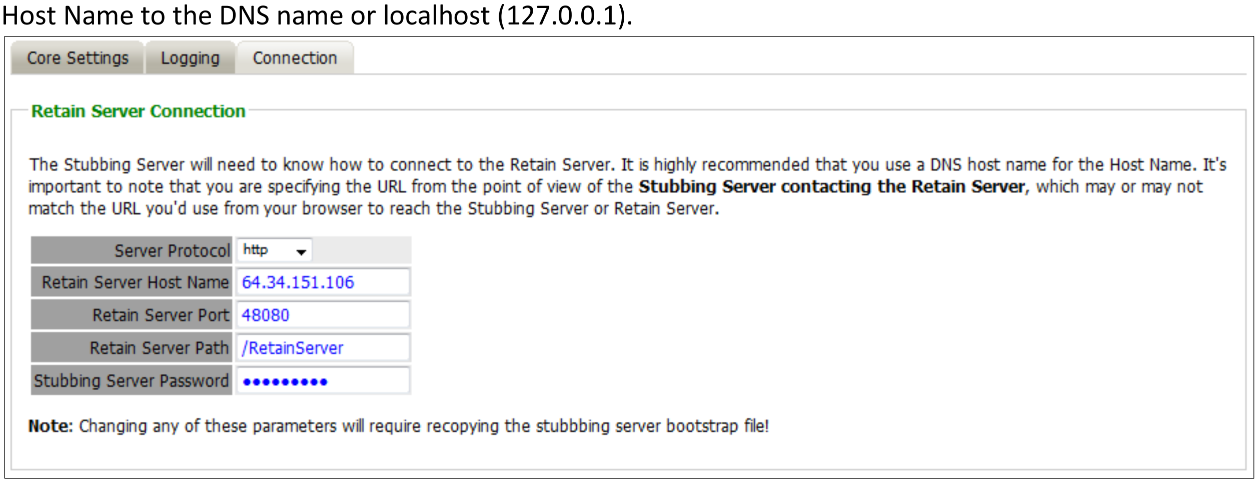
Logging

Log levels higher than Normal are not necessary unless troubleshooting or working with Support. It is strongly recommended to compress and remove logs after a time period to protect system space. Set time to desired level.

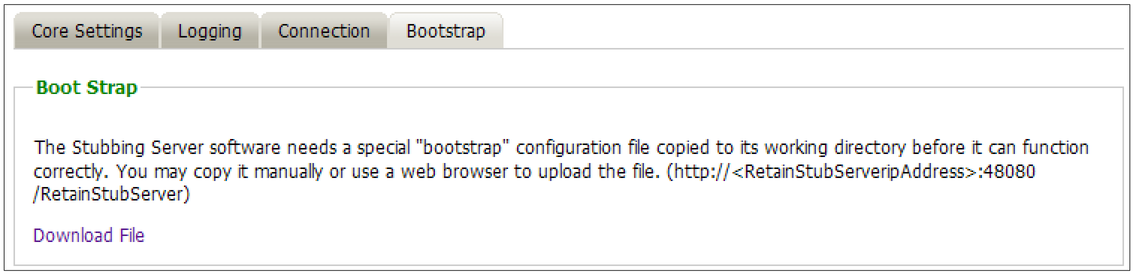


Connection

The connection to the Retain Server is very important. This must be set to the address of the Retain Server, and is automatically filled out for you. Verify that the Retain Server is located at the specified address and is accessible. Generally you may leave this section default as the Stub Server should be installed local to the Retain Server. If your Retain Server IP address is assigned by DHCP, change the Host Name to the DNS name or localhost (127.0.0.1).



When you have finished configuring the Stub Server, Save your changes and select the Bootstrap tab. (The bootstrap tab will not be available unless the Stubbing Server has been enabled and settings saved.)



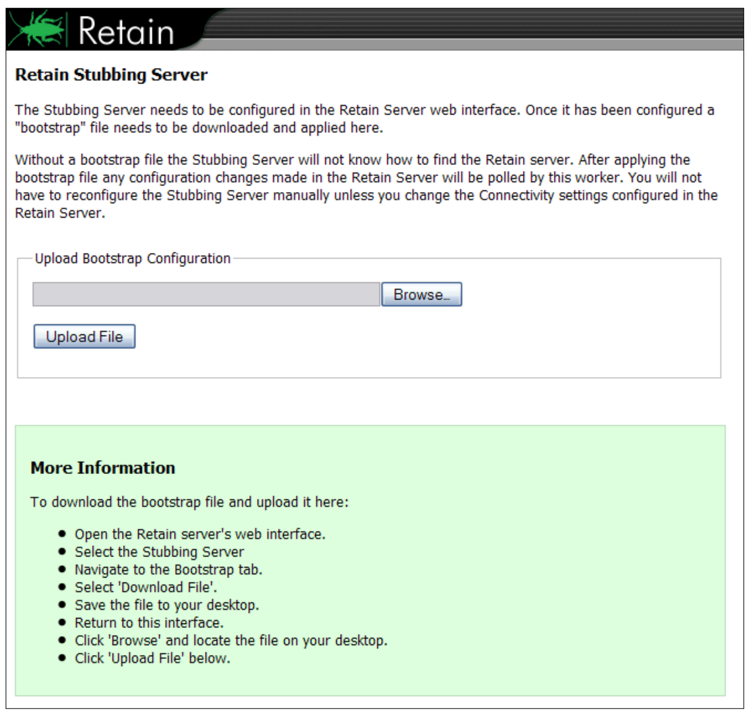
Download and save the bootstrap file.

Open a new browser tab or window, and browse to the Stub Server. The Stub Server answers to the following address (The address is case sensitive):

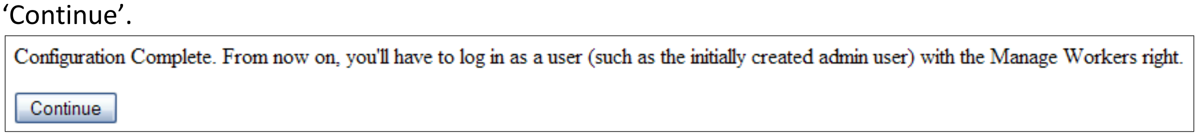
http://<IP address of StubServer>:48080/RetainStubServer

You should see a window like the one pictured here.

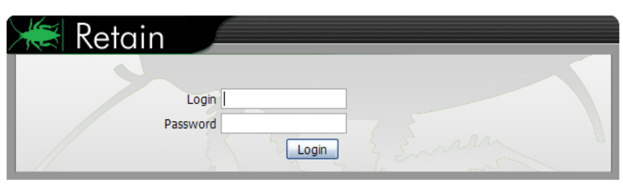
- ➢ Click 'Browse' and browse to the location where you saved the bootstrap file.
- ➢ Select the "StubConfig.cfg" file and select 'Open'.
- ➢ Select the 'Upload File' button.



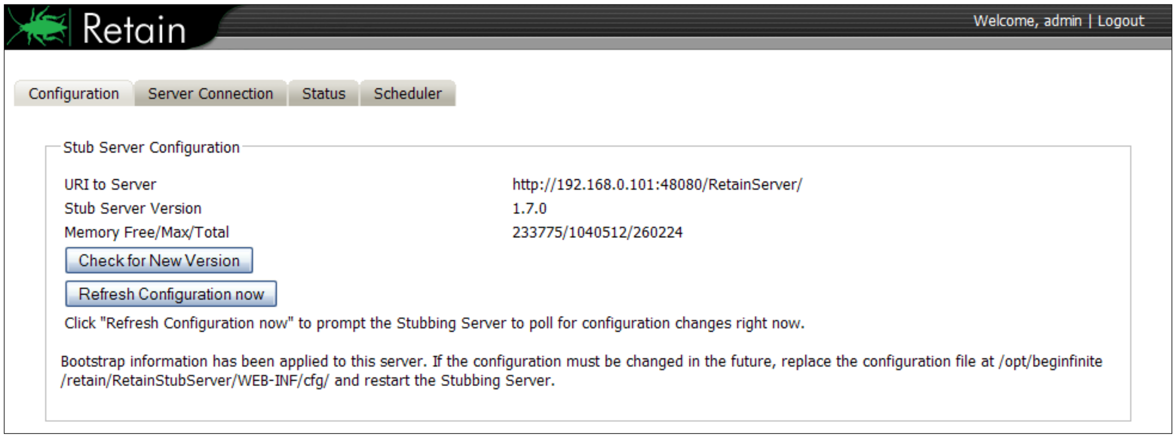
After uploading the configuration file, the Stub Server will alert you that it requires authentication from a user with the "Manage Workers" right. Click 'Continue'.



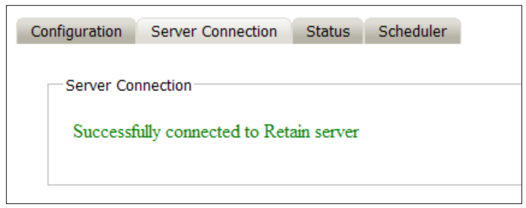
We can now Login to the Stub Server.
You must Login with a user that has sufficient rights. See the User Rights section to add or remove rights.



The Stub Server Interface is nearly identical to the Worker interface. You may check for updated versions of the Stub Server or manually trigger server polling by selecting the Refresh 'Configuration now' button.

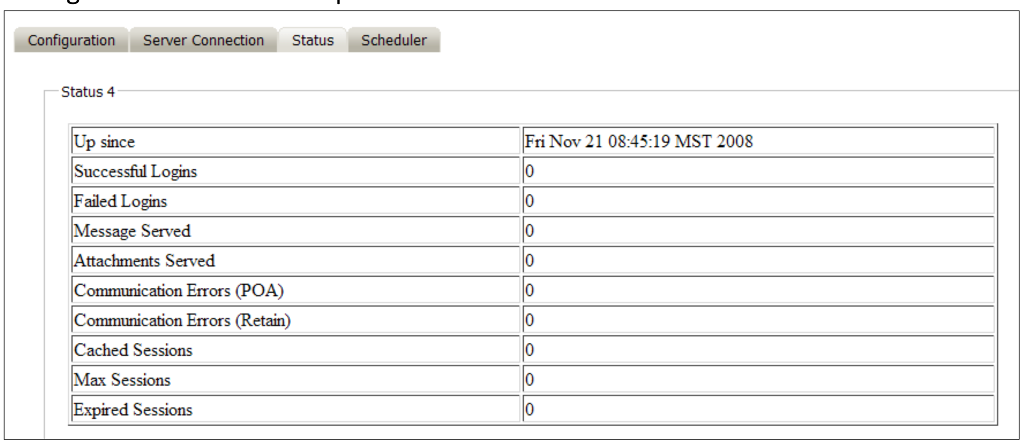


Check the **Server Connection** tab to verify the connection to the Server.



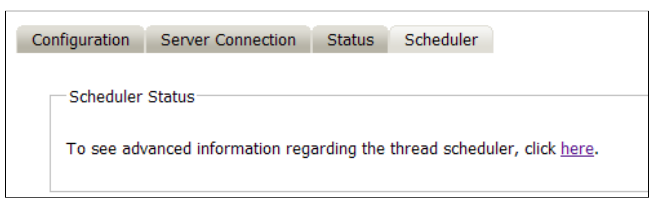
Status

The Status tab gives statistics about up-time and function.



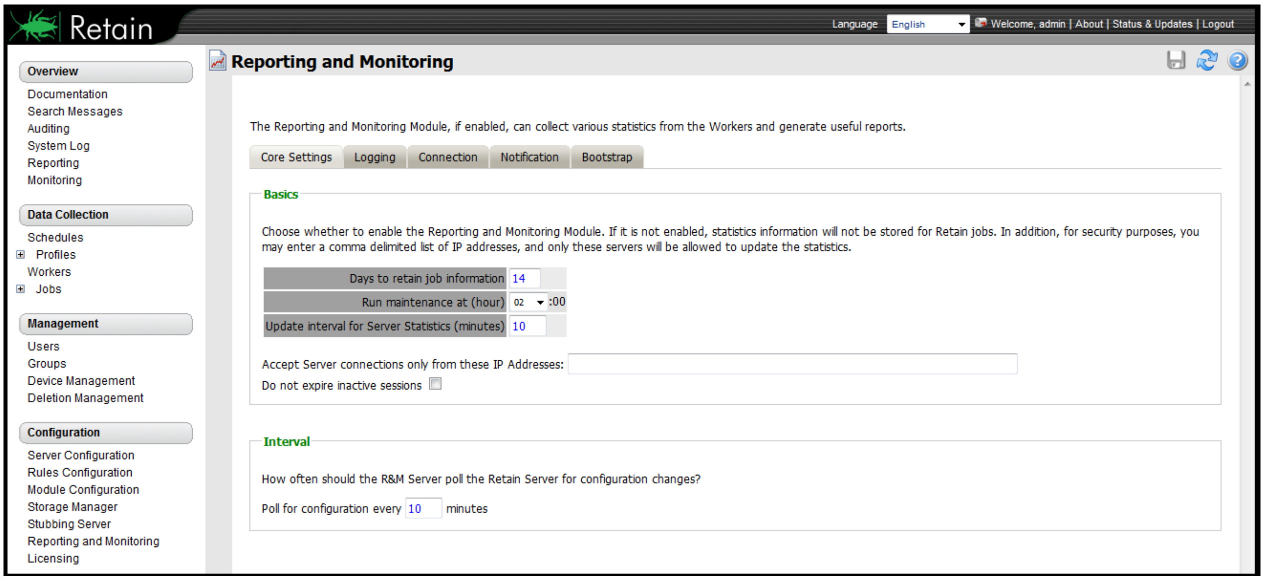
Scheduler

The scheduler tab contains the configuration details sent by the Server this tab is mainly used for Support.



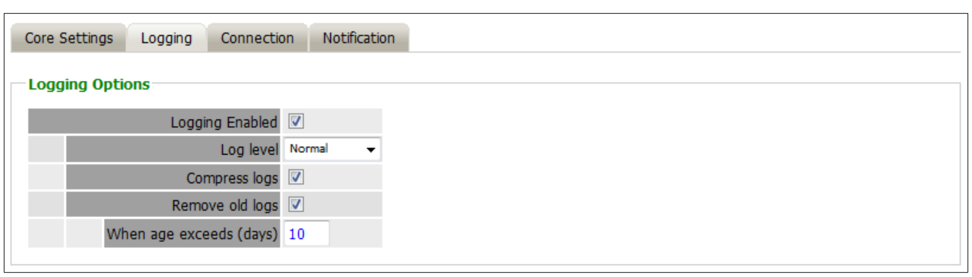
Reporting and Monitoring Configuration

Retain comes equipped with a separate Reporting and monitoring server. Reporting and Monitoring may be installed on the same or a different physical or virtual machine as the Retain Server.

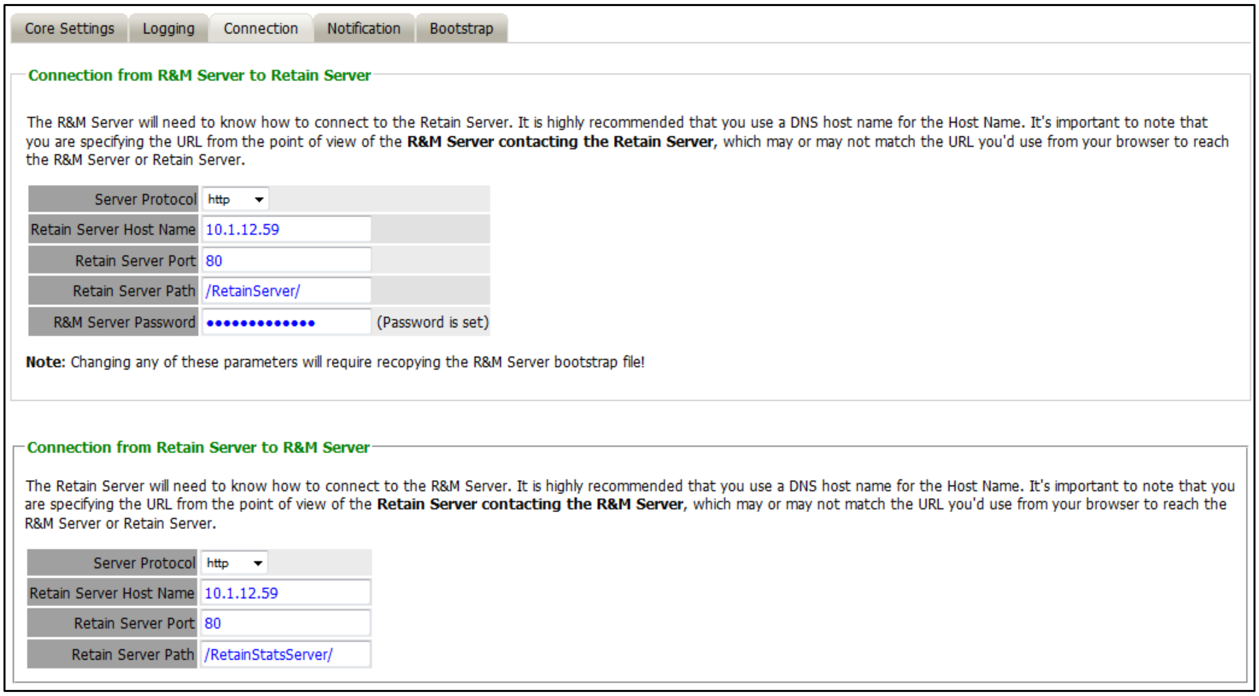


Reporting and Monitoring functions much like the Retain Worker in that it is installed as a separate entity and requires connection information from the Retain Server. Additional security is provided through the option to specify exactly which IP address(es) the Retain Server will allow a connection from. Separate with commas the IP addresses allowed if more than one. No mail data is transferred through this connection, only server statistic information.

The Core Settings, Logging, Connection and Notification sections of Reporting and Monitoring configuration work identically to the Worker connection settings, and should be filled-out accordingly. Most server implementations will require little to no modification to these settings save the notification tab. Putting a checkmark in the 'Do not expire inactive sessions' will allow sessions with the R&M module to never expire. This is useful in conjunction with the 'monitoring' page.

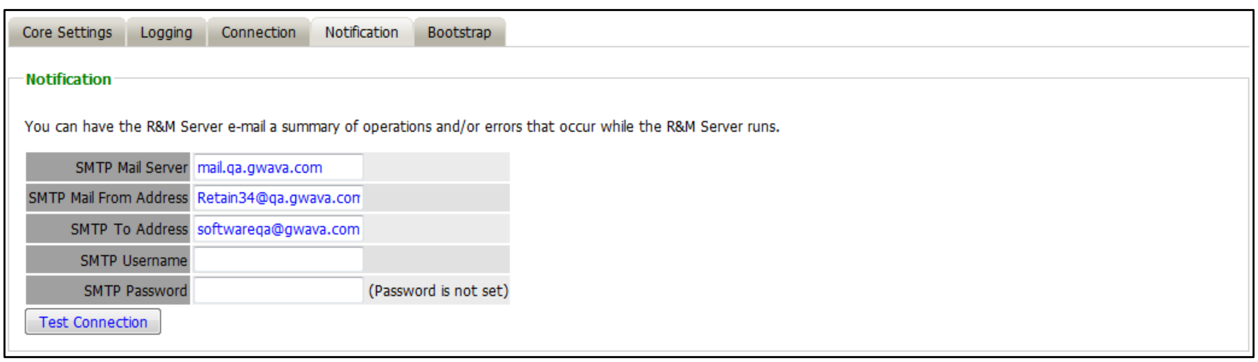


Set the logging level to the desired setting. Leaving the logging as default 'normal' is recommended unless instructed to increase the logging level by Support.

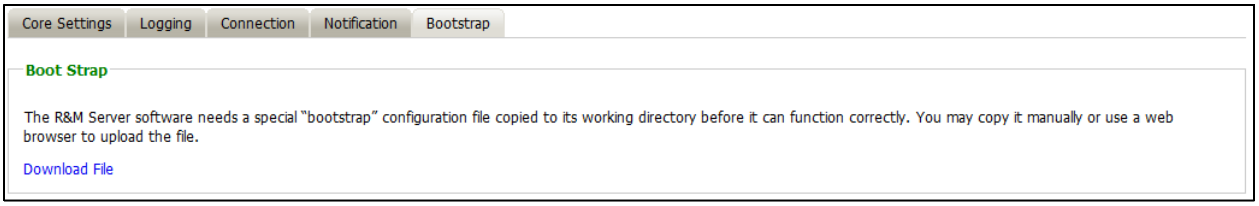


The Connection between Reporting and Monitoring, and the Retain Server should not be changed unless the Retain Server requires a modified connection path, (such as a custom port.)

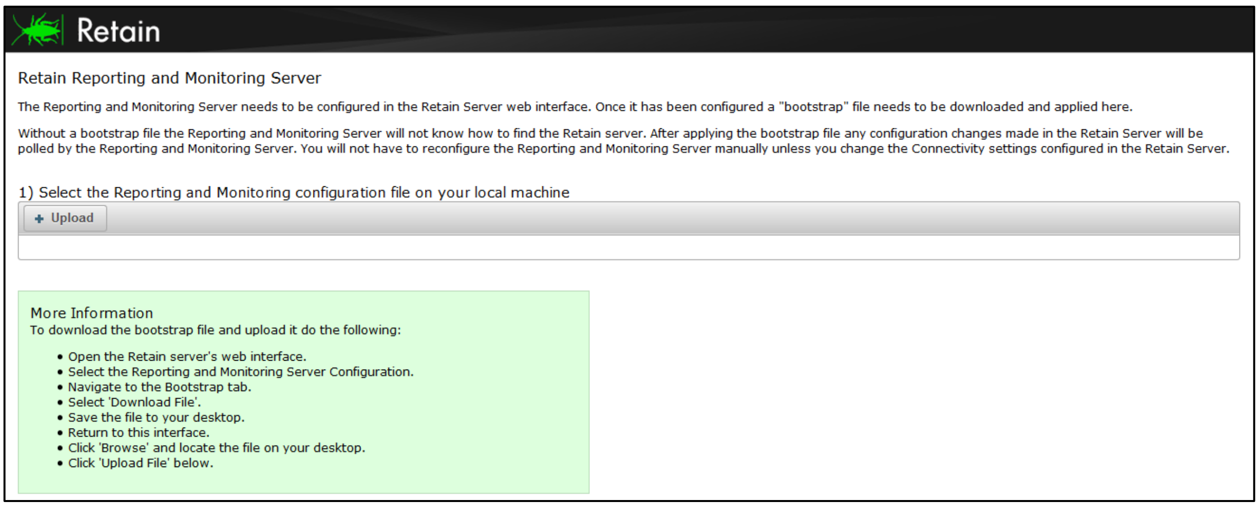
The R&M server is different from the Retain Worker in that the Retain Server is able to contact the R&M server as well. The connection address to R&M should not be modified unless custom connection settings have been created.



Notification defaults to the standard notification address specified in the Retain Server activation and initial configuration. If the notification is desired to be different, modify the settings here. Make sure to test the connection to ensure proper function.



Like the Retain Worker, the R&M server must be uploaded a saved configuration or 'bootstrap' file. To access this tab, the configuration must be saved first. Then the bootstrap tab will become available. Download the file to a known location and then browse to the R&M server webpage. The default connection address is shown on the connection tab.
Ie. http://<ip_address_of_server/RetainStatsServer



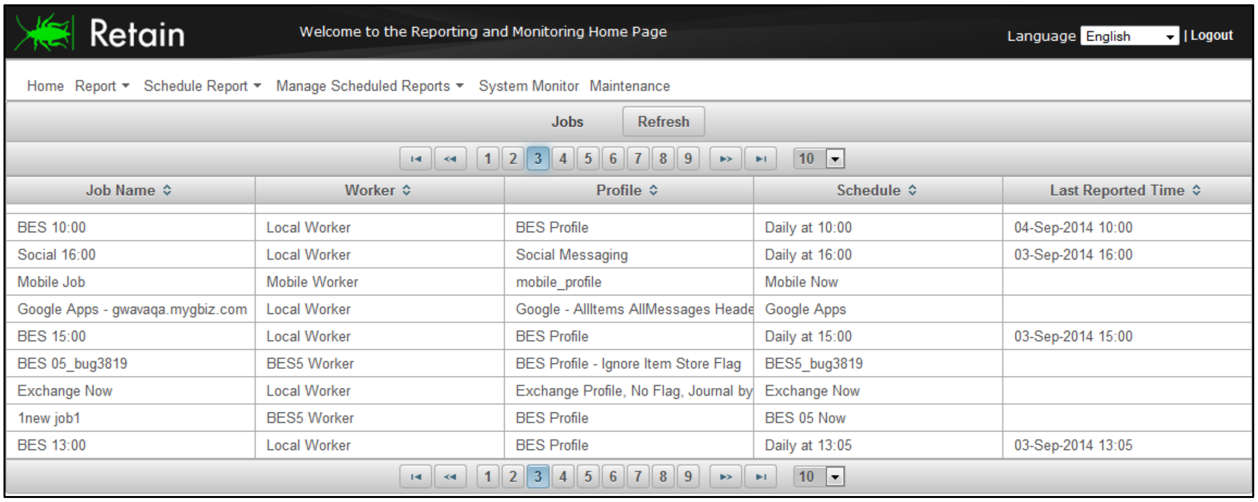
From the R&M initial webpage, click on the "Browse" button and browse to the saved bootstrap file and select it.

Click 'Continue' to upload the bootstrap file. As the bootstrap file is uploaded, R&M functions will become available. Only users with the administrative "manage server" rights will be able to login to the stat server.

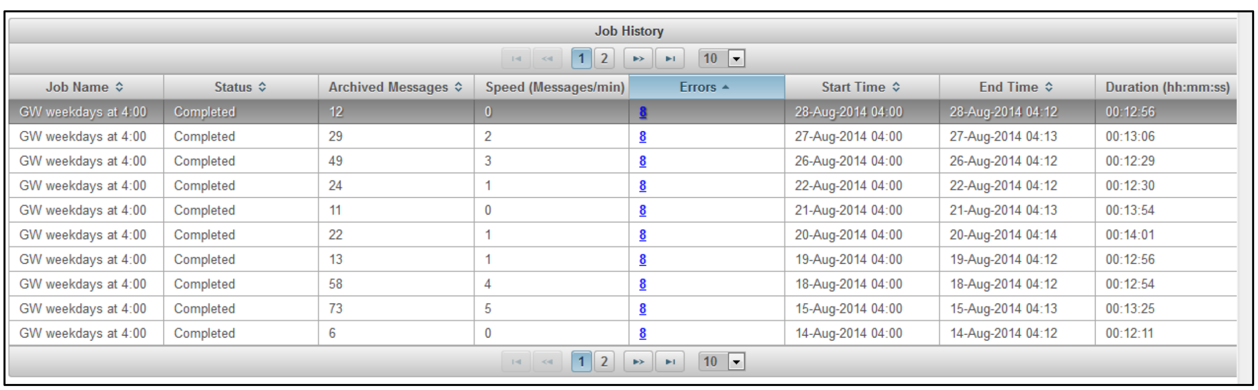
To log into the R&M server, select the 'Reporting' or 'Monitoring' links from the Retain Server left menu to spawn a new tab or page to the R&M module.

Home

On login, Reporting and Monitoring opens to the Home page. The Home page is also accessible through the 'Home' button along the top bar. The R&M server has different page links and menus across the top of the menu bar, accessing different functionality. The R&M server has many tables and columns displaying a large amount of information. To make this information more accessible, every column has been made sortable. To sort the columns, simply click on them. They may be sorted to show the highest number first, lowest number first, or not sorted at all.

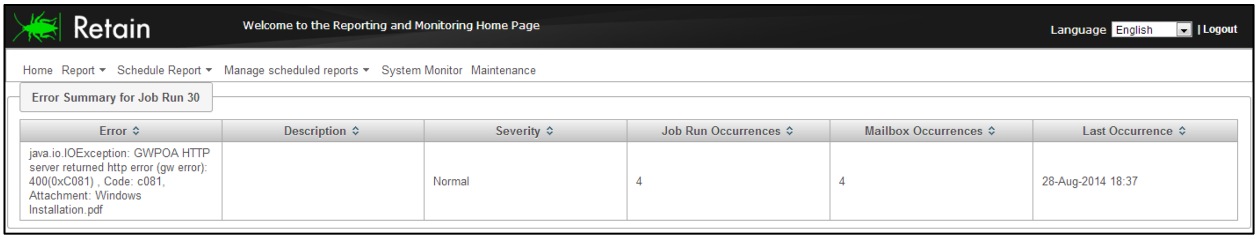


The Home page list the different jobs, associated workers, profiles, schedules, and last reported run times configured for the system. These jobs can be selected to display the job history and detailed information for each instance of when that job was run.



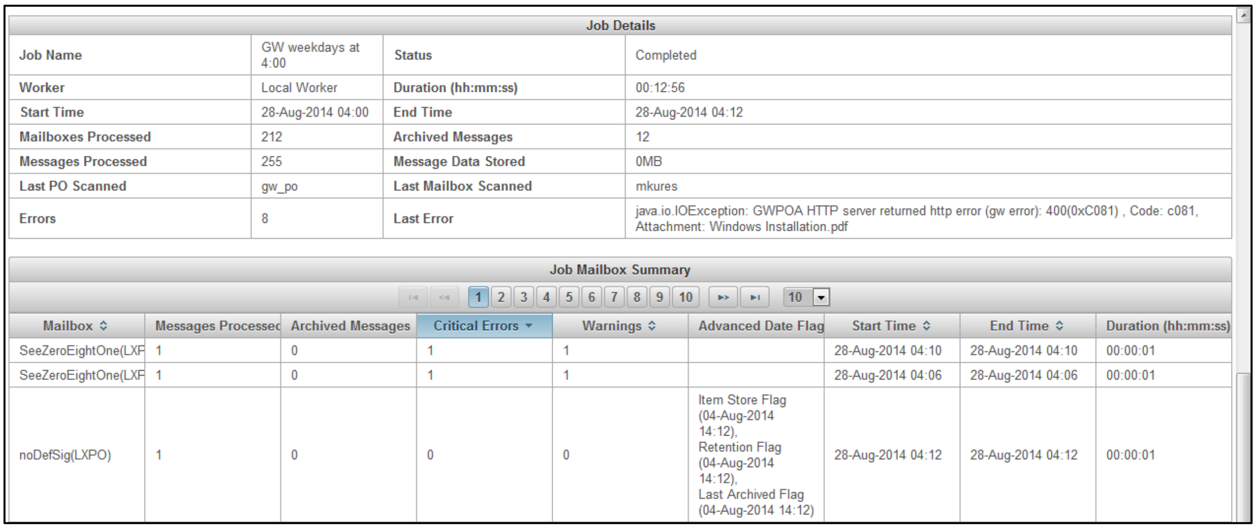
Further selection of a listed job instance will display details for that selected run of the selected job. If an error exists on any job, it will show up as a linked number under the error column. Errors reported here are linked to information on the error which has occurred.

A selected error will spawn a new window which displays the error and any applicable information, such as any associated files or error code numbers, a quick description (if a Retain error), the severity level, how often it has occurred, and in how many different mailboxes it has occurred.



Error	Description	Severity	Job Run Occurrences	Mailbox Occurrences	Last Occurrence
java.io.IOException: GWPOA HTTP server returned http error (gw error): 400(0xC081) , Code: c081, Attachment: Windows Installation.pdf		Normal	4	4	28-Aug-2014 18:37

The last error encountered in a job is also displayed in the Job details window. Select a column header to sort it as desired. The Critical Errors column shown below has been sorted to show the highest number of errors first.



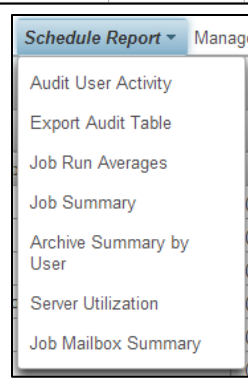
Job Details

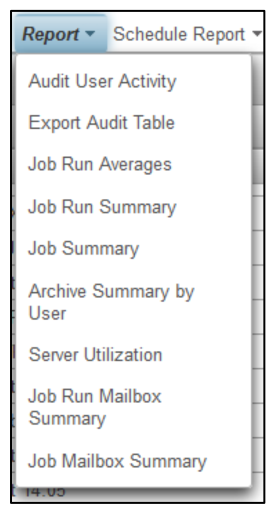
Job Name	GW weekdays at 4:00	Status	Completed
Worker	Local Worker	Duration (hh:mm:ss)	00:12:56
Start Time	28-Aug-2014 04:00	End Time	28-Aug-2014 04:12
Mailboxes Processed	212	Archived Messages	12
Messages Processed	255	Message Data Stored	0MB
Last PO Scanned	gw_po	Last Mailbox Scanned	mkures
Errors	8	Last Error	java.io.IOException: GWPOA HTTP server returned http error (gw error): 400(0xC081) , Code: c081, Attachment: Windows Installation.pdf

Job Mailbox Summary

Mailbox	Messages Processed	Archived Messages	Critical Errors	Warnings	Advanced Date Flag	Start Time	End Time	Duration (hh:mm:ss)
SeeZeroEightOne(LXF	1	0	1	1		28-Aug-2014 04:10	28-Aug-2014 04:10	00:00:01
SeeZeroEightOne(LXF	1	0	1	1		28-Aug-2014 04:06	28-Aug-2014 04:06	00:00:01
noDefSig(LXPO)	1	0	0	0	Item Store Flag (04-Aug-2014 14:12), Retention Flag (04-Aug-2014 14:12), Last Archived Flag (04-Aug-2014 14:12)	28-Aug-2014 04:12	28-Aug-2014 04:12	00:00:01

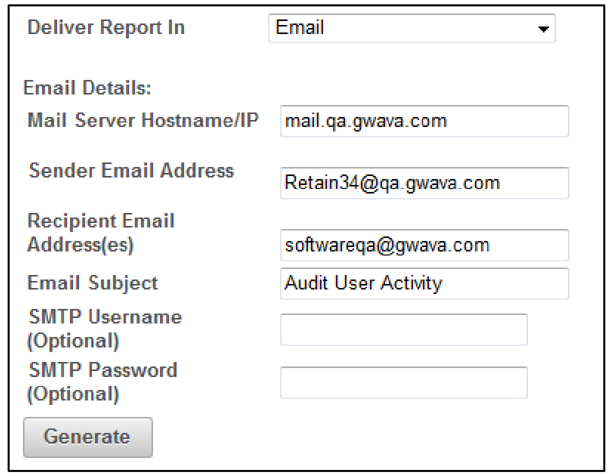
Report and Schedule Report





Report and Schedule Report functions are accessed through drop-down menus in the interface. To access the different reports, select the 'Report' or 'Schedule Report' menus from the top menu and then click on the desired report. Most reports which are accessible through the 'Report' menu are also available as a 'Scheduled Report', except for 'Job Run Summary, and 'Job Run Mailbox Summary'. All reports under the 'Report' menu except 'Job Run Summary and Job Run Mailbox Summary, can be scheduled and have a 'Schedule' button at the bottom of the delivered HTML report. Selecting this button copies the settings used to generate the visible report to the Schedule Report interface. This convenience is designed to allow rapid fine-tuning of reports to deliver the desired information. First select the report you wish to run, and then fine-tune the report until it reaches the desired effect. Once the desired settings have been achieved, select the 'Schedule' button from the bottom of the report to carry all settings into the corresponding 'Schedule Report' interface, and schedule the report.

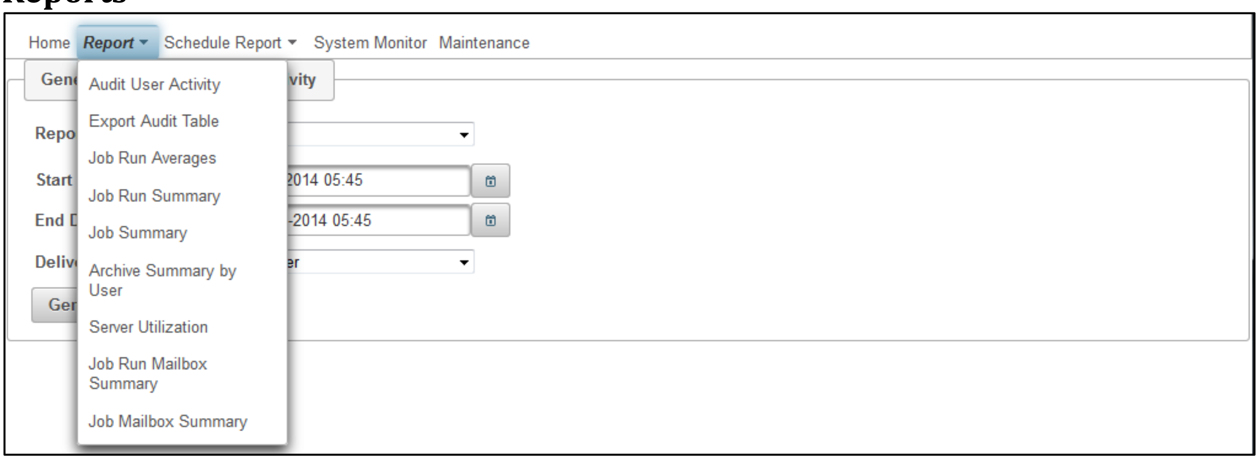
Reports differ from Scheduled reports in more than immediate delivery, reports support HTML in addition to PDF and XLS delivery formats. However, both report structures may be emailed to a desired recipient. When a report is created and emailed it is formatted as selected and then attached to a message which is sent to the desired recipient. When the Email delivery option is selected, additional configuration is required. The R&M module needs to know not only what address to send the report to and what mail server to use, but also allows the configuration of the email subject and sender address. If an SMTP username and password are required for the desired host system, they should be provided.



The R&M module will automatically copy the SMTP configuration from the Retain Server. If this information is not correct, it should be configured here before selecting the 'Generate' button.

This configuration is the same interface for all emailed reports, immediate and scheduled.

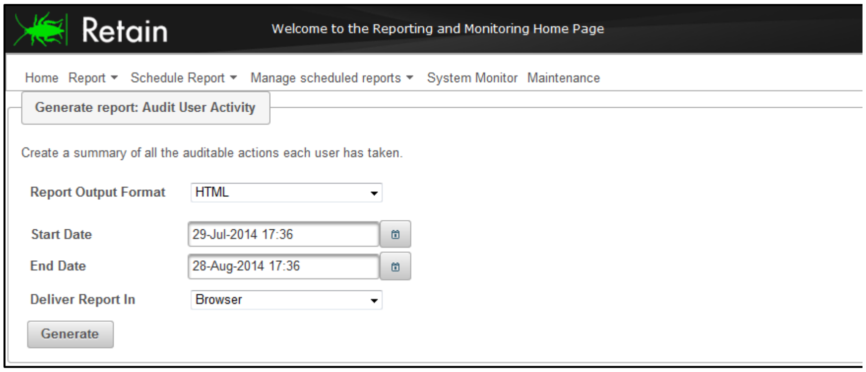
Reports

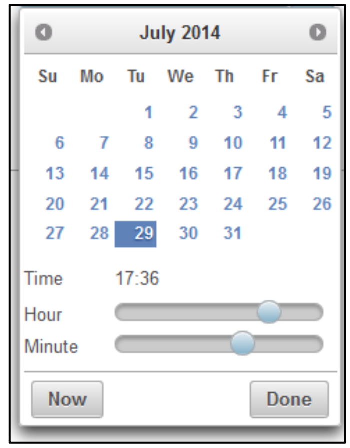


Reports may be created in HTML, PDF, or XLS, and may be delivered straight to the Browser or in a specified email. Different reports have different settings, however the basics are the same; select or specify the desired criteria, specify the format and delivery method, then click on the "Generate" button to create the report.

Audit User Activity

The Audit User Activity report details the different actions performed in the Retain system by different users. This report is a detailed list of all auditable actions taken and which users took them in the Retain system.





While this report lists all actions by all users, it may still be restricted by a date range. The date ranges are specified through a calendar interface.

The date and year are selected through the top bar, while the hour and minute, if desired, are selected through sliders. The date can be immediately set to the current moment by selecting the 'Now' button. When configuration has been completed, select the 'Done' button to set the date. Both the Start and End Date have identical date tools.

When the settings are as desired select the 'Generate' button to create the report.

The report lists all users, a quick description of the action taken and how many times it was performed, and the date of the last time it was performed. Actions such as viewing an item, searching the archive, changing settings on either the server or in the interface, forwarding items, applying litigation holds, publishing items, etc. To take the same settings used when creating this report, select the 'Schedule' button to enter the Schedule Report interface with the same settings.

Schedule

Retain

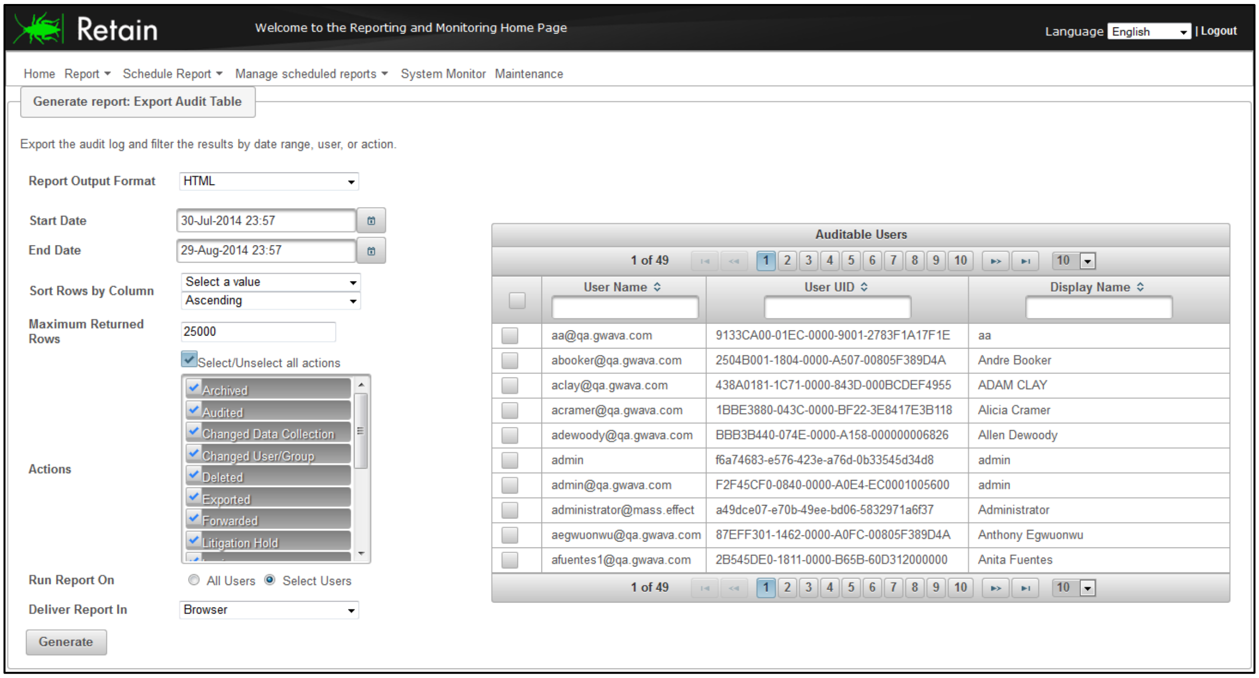
Actions Performed on Archive

User Name	Count	Action	Last Action
admin	9	Changed Server	18-Aug-2014 14:55
admin2	4	Viewed	14-Aug-2014 09:02
	3	Searched	28-Aug-2014 09:47
	5	Changed Server	28-Aug-2014 14:13
benb			
benb.ntpo2.ntdom			
briceb			
daronp			
demo			
dlnuttall			
ericm			
hakimr			
james			
james2			
jasonb			
johns			
matts			
rickl	69738	Published	21-Aug-2014 09:22
saren@mass.effect			
shepard@mass.effect			

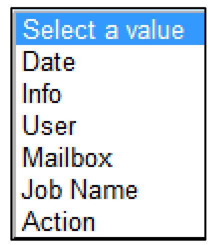
Friday 29 August 2014 Page 1 of 1

Export Audit Table

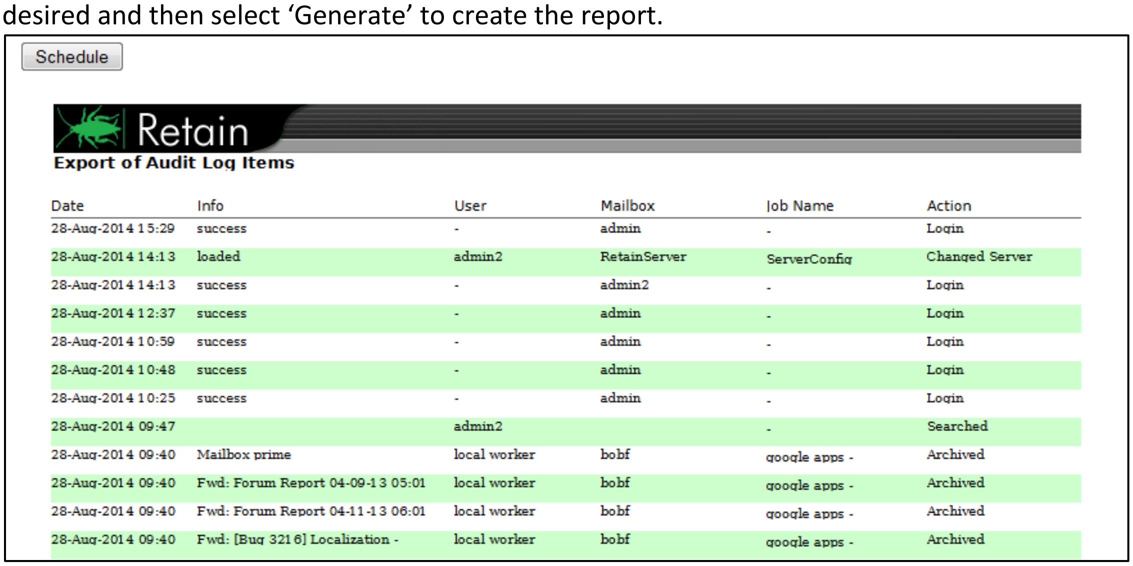
The Export Audit Table sorts the entire Audit log with the settings desired and creates a report for specific users or all users, with specific events or all events. This report can be limited in size and date.



If restricting the report to a specific user or users, a menu displaying ‘auditable users’ is displayed. The different fields are searchable. The option to select all, or none, is also present. Users may be searched for via User Name or email address, User UID, or the user Display Name.



The rows and columns are not sortable in the generated report, but they can be sorted or organized from the report generation interface. The rows may be organized by the columns listed. This has the exact same effect as organizing columns for the jobs on the reporting and monitoring home page. Configure as desired and then select ‘Generate’ to create the report.

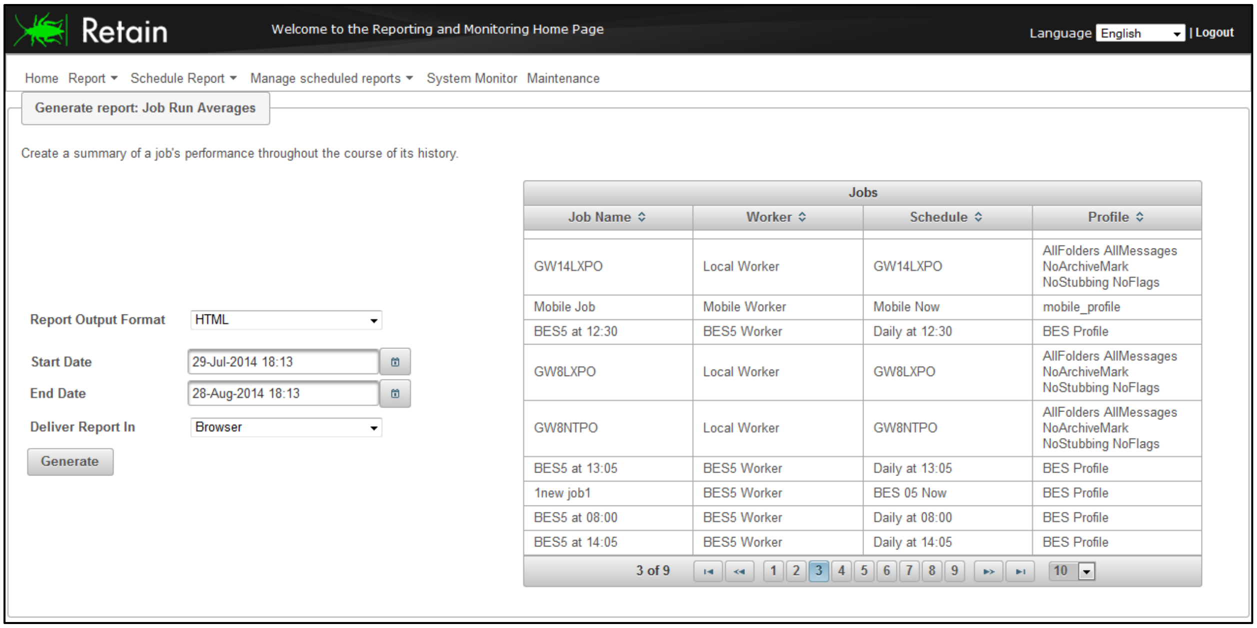


Date	Info	User	Mailbox	Job Name	Action
28-Aug-2014 15:29	success	-	admin	-	Login
28-Aug-2014 14:13	loaded	admin2	RetainServer	ServerConfig	Changed Server
28-Aug-2014 14:13	success	-	admin2	-	Login
28-Aug-2014 12:37	success	-	admin	-	Login
28-Aug-2014 10:59	success	-	admin	-	Login
28-Aug-2014 10:48	success	-	admin	-	Login
28-Aug-2014 10:25	success	-	admin	-	Login
28-Aug-2014 09:47		admin2		-	Searched
28-Aug-2014 09:40	Mailbox prime	local worker	bobf	google apps -	Archived
28-Aug-2014 09:40	Fwd: Forum Report 04-09-13 05:01	local worker	bobf	google apps -	Archived
28-Aug-2014 09:40	Fwd: Forum Report 04-11-13 06:01	local worker	bobf	google apps -	Archived
28-Aug-2014 09:40	Fwd: [Bug 3216] Localization -	local worker	bobf	google apps -	Archived

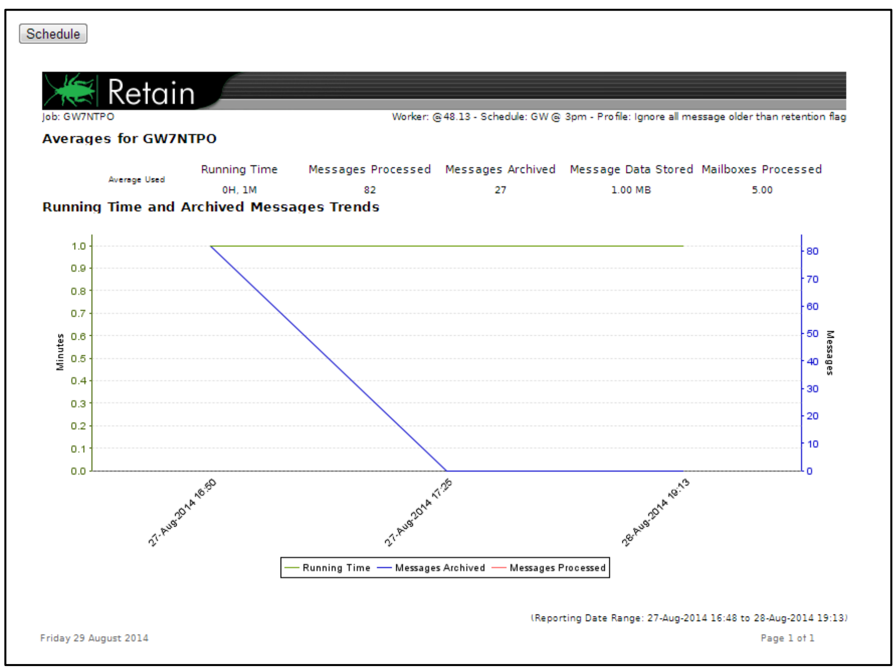
To Schedule the report, select the ‘Schedule’ button from the top of the report to keep the settings.

Job Run Averages

The job run averages report takes the performance of any selected particular job and creates a chart to display the trends. The effectiveness, overall load, and performance can be rapidly displayed. The Job Run Averages report requires a single job to be selected. The 'Jobs' selection window has columns which are sortable for convenience.



Once the date period has been configured, select 'Generate' to create the report.

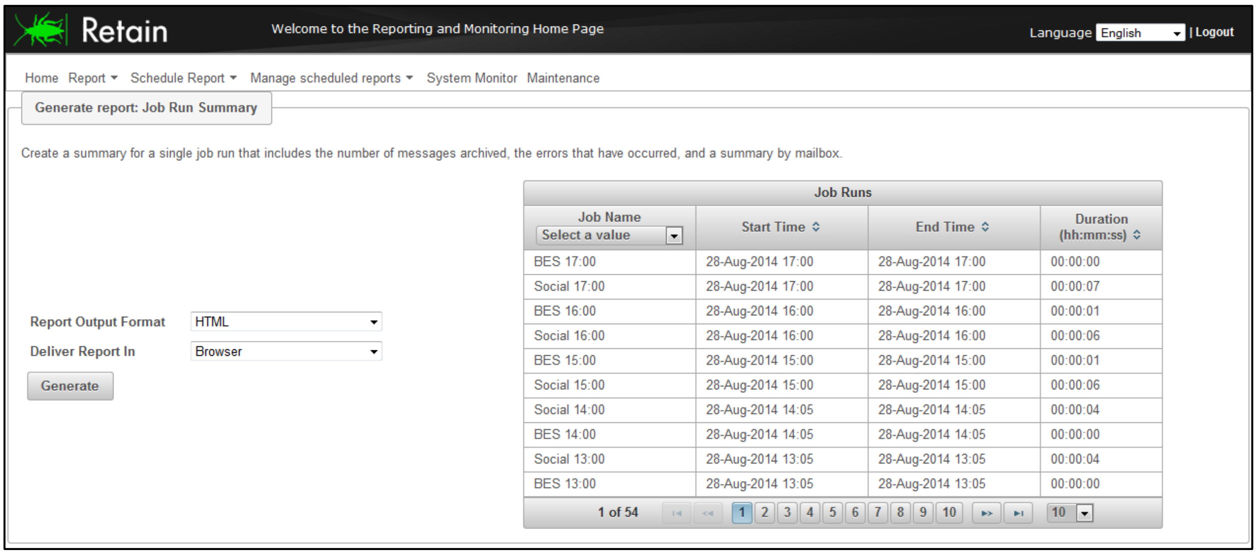


Performance trends are immediately apparent as run time is compared with message counts over a time period. The averages used to create the graph are listed above the graph, as well as a legend below.

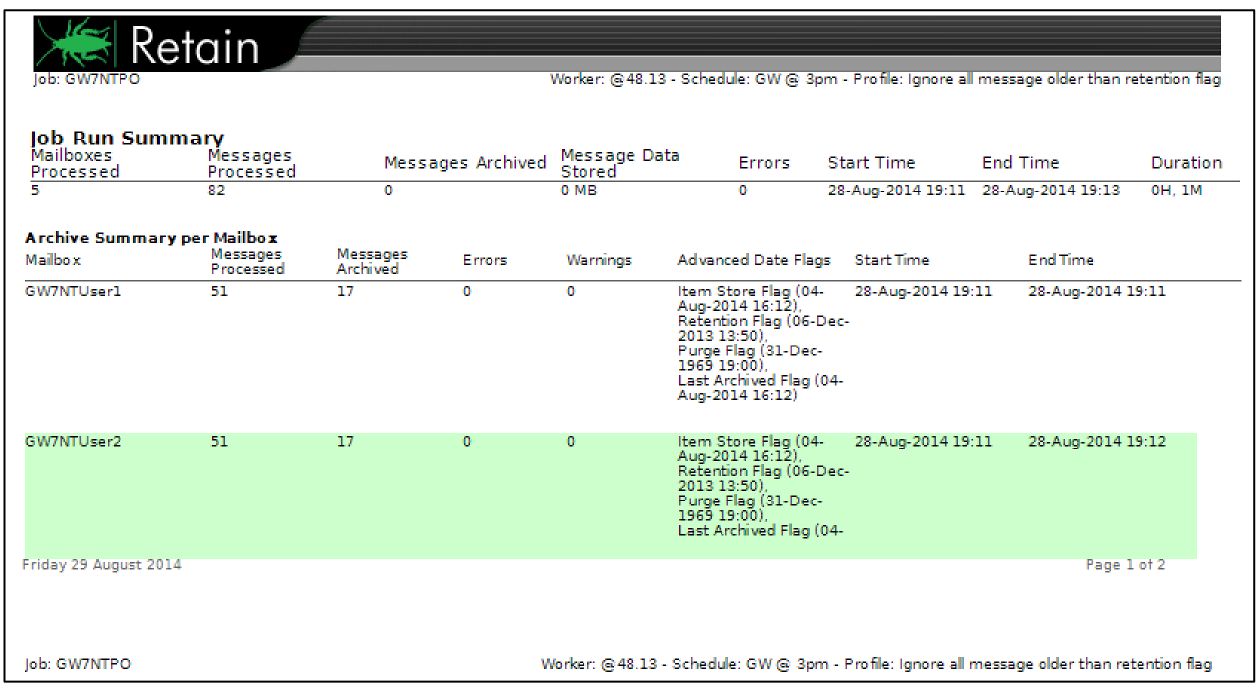
As with the rest of the reports which exist in the 'Schedule Report' interface, to schedule this report with the settings which created it, select the 'Schedule' button from the top of the report to use the same settings and be linked directly to the 'Schedule Reports' interface.

Job Run Summary

The Job Run Summary report gives a complete report of the performance of a single job. Whereas the Job Run Averages report charts raw performance averages, the Job Run Summary report goes into greater detail on the total number of archived messages, the errors, and mailbox summary for a single instance of a job.



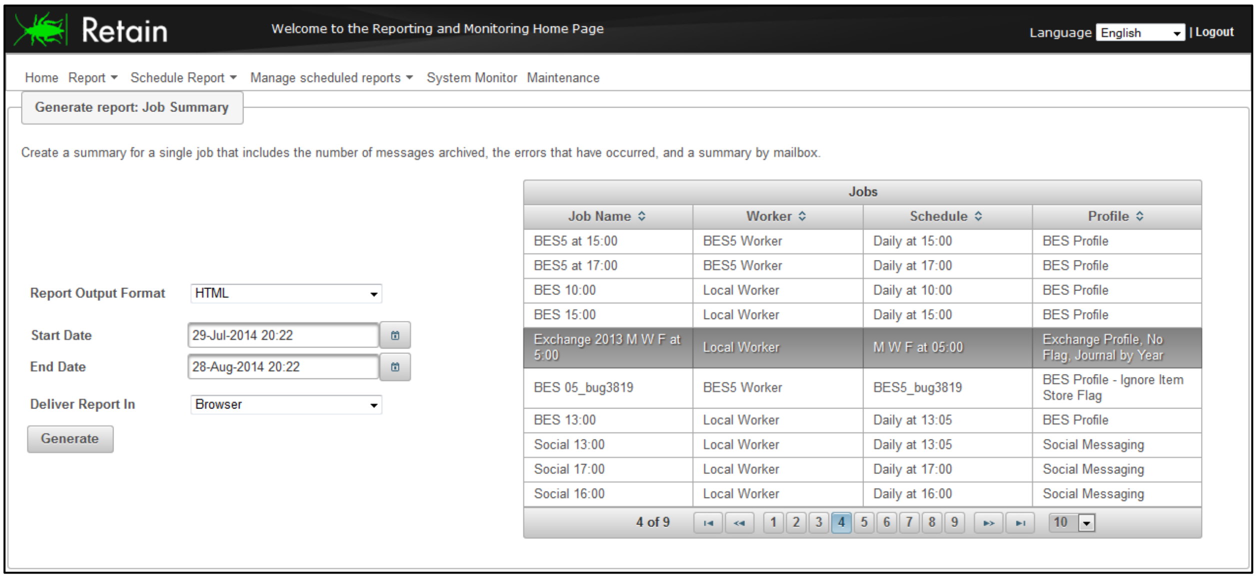
Select the desired single instance of a job and then select 'Generate'.



The summary displays the total mailboxes, messages, data store, errors, and running time of the job. Afterwards, this information is broken down by each mailbox the job covers. Due to a single instance needing to be selected, this job cannot be scheduled.

Job Summary

The Job Summary report is much the same to the Job Run Summary report, except that this report covers the entire history of a job and not just a single run. To run the report, select the desired job and any time period, if desired, the desired output and delivery method, and click ‘Generate’.



The report generated displays the number of mailboxes that the job processes, the total messages the job has processed, how many messages are actually archived, the message data stored, the total errors encountered, when the job first started, and the total time the job has been active.

Immediately below the initial information, a pie chart displays the amount of messages actually archived in comparison to the number of messages the job processed.

Finally, below the pie chart is a summary, by individual mailbox, of job actions. Each mailbox is displayed with the pertinent information, including the messages archived, messages processed, critical errors, a record of the advancement of message store flags, and the duration of the job in that mailbox.

To schedule this job with the settings desired, select the ‘Schedule’ button from the top of the report. All settings used to create the report will automatically be copied into the ‘Schedule Report’ interface.

Schedule

Retain

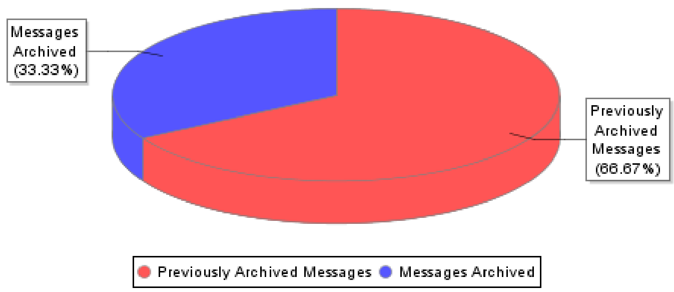
Job: GW7NTPO

Worker: @48.13 - Schedule: GW @ 3pm - Profile: Ignore all message older than retention flag

Job Summary

Mailboxes Processed	Messages Processed	Messages Archived	Message Data Stored	Errors	Start Time	End Time	Duration
15	246	82	3	0	27-Aug-2014 16:48	28-Aug-2014 19:13	26H, 24M

Archive Ratio of Processed Messages



Archive Summary per Mailbox

Mailbox	Messages Processed	Messages Archived	Critical Errors	Warnings	Advanced Date Flags	Start Time	End Time

Friday 29 August 2014 Page 1 of 3

Job: GW7NTPO

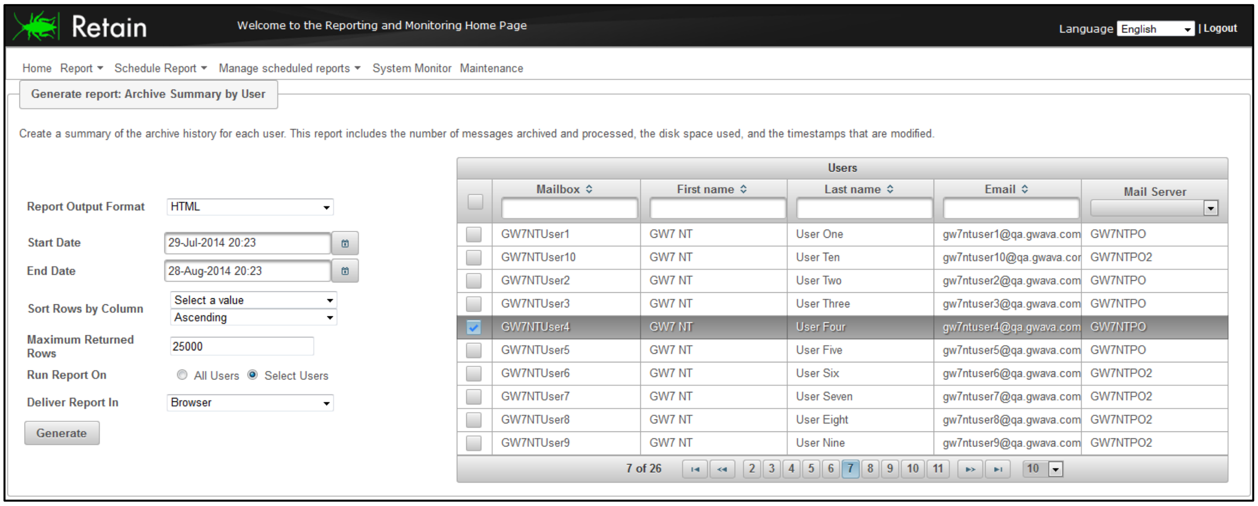
Worker: @48.13 - Schedule: GW @ 3pm - Profile: Ignore all message older than retention flag

Mailbox	Messages Processed	Messages Archived	Critical Errors	Warnings	Advanced Date Flags	Start Time	End Time
GW7NTUser1	51	17	0	0	Item Store Flag (04-Aug-2014 16:12), Retention Flag (06-Dec-2013 13:50), Purge Flag (31-Dec-1969 19:00), Last Archived Flag (04-Aug-2014 16:12)	27-Aug-2014 16:48	28-Aug-2014 19:11
GW7NTUser2	51	17	0	0	Item Store Flag (04-Aug-2014 16:12),	27-Aug-2014 16:49	28-Aug-2014 19:12

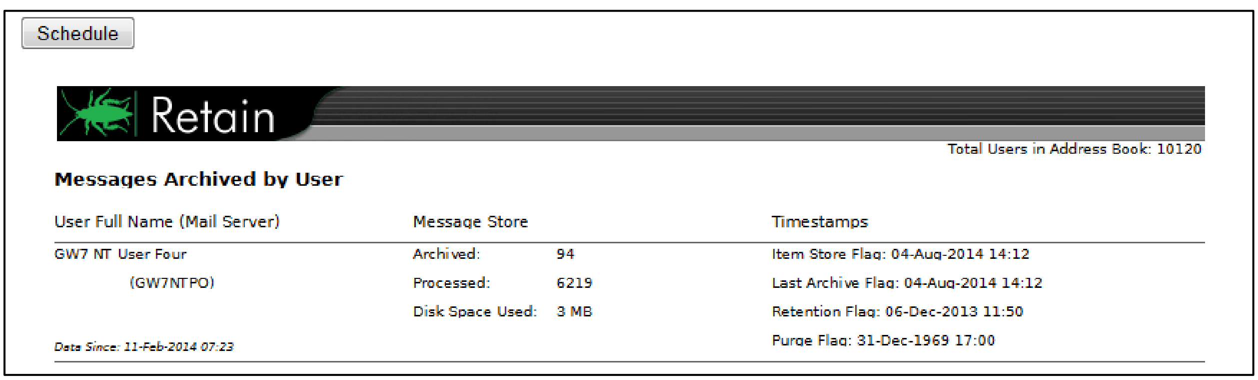
Archive Summary by User

The Archive Summary by User report creates a summary of all users', or a specific user's, archive history. The summary includes all pertinent information for each mailbox's archive. To run the report, either all or one mailbox must be selected. If all mailboxes are selected, the maximum returned rows may be a very important setting to keep the report from becoming immense.

While the report cannot be sorted after it is generated, it may be sorted at generation through the 'Sort Rows by Column' feature. The columns may be sorted by either descending or ascending order. Select 'Generate' to create the report.



The report displays the total information for every mailbox selected; User name, the time stamps and their advanced dates, and the message store for the associated user.

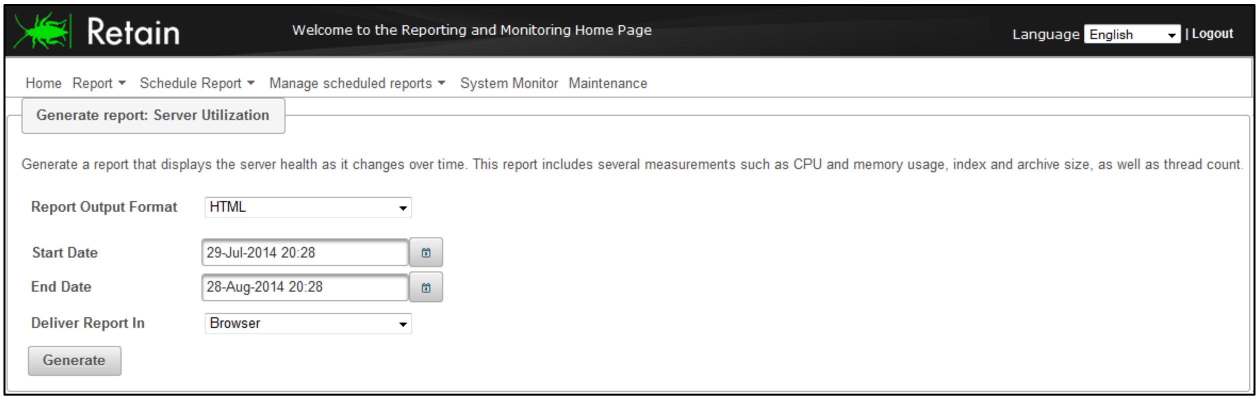


The most valuable part of this report, and what will make this report a staple for administrators, is the ability to monitor and get a concise report for the disk space used for each individual user along with the messages processed and stored.

If the report is to be scheduled, select the 'schedule' button from the top of the report to use the same settings which created the report.

Server Utilization

The Server Utilization report is a direct report on the load that the Retain Server is under. The only option is to limit the date range for which the report is active. Select the report period and then select 'Generate' to produce the report.



The Server utilization report details the memory, CPU utilization, Archive size, Thread usage, Index size, heap memory, and non-heap memory usage all in quick to digest charts.

To schedule the report, select the 'Schedule' button from the top of the report to utilize the same settings.

Schedule

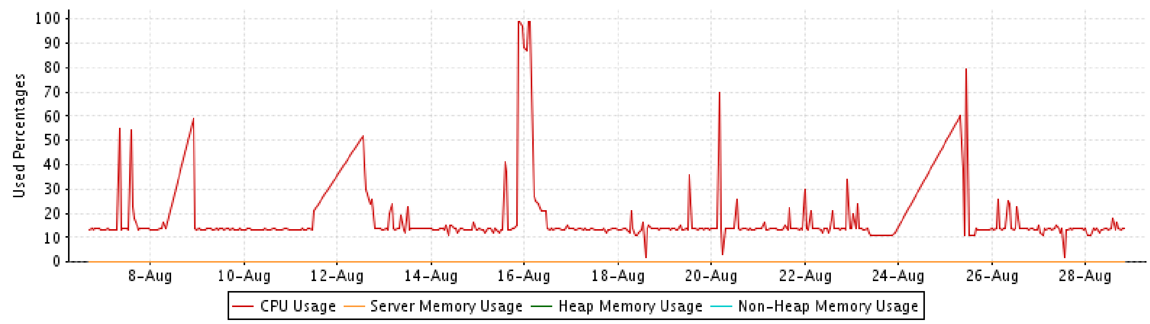
Retain

8 server(s) known

Server Usage Report for 127.0.0.1

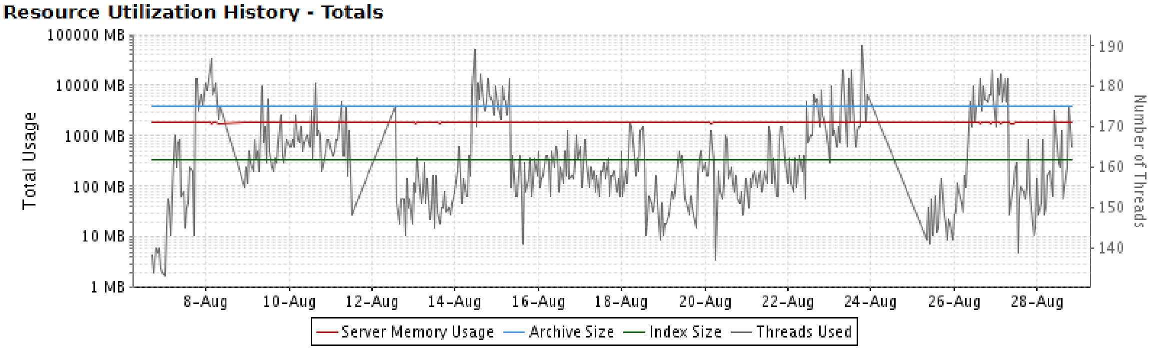
	Average Used	Minimum Used	Maximum Used	Total Available
CPU Usage	16.85 %	0.00 %	99.00 %	Not Applicable
Server Memory	1,821.63 MB	1,730.23 MB	1,843.12 MB	1,894.91 MB
JVM Heap Memory	365.55 MB	87.65 MB	872.39 MB	1,979.75 MB
JVM Non-Heap Memory	184.63 MB	128.73 MB	236.10 MB	560.00 MB
Index Size	0.33 GB	0.32 GB	0.34 GB	Not Applicable
Archive Size	3.79 GB	3.50 GB	3.89 GB	Not Applicable
Threads	161	131	197	Not Applicable

Resource Utilization History - Percentages



Thursday 28 August 2014 Page 1 of 2

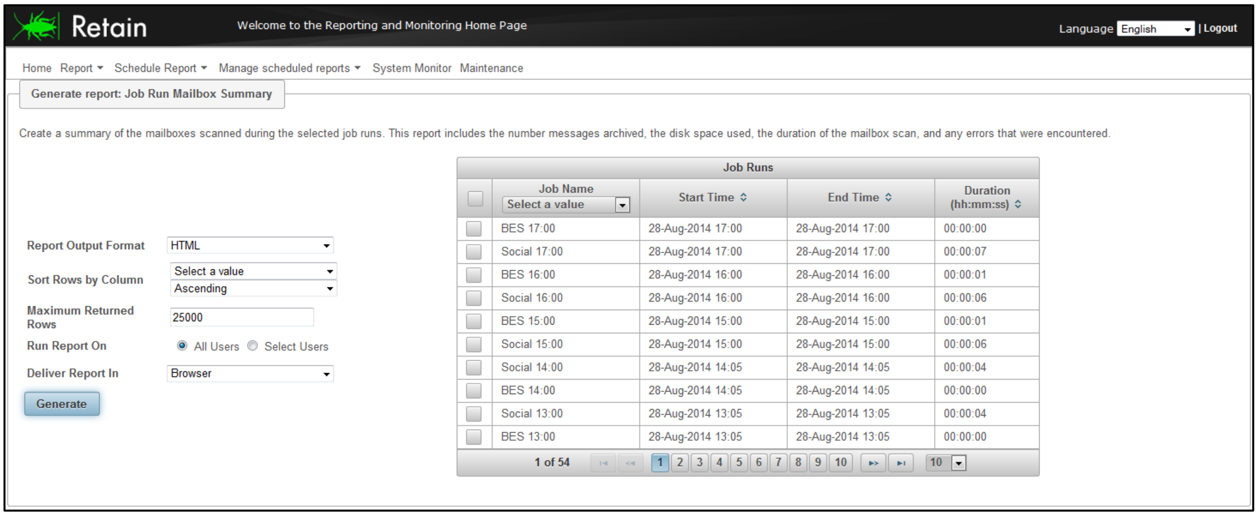
Resource Utilization History - Totals



(Reporting Date Range: 06-Aug-2014 17:20 to 28-Aug-2014 20:18)

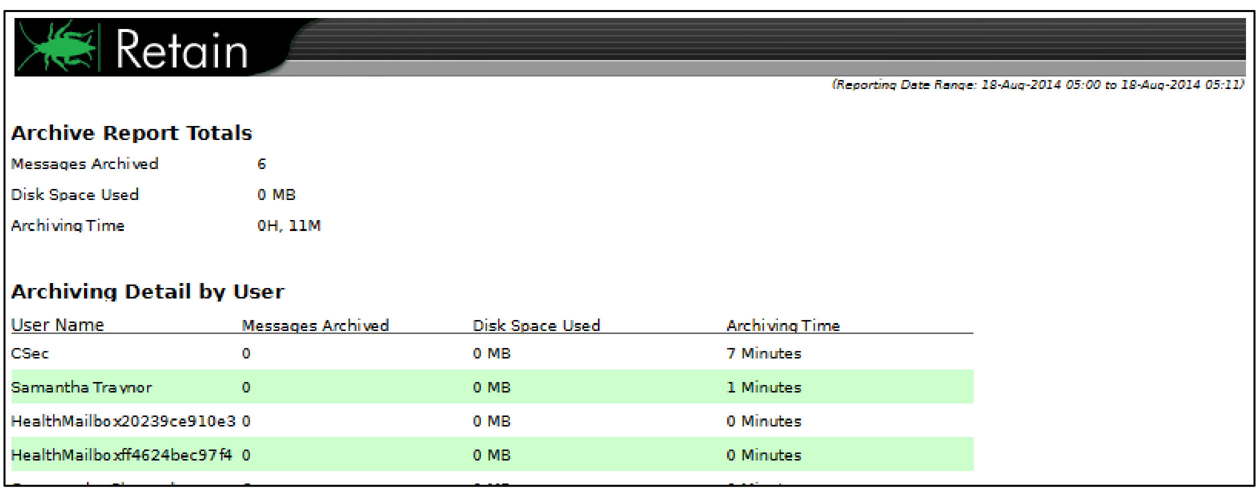
Job Run Mailbox Summary

The Job Run Mailbox Summary is much like the Job run Summary except it is dedicated to specific mailboxes and specific jobs. This job requires both a job, and a user or users to be selected.



Select the desired job and either all users, or only select users. If desired, the columns may be sorted by a selected value through the 'Sort Rows by Column' drop-down menu. Once set as desired, select the 'Generate' button.

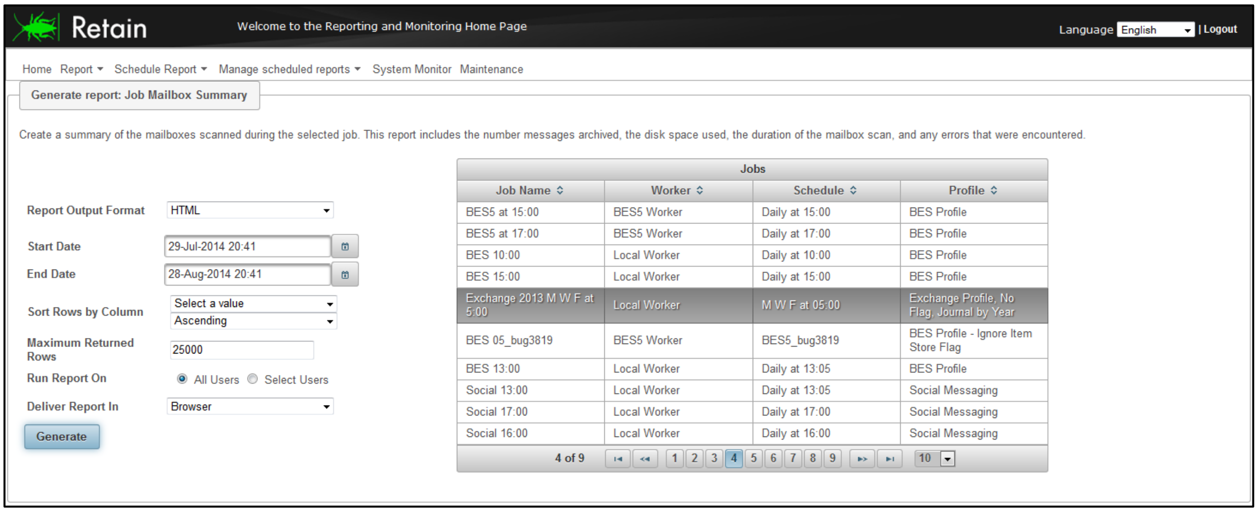
The report shows the details for the selected job and mailboxes. The user name, messages archived, disk space used, and archiving time is all displayed for each mailbox as well as for the total job.



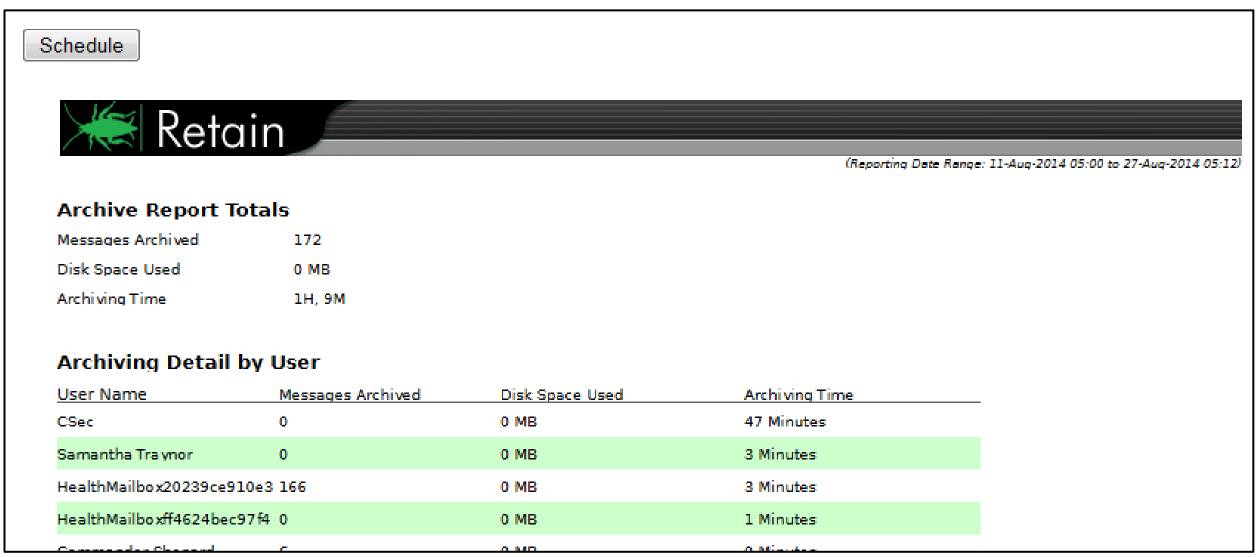
This report cannot be scheduled.

Job Mailbox Summary

The Job Mailbox Summary report displays the number of messages archived, the disk space used, and the time the job took, separated by separate mailboxes. This report may be restricted to a date range, a limited amount of rows, and may be performed on all, or only select users. This report may also sort the data according to a selected column, in either ascending or descending value.



Select the 'Generate' button to create the report.

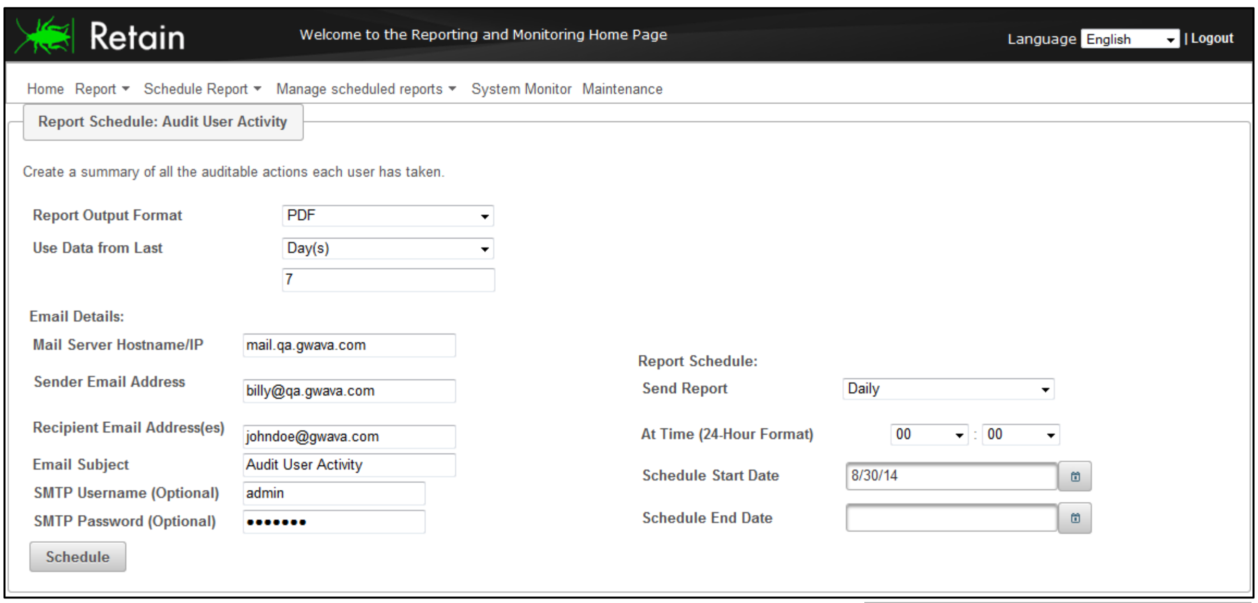


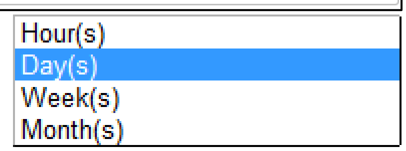
To create a scheduled report with the same settings as used to generate the report, select the 'Schedule' button from the top of the report.

Schedule Report

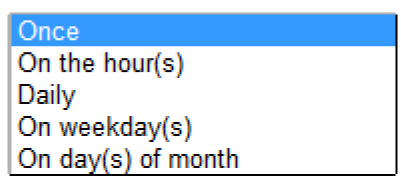
Scheduling reports is accomplished through the Schedule Report interface. Every report which can be scheduled is also available as an instant report with a 'schedule report' button located at the top of the HTML report. Because these instant reports are easier to fine-tune, it is recommended to first configure a scheduled report through the 'Report' interface first, to allow immediate fine tuning and viewing of the results. Once achieved, selecting the 'Schedule' button on the report will take all settings used to generate that report and input them into the schedule Report interface. To schedule any report, a destination email address, SMTP information, and a set schedule are required.

Scheduled reports differ from normal reports in that, due to the scheduled nature, they must be given a time to generate the report and be given an email address to deliver the report to. Reports are delivered as an attachment in an email sent to a specified user. As such, scheduled reports are only offered in PDF and XLS formats.





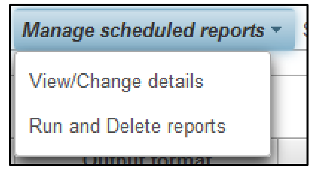
Reports which have a time frame attached to them as part of the criteria will have a floating time window which they may take information from. The configuration allows reports to the use data created in the past number of hours, days, weeks, or months. The number may be set by the user.



Also, the frequency of the report may be configured to be either a single instance or a reoccurring report. The frequency allows for hourly, multiple times on specified hours every day, daily, weekly or on any specified number of days in the week, or at any specified day or days in the month.

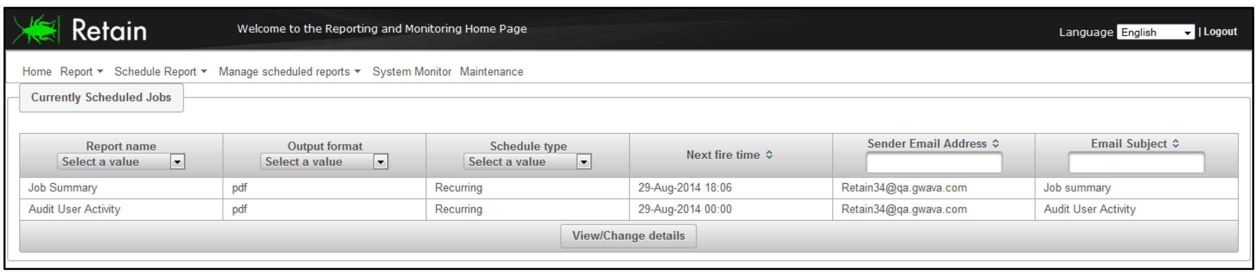
In addition, a scheduled start and end date allow the administrator to control exactly when the start and stop dates for any specific report can be. The end date is not required, but is optional.

Manage Scheduled Reports



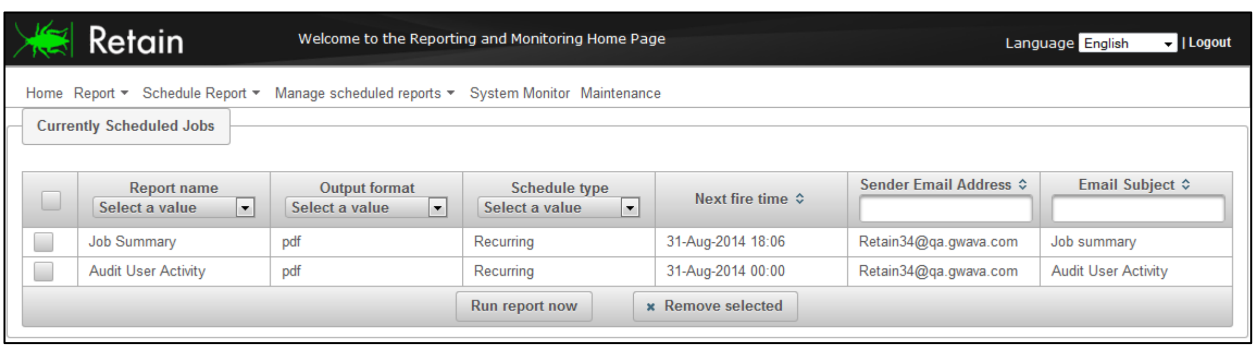
Once reports have been scheduled, it may be necessary to either cancel or modify the frequency or settings of the report. The Manage Scheduled Reports interface allows jobs to be immediately run, modified, or removed. As with all other columns in the R&M interface, the columns are sortable and even searchable to allow quick access to any desired Report through any of the scheduled criteria. For instance, a user which doesn't want to receive a report anymore, but doesn't know what report is being delivered to their email, only needs to know the email subject, or the next delivery time, to immediately identify the report. Unique sender addresses or subjects will readily allow any report to be identified.

To modify or view a report's settings select the 'View/Change details' window.



Once the desired report has been located, select the report and then select the 'View/Change details' button at the bottom to be taken to the Report's configuration. Make any desired changes and select the 'Update' button at the bottom to save the changes.

To remove or immediately run a scheduled report, select the 'Run and Delete reports' window.



Any report or reports may be immediately run or removed from the system through this window. All scheduled reports will be displayed. A select all/none box is at the top left of the table, and allows for a quick selection or clearing of all previous selections which have been made.

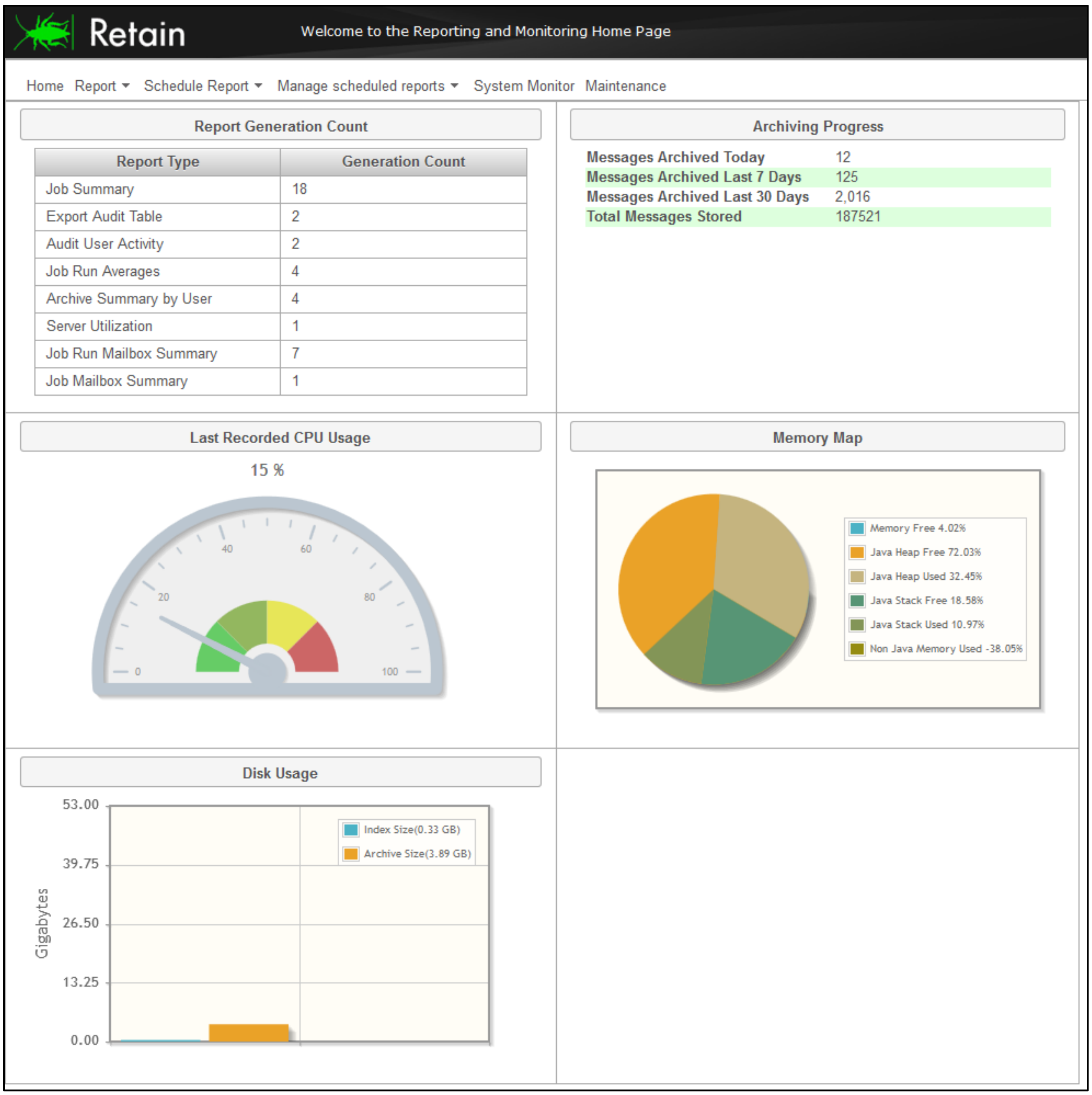
To run a report or reports, select the desired report by clicking on the associated checkbox and then select the 'Run report now' button at the bottom. The report will be immediately triggered, and emailed to the specified recipient.

To remove a report or reports, select the desired report(s) by placing a check in the associated checkbox. Once the reports are selected, click the 'Remove selected' button at the bottom of the table.

System Monitor

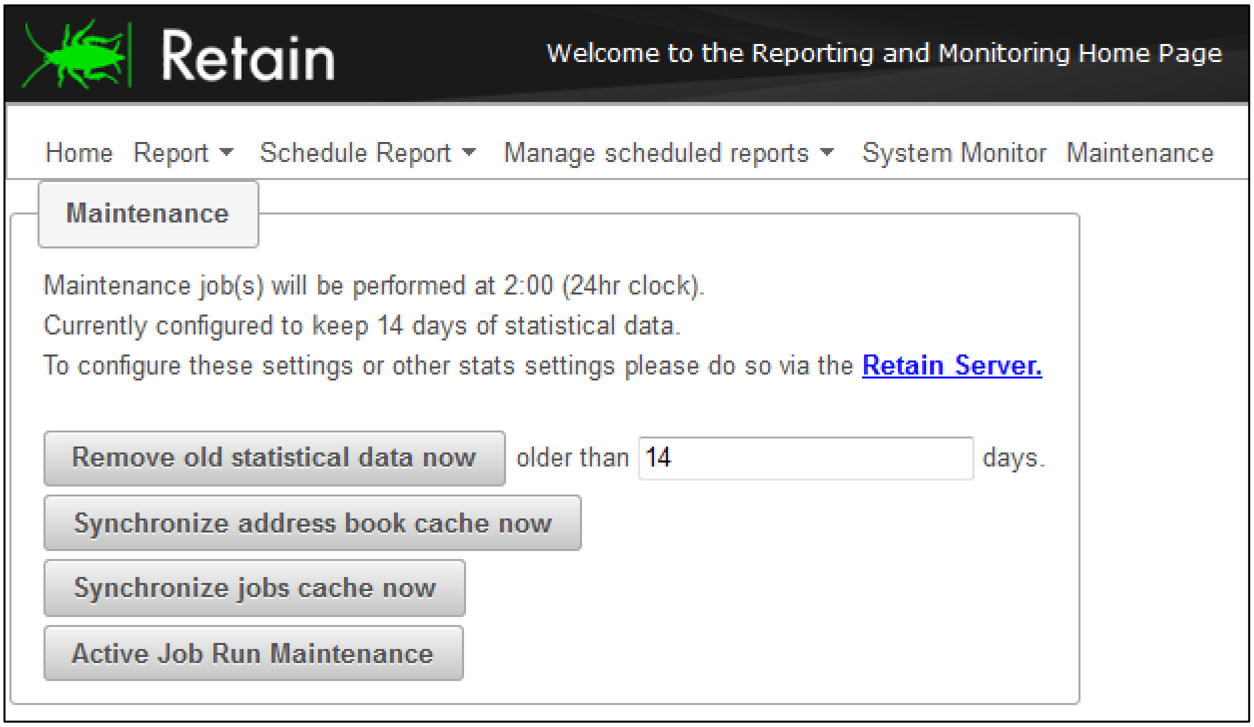
The System Monitor page is a quick, graphed page which displays the essential stats of the Retain Server system. The R&M module statistics are displayed, with how many reports have been created and of what type. The basic archive progress is also displayed showing the daily, weekly, monthly, and total amount of messages which have been archived in the system.

The system CPU load, memory usage map, and Disk Usage are displayed. These numbers are for the actual host server, and not just the Retain system, with exception of the memory map, which has both. The Memory map is broken out to total system memory free and used, but also includes Java memory statistics – which will be Retain specific unless additional Java applications are running on the Retain Server. This page will not time-out or expire, to allow quick monitoring of the system.



Maintenance

The Maintenance page contains the basic maintenance for the R&M module. This is not maintenance for the entire Retain Server. Because the R&M module maintains individual statistics, it needs to be refreshed and purged at regular intervals. The defaults are shown.



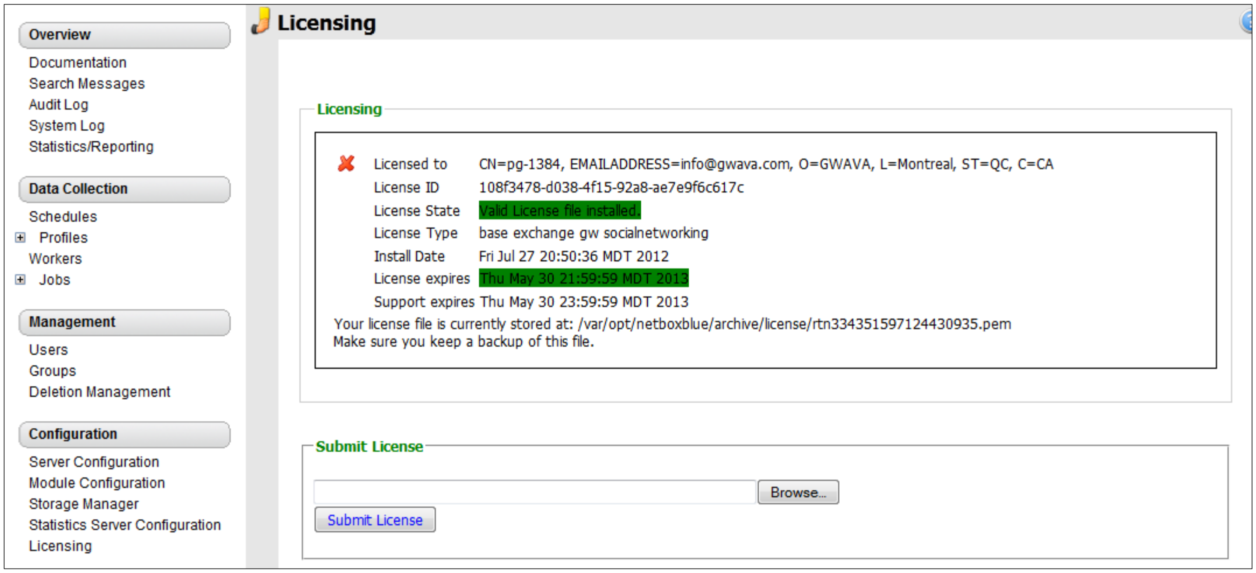
The R&M Module maintains a separate record of the address book and the job cache. The system automatically synchronizes this information with the Retain Server every 24 hours. Still, the different records may become out of sync. If a synchronize job is required before regular maintenance, a manual sync may be individually triggered.

By default, the statistics server only maintains a record of statistics for 14 days, and all data older than 14 days will be automatically expired and the data deleted. If the statistic data is required for longer or shorter, configure and save the setting.

It is not recommended to maintain statistical data older than 30 days.

Licensing

The Retain license is a file with a PEM extension which should be uploaded through this screen. To acquire a license, contact your GWAVA sales representative.



Without a license, Retain will function for 30 days for evaluation purposes.
After this period elapses, the following occurs.

- Users without the "Manage Servers" right are not allowed to log in at all.
- Users with the "Manage Servers" right are allowed access, but only to the Licensing Page.
- All jobs continue to be processed normally

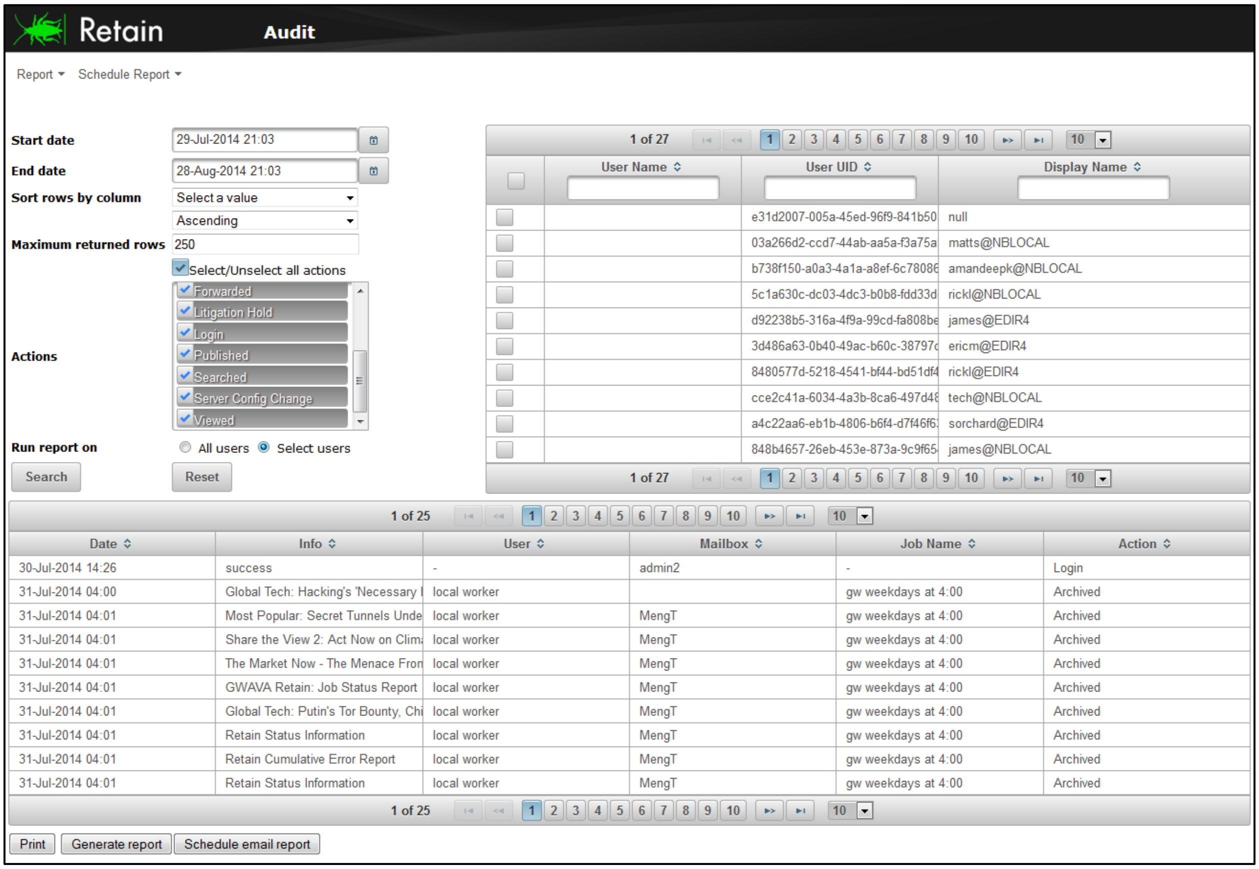
To submit your license, browse to your PEM file and click “Submit License”.

Logout and re-login to the server to see the license in effect.

Overview

Audit Log

All pertinent actions performed by users in Retain are logged and can be discovered and printed. If Reporting and Monitoring is installed, four buttons are added to the following page, as shown below.



- Accessing the audit log requires the "Access all audit logs" administrative right.
- Ordinary users cannot access their audit logs unless you grant the "View Personal Audit Log" right, in which case they can find the audit log on a per-message basis under the Properties tab.

To view actions, select the desired actions, one or all, a date range, and a user, one or all, and then select 'Search'. The results will be displayed in a table below. All columns in this table are sortable.

The results appear below. This may be printed by selecting the 'Print' button at the bottom. The print button will only print what is shown in the action table, not the criteria or the interface.

If you have rights, you may click on the Action link to open the message. An auditor does not automatically gain the rights to READ messages in mailboxes that are not assigned to them.

If the Reporting and Monitoring module is installed, the 'Report' and 'Schedule Report' menu options on the top bar, and the 'Generate Report' and 'Schedule email report' buttons along the bottom will appear. These buttons link to the R&M interface to extend R&M ability to generate and schedule reports based on the selected criteria. If the Generate report or Schedule email report buttons are pressed, the criteria used in the Audit window will be automatically propagated to the Reporting interface.

System Log

This option lets you read and parse through the latest system log file. The level of detail is controlled in system configuration.

The actual filename and path on the server is also listed. You may clear the view buffer at any time in case you want to monitor a particular operation for troubleshooting purposes.

Searching the Retain Archives

Now that there is data in your Retain archives, you will want to retrieve this information. This is the core of the information retrieval system in Retain. You search for what you want, the results appear and you can view, print, export, or forward the results. If the logged on user has at least one administrative right assigned, the user is brought to the administrative menus upon login, and must click on “Search Messages” to access the search interface.

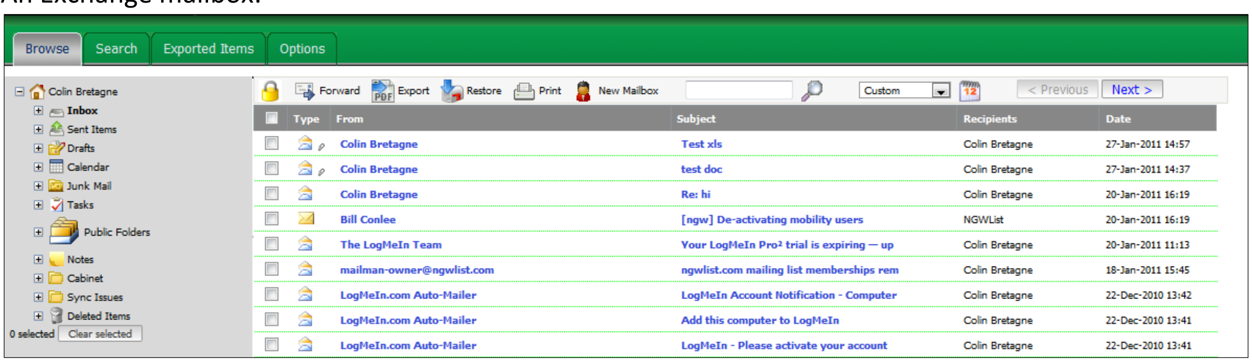
There are four tabs in the Search Interface:

- Browse- for casual browsing and filtering. You may only browse one mailbox at a time.
- Search- for in-depth search, possibly across many mailboxes.
- Exported Items- List of all export
- Tag Definitions- ONLY VISIBLE if the user has rights to Tag Definitions.
- Options- for changing user settings. Similar to settings in the User Admin.

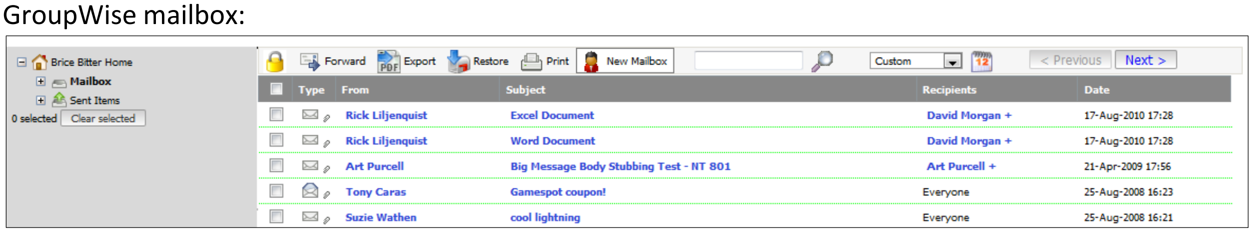
The browse screen shows you one mailbox at a time. The mailbox you’re viewing is listed at the top left and the folder structure is replicated as it is in the mail system. The view the screen displays is dependent on the source mail system for the selected or displayed mailbox. Accordingly, the icons and folder structure of different mailboxes will appear differently for a GroupWise account than it does for an Exchange account.

If you have the rights to access more than one mailbox in the mail system, (such as GroupWise proxy rights and the proxy option enabled in Retain), you will see the “New Mailbox” icon along the toolbar allowing you to switch between mailboxes you have access to. In addition, you may switch display languages using the drop-down language selector along the top.

An Exchange mailbox:



GroupWise mailbox:



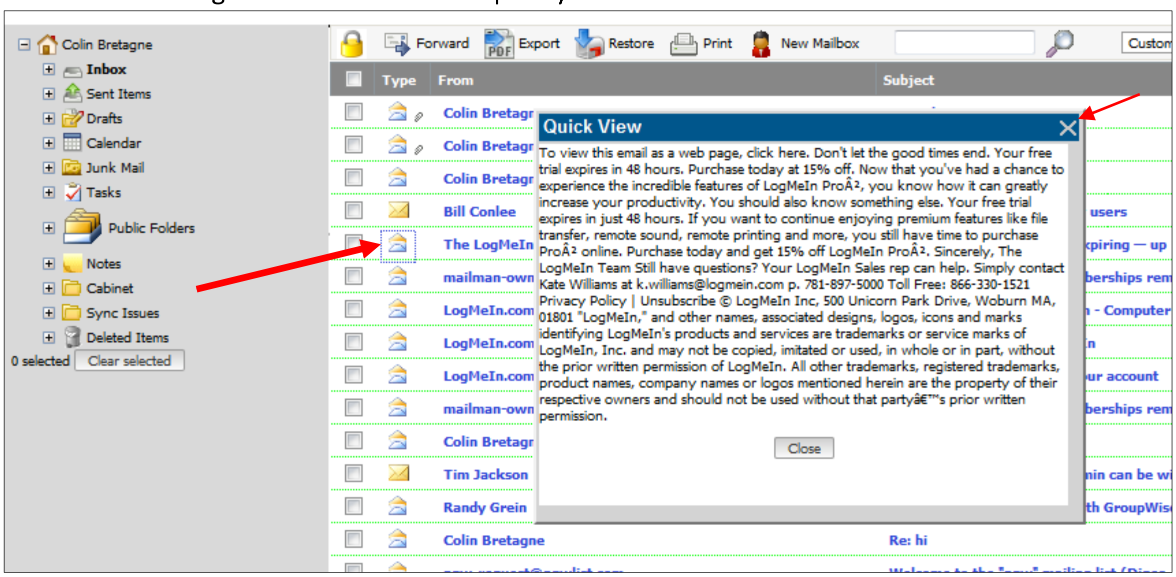
Social Messaging:

Cumulative Selections

In browse and search as you click on selections, these are preserved cumulatively from page to page or across searches, folders, etc. So you can forward, restore stub, PDF export from many places at once.

Quick View

The search messages interface allows to quickly view items.



Accessing the quick view is simple. Simply select the item icon in the 'Type' column, (mail envelope icon), to spawn the quick-view for that item. The quick view displays up to the first 2kb of text for that item in a small window.

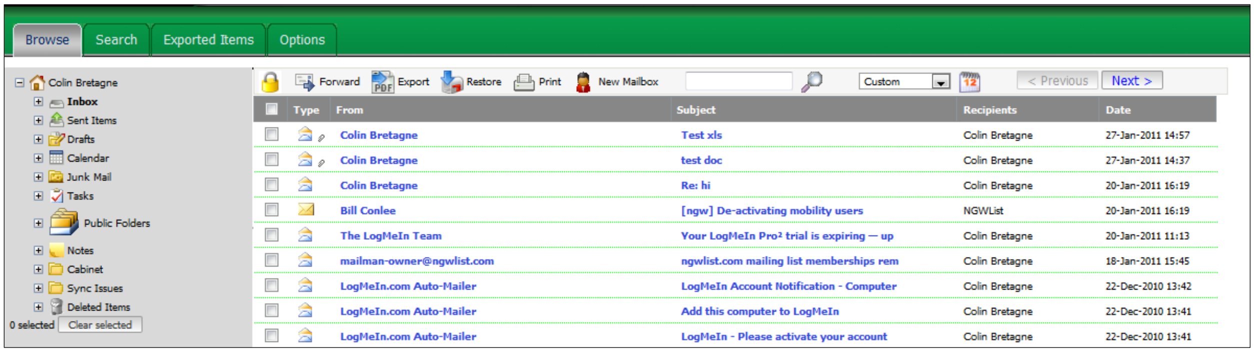
NOTE: Date Range Filter

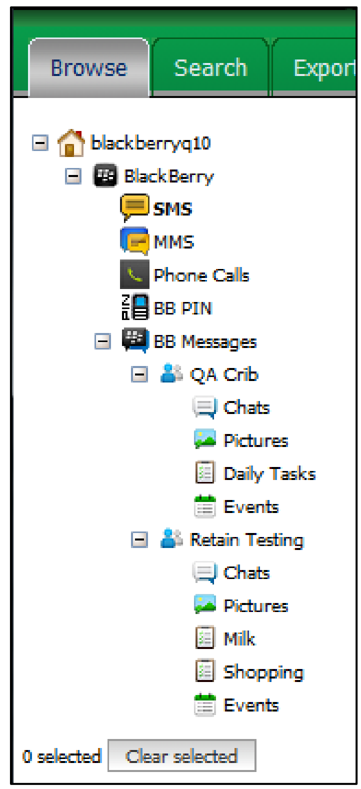
Please pay particular attention to the date range filter. Only messages that match the date range filter are displayed. If you don't see the results you expect, check the date range filter to be sure that the settings are correct. See Specifying a Date Range.

Using Online Help

Retain has context-sensitive help screens that appear in the left column when you click the help icon. ()

Browse





This is the default **Browse** screen.

The logged-in user's mailbox will be displayed by default along the top of the window. You may choose to browse through another mailbox if you wish (and if you have rights to do so).

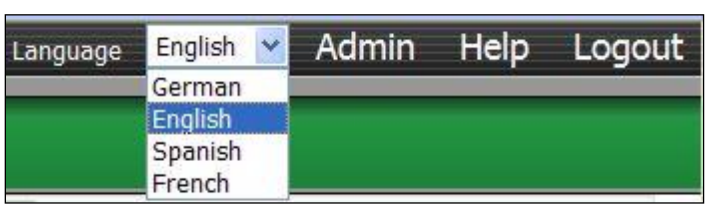
If the user's mailbox is empty, or the user has no specifically assigned mailbox, then the user will be prompted to select a mailbox to browse. Only mailboxes which the user has rights to, will be available.

Notice that the folder structure of the mailbox is reproduced at left. You can expand the folder list until there are no more sub folders.

You browse the folders in the current mailbox and when selected, their contents are displayed.

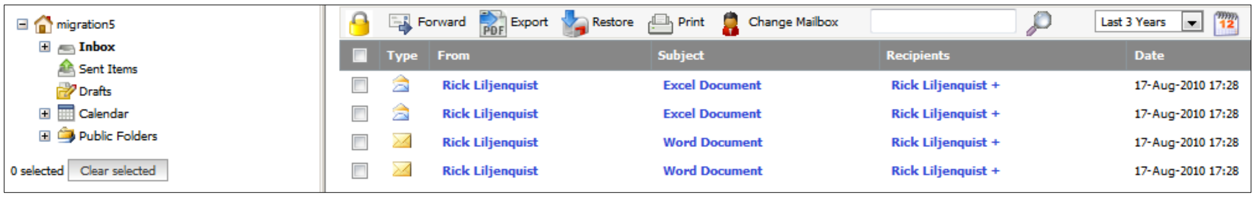
Language Selection

You may select what language the browse screen will use by selecting the drop-down language selector control and choosing your desired language. This selection applies to the search screen as well as the administration interface.

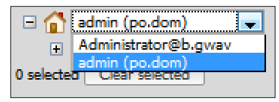


Merged Mailboxes

If a mailbox has been merged with its migrated counterpart or any other specified mailbox in Exchange, then the user will have the option to switch mailboxes with a drop-down selection box.



Mail from both systems will be viewable and manageable in the same window without having to logout or switch mailboxes.



Browsing Tools (Widgets)

Retain will display various options for the user. The specific options displayed depend upon the user's rights, if a user has not been granted the rights to a particular tool, that tool will not be present in their Search Messages interface. The rights are found in the Retain Server Management section, on the Users page. The full range of options includes (From Left to Right):

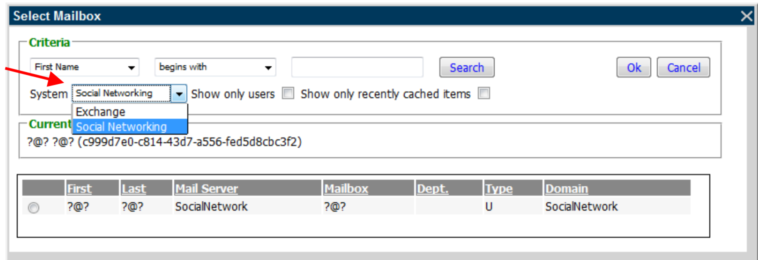
- LITIGATION HOLD — Applies or removes the litigation hold, banning removal from archive. Litigation hold prohibits the deletion manager and jobs from removing applied and marked messages.
- CONFIDENTIAL — Toggles the confidential state. Confidential items are only visible with Admin rights, or to those specified by the user under the **Options|Confidential Exceptions** tab.
- TAG DEFINITIONS — Apply or remove tags to messages. ONLY visible with rights.
- DELETE — The Delete option is ONLY visible for users with rights to delete data.
- FORWARD — forward selected items by e-mail.
- PDF EXPORT — opens the PDF export window to create a PDF of the selected items to be emailed to a specified mailbox
- RESTORE — Restores messages to the Mail system. See section for details.
- PRINT — prints a list of selected items.
- NEW MAILBOX — select a new mailbox to view.
- QUICK SEARCH — search the current folder for text in “from”, “to”, “subject” or body.
- DATE SELECTOR — select a custom date range. Retain will show items within this range. The date filter selection is saved automatically whenever it is changed in the browse and search windows and persists between logged-in sessions. Users should take care that the date range sufficiently covers the time range of interest.
- PREVIOUS/NEXT — move to the next or previous page of items.

Browse Window Defaults

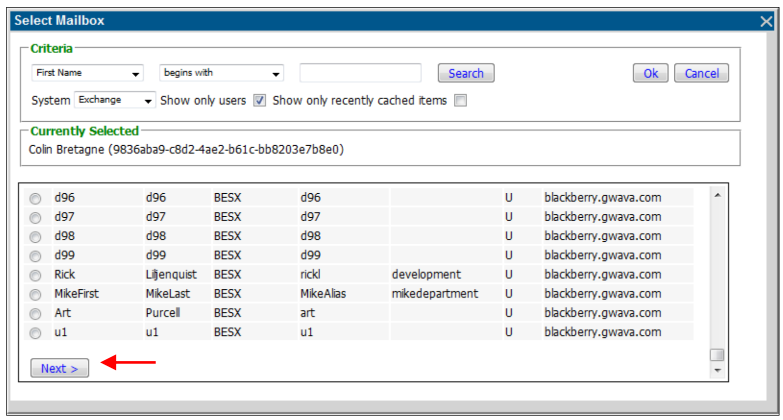
- Retain remembers what the last browsed mailbox was.
- Non administrators go right to their mailbox when they log in.
- Administrators get a prompt to select the mailbox they want to view.

New Mailbox

If you click “Change Mailbox” (which is available if you have access to at least one other mailbox in the system), you will see the mailbox selector screen pop up. Select which mailbox you want to see by clicking on its radio button and clicking OK. This is just like the [mailbox selector used in the user rights administration section.]()



(If Retain for Social Messaging is set to anonymous user, all Social Messaging data will be contained under the single user ‘?@?’, and separate user names and pertinent information is contained in the ‘from’ dialog. Otherwise, individual user accounts will be displayed.)



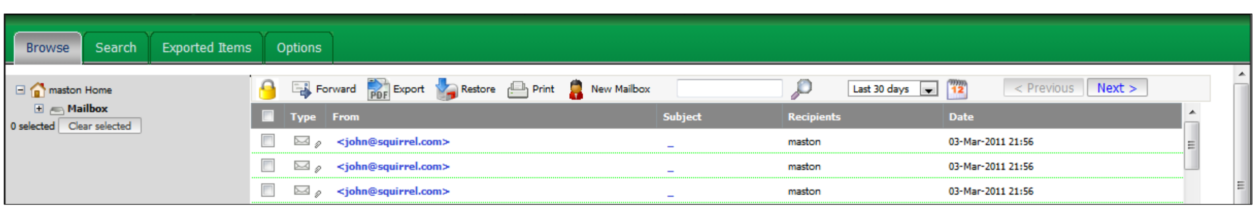
When selecting a single mailbox, the source of the mailbox must be selected as mailboxes from different systems may have the same user name or criteria. Select which mail system the desired user belongs to, specify any further criteria, or leave the criteria blank to display all possible mailboxes from that system.

If the search results are extensive, the system will have a ‘Next’ or ‘Previous’ button at the bottom of the search results window, which displays the next set of results.

Refine search parameters to reach a manageable search result.

In Retain, you can only browse one mailbox at a time. To search multiple mailboxes simultaneously, use the search function.

After selecting a mailbox, click ‘Ok’ to load that mailbox into the viewer.



Toolbar Options

Specifying a Date Range

You can narrow the scope of your browse by entering a date range. This is what it looks like.

Litigation Hold

See the Litigation Hold section later in the document.

Add / Remove Tag Definitions

See the Tag Definitions section later in the document.

Delete

The user delete option allows for the removal of data from personal archives. This option will not be displayed unless the user has been granted the delete right or rights in the administration console. The Delete right is not a default right, it must be specifically added to users or groups. Messages or data marked to be deleted will not necessarily be immediately removed, but will be queued for deletion. The actual item removal will depend on server availability and the amount of items queued for deletion.

Forwarding a Message

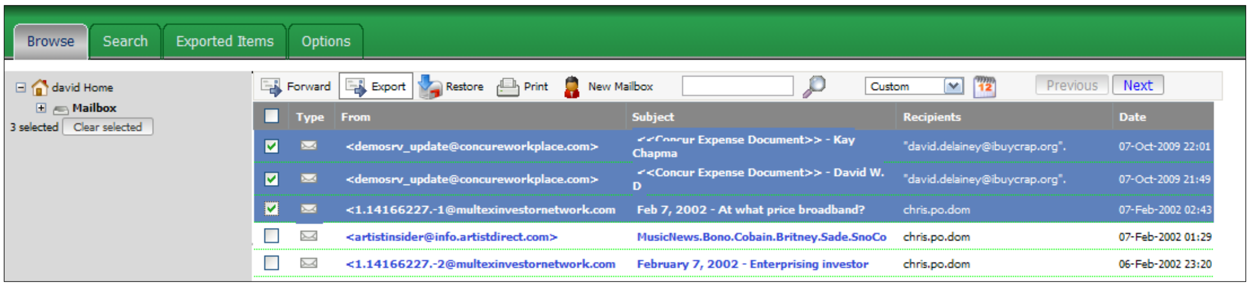
In the main browser window, you can select a message by checking its checkbox and the click "Forward". You will see this dialog:

Enter the recipients (where you want the message(s) to be forwarded), separated by commas. Enter a comment if desired and click "**Forward"**. Retain will send the message(s) via SMTP.

PDF Export

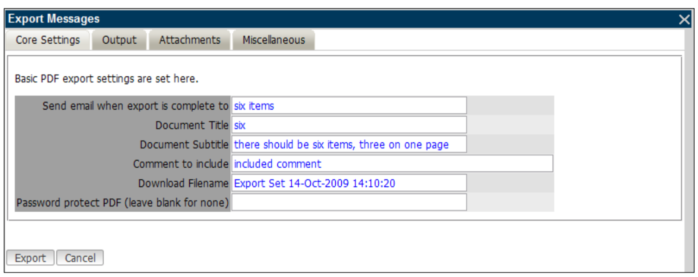
PDF Export is a new function which allows users, (with appropriate rights), to export single or multiple items into a PDF file. This PDF can be named and defined by the user exporting the document. Items will appear as navigable files in the PDF. The default view provides a list on top of the PDF viewer which works as a table of contents to provide access to the exported archive.

If you have rights to do so (new user right), can export browse or search results to PDF.
Select the desired items and then select the "Export" button.

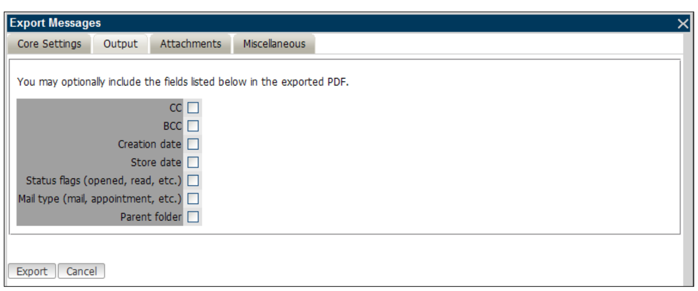


Fill out the various options as desired.

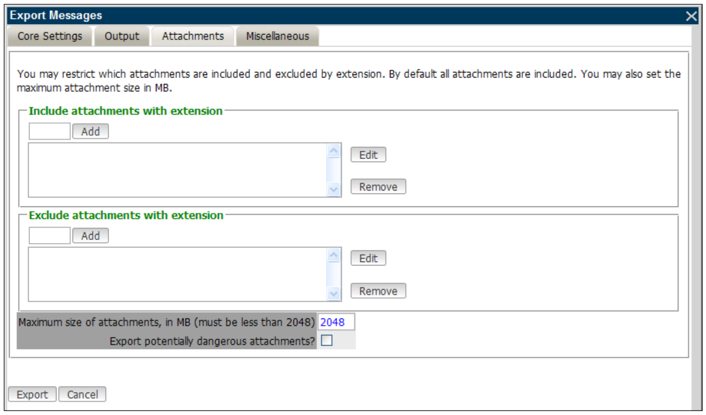
The different options include the file information.



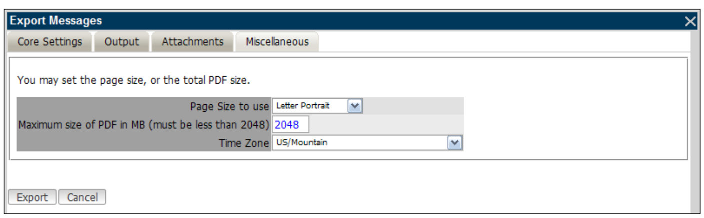
The File output and included fields can be edited.



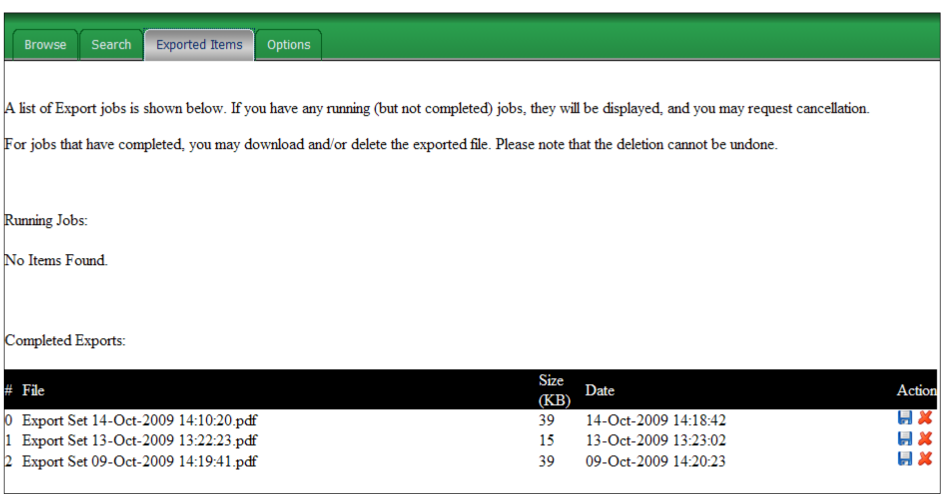
Any attachments to the email sent to the defined recipient.



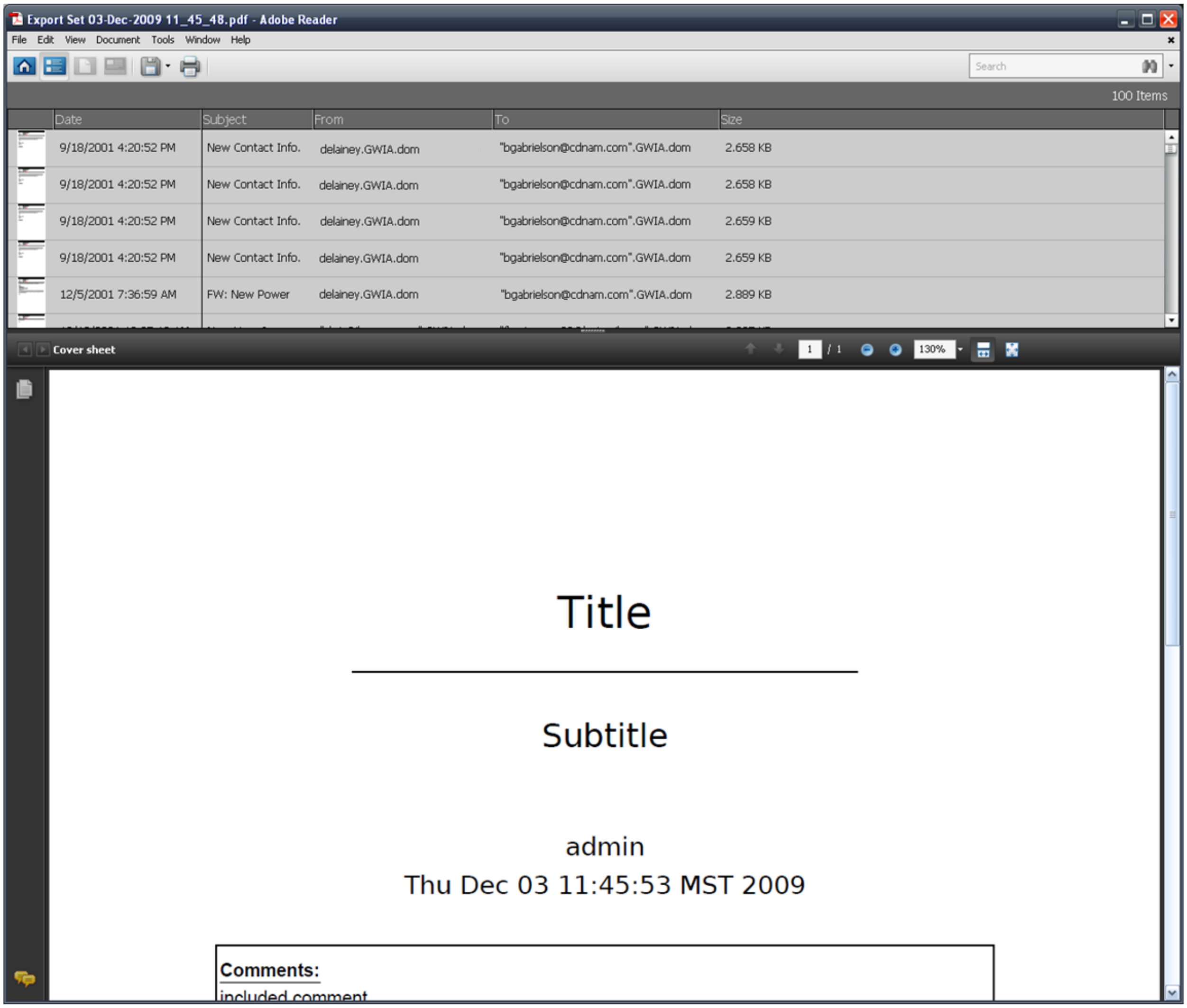
…And finally, any restrictions to size or time zone for the PDF. If the archive size does not exceed the maximum size, then the archive will be contained in one file. If larger, the archive will be exported into multiple PDFs will be created according to the maximum limit, until the archive export is complete. Time zone information will be used for formatting any time and date information in email headers. The time written to the cover sheet and date column in the PDF table of contents is written according to the time zone of the Retain Server.



When finished, select 'Export'. Depending on the size of the PDF export list, the export may take some time. The Export will notify via email when it is complete, if a notification address was provided. Currently running export jobs are also listed under the 'Exported Items' tab.
Once the Export has completed, the finished PDF is available under the 'Exported Items' tab. Locate the appropriate export list and select the disk icon to download the finished PDF.



The finished PDF is structured with an email or item list on top as a working table of contents, and the selected item is displayed below. The title, subtitle, and comments are listed on the title page, as shown.

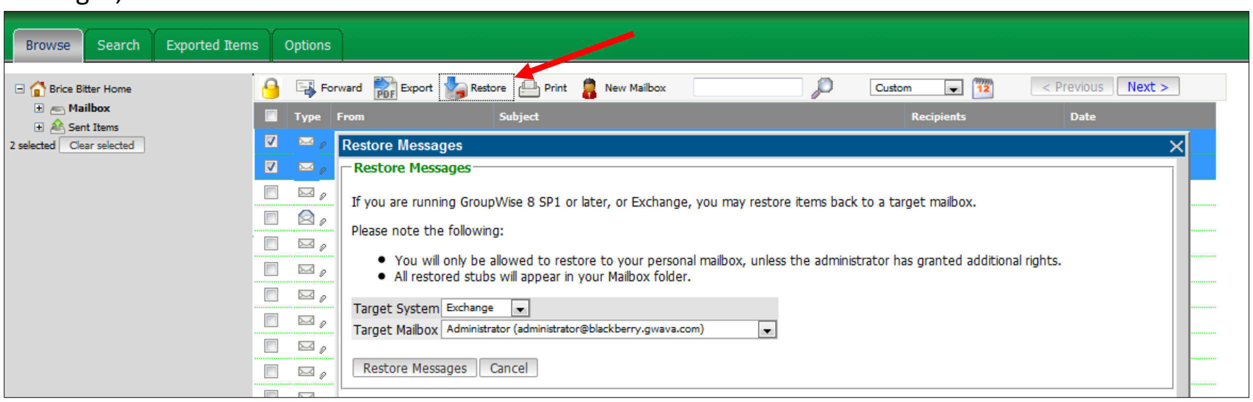


Restore

Retain can restore messages to target mailboxes in the mail system, for those users who have the appropriate rights to restore messages. If a user has the rights to restore messages their user interface will have the 'Restore' button visible on their toolbar. Restoring messages **requires** GroupWise 8, or Exchange.

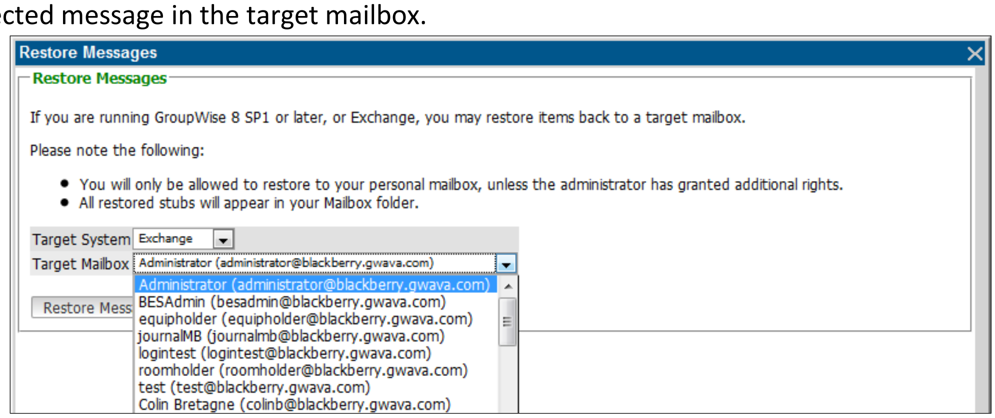
The action that the restore function performs is dependent on what platform the messages are to be restored to. For GroupWise, when the restore function is called, the selected GroupWise message(s) will have a stub restored to the mail system. Because the stub connects to and references the full item in the Retain archive, this function is effectively a 'full restore' of the message or messages. If message(s) are restored to Exchange, a full copy of the entire message with attachments is restored to the mail system. GroupWise messages may be restored to either Exchange or GroupWise.

To restore a message or messages, log into the Retain archive, locate and select the desired message, or messages, and click on the 'Restore' button.

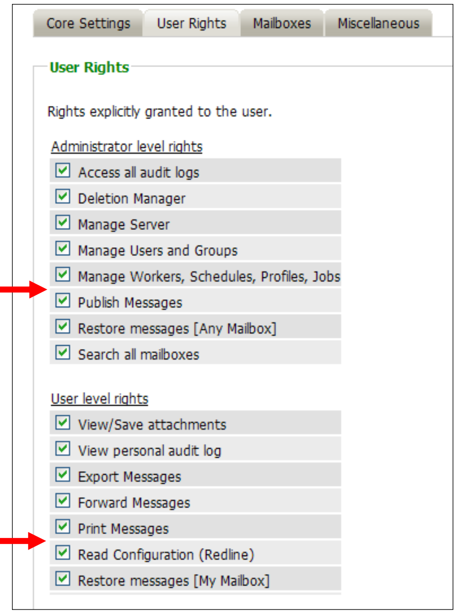


Select the desired target mail system for the restored messages. (This is usually the source mail system, though GroupWise messages may also be restored to the Exchange system.)

After the 'Restore' option has been selected, and if the user has rights to restore to any mailbox, the target mailbox must be specified, otherwise, only the user's mailbox will be available. When the 'Restore Messages' button is selected, Retain connects to the mail system and places a stub or the entire selected message in the target mailbox.



The Users Right that is required to use the Restore feature is called "Restore Messages". Administrator level right allows users to restore messages to any mailbox, including mailboxes which did not have the message before.
Restoring a message which currently exists in the target mailbox results in a duplicate message existing in that mailbox. It is recommended to only restore messages that have been deleted from the mail system, but exist in the Retain archive.

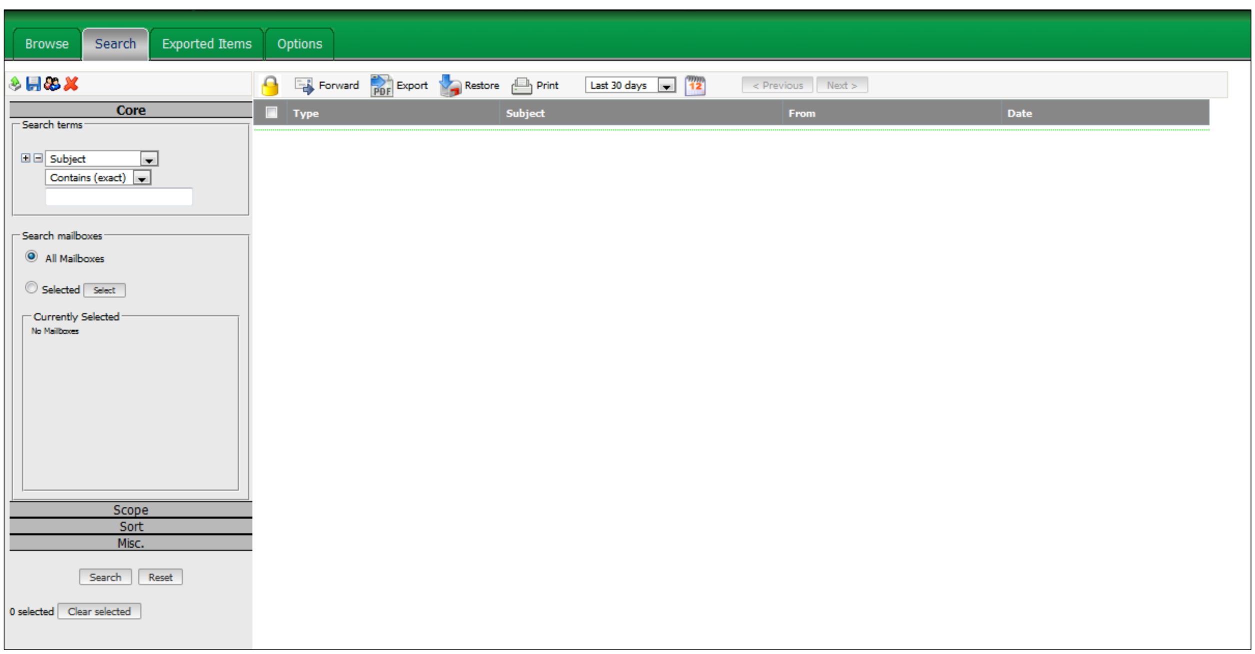


The Restore Stub feature requires:

- GroupWise 8 Client
- GroupWise 8 Post Office
- Retain Stubbing Server
- Stubbing correctly setup in ConsoleOne.
- Sufficient user rights to restore messages.

Search

This is the default **Search** screen.



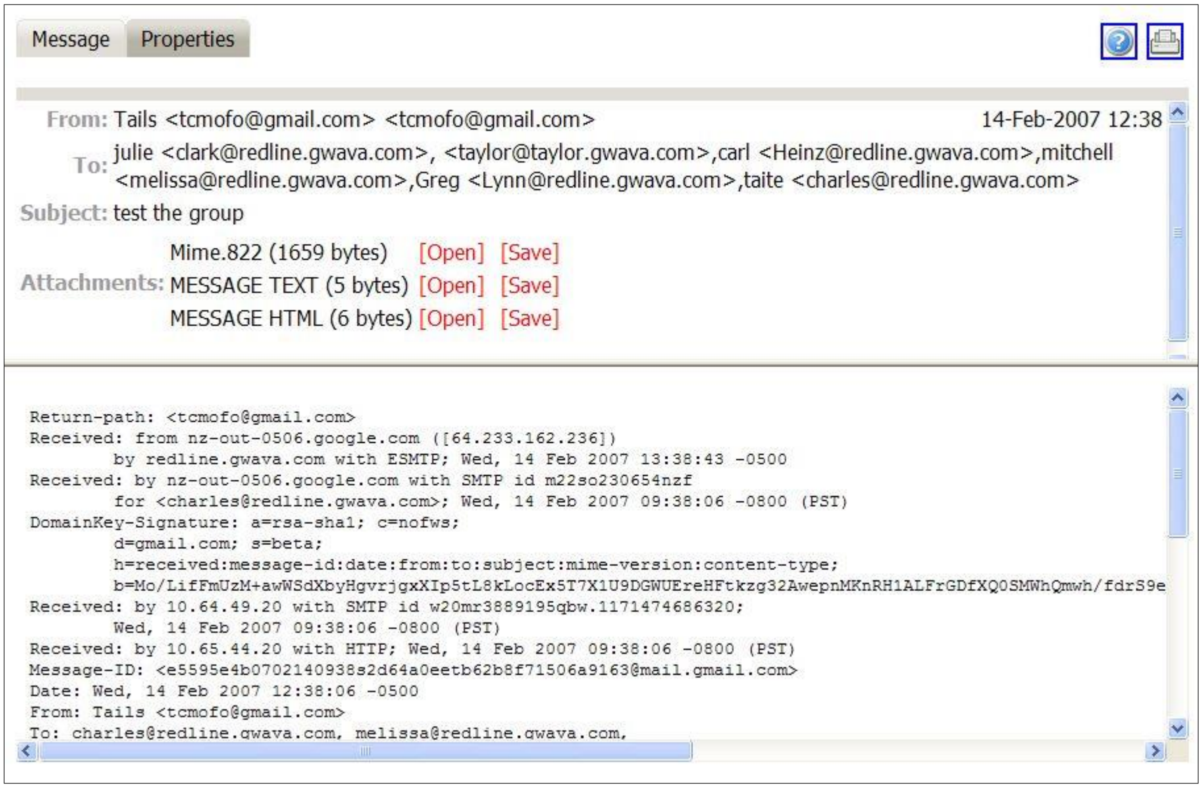
In Search, you enter your criteria on the left, including the scope of your search. Multiple criteria are permitted and you can perform a precise search this way. Your search results appear in the main window. Users with more rights will have more tools and search options available. Only users with rights to the different options in the archive will have those options appear in their toolbar.

Retain will search across all mailboxes you have rights to. By default, a regular user only has rights to their own mailbox and therefore will only see results from that.

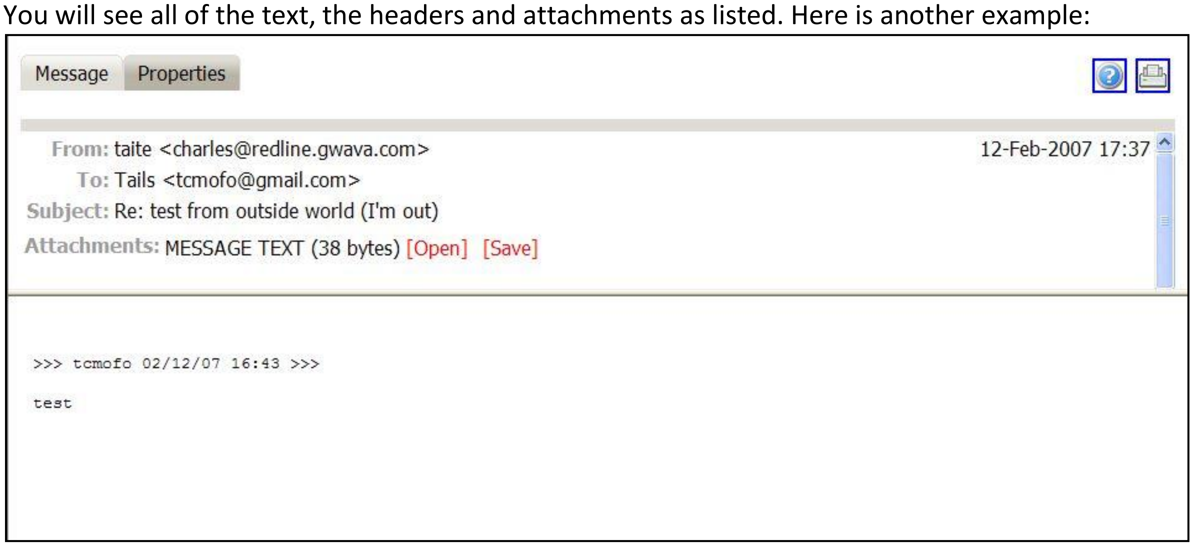
See Search in More Detail

Opening/Viewing a Message

Here is an example of a message opened in the Retain message window:

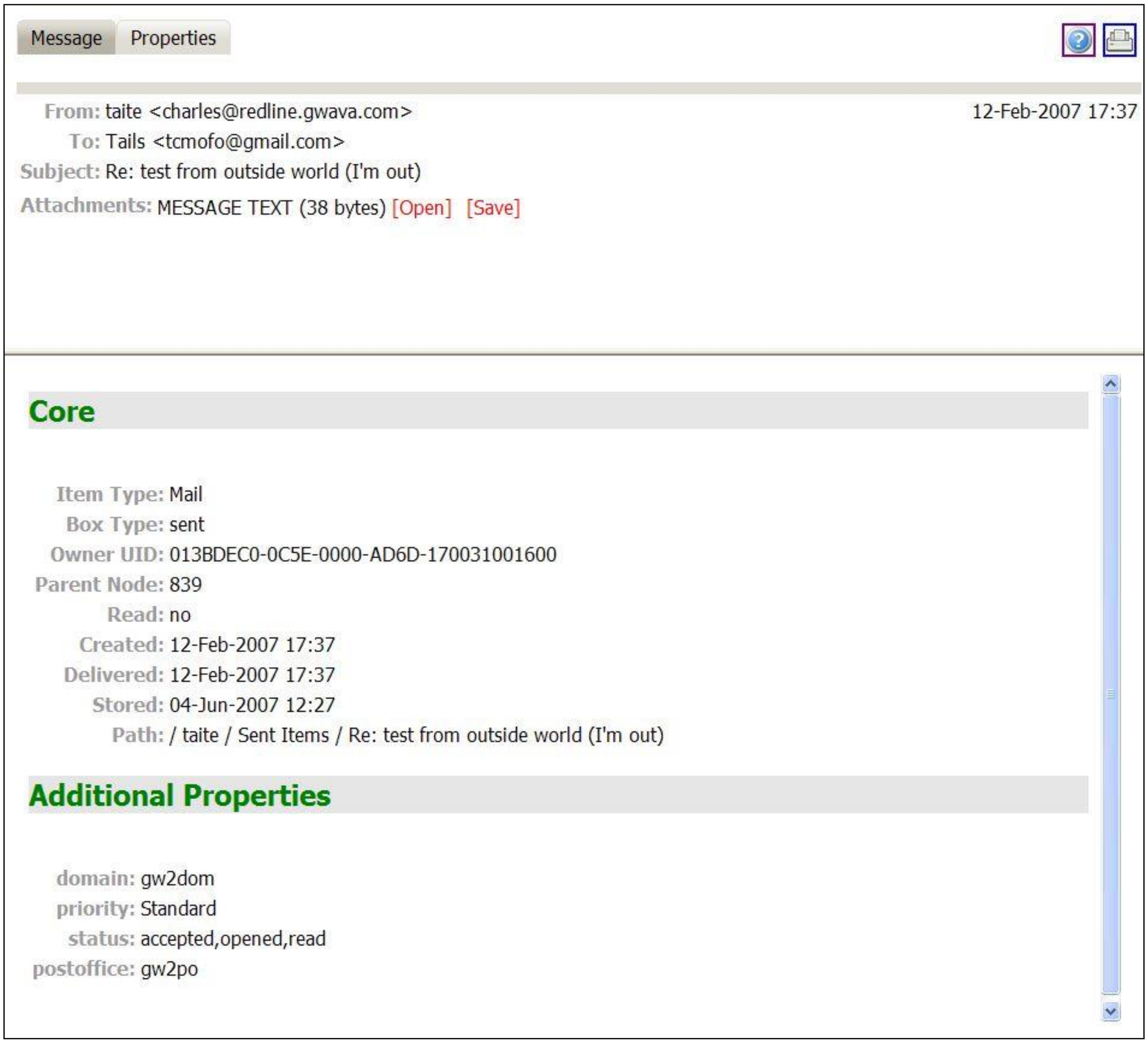


You will see all of the text, the headers and attachments as listed. Here is another example:



Notice how the message's metadata has all been saved: time/date, status of attachments and so on.

The user may print the message or save it to disk, if they possess the necessary rights. You can also select the properties tab to see more information about the message:

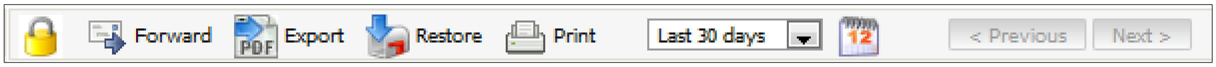


The message's item type, status, relationship information, opened status, original location and so on are all stored. All of these items are valid based on the time the message was archived from GroupWise.

The properties section is where a lot of fields that are specific to the Mail system are saved.

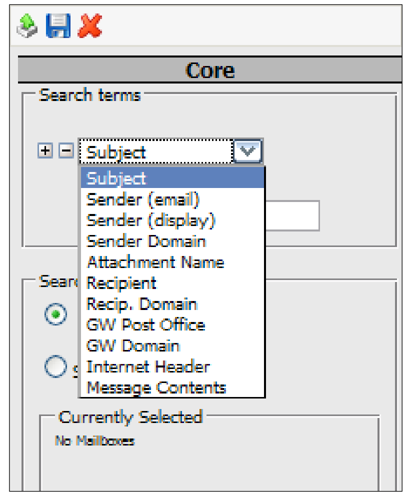
Search in More Detail

The search window has some of the same top buttons as the browse window.



Search Window

The browse window allows the user to access a single mailbox at a time, access the folder tree of the mailbox and perform some basic searching and filtering. For more advanced searching options, and the ability to search multiple mailboxes at once use the Search Window.



Core Tab

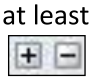
Search Terms – What To Look For

You specify up to 5 additional criteria here. All items are logically AND-ed together to narrow the search unless specified with a double pipe. Using the double pipe denotes an 'or' search criteria. (I.e. A search criteria with 'Retain || Vertigo' would result with messages containing the words 'retain' OR 'vertigo' in the specified field.) To use the Internet Header search term, you must

[enable the Internet Header options in the profile](#).

You can search based on all items shown on the right with operators including:

- Contains (fuzzy)
- Contains (exact)
- Starts with
- Does not contain

You must have at least one search item. You can add and delete them using the  buttons to the left.

Search Mailboxes – Where to Look

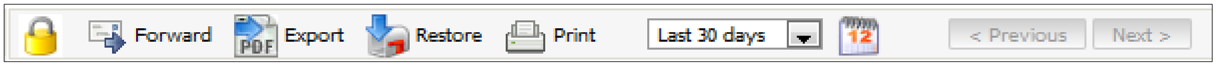
Click the radio button to search through all mailboxes (that you have rights to) or click the other radio button to search through selected mailboxes.

You choose which mailbox, or mailboxes to search through using the mailbox selection tool. (See below) Mailboxes that you have selected for the search are listed in the Currently Selected panel.

Start Your Search

To initiate a search, click the search button. The results will appear on the right, and will be saved as a persistent query. Every time you execute search, even between login sessions, the same query will be executed. If you click on the Reset button, the current query is cleared.

The toolbar on the right provides similar functionality to the browse window toolbar, and allows the user to forward messages from the search results, print, etc. - assuming the user has rights to do so.

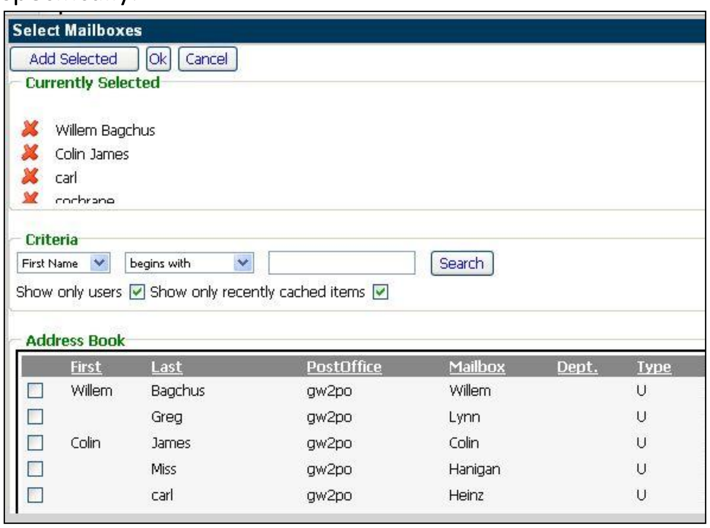


RESET – clears the query entirely.

Selecting Mailboxes

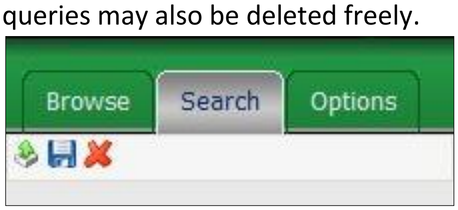
When you click on SELECT, you choose which mailboxes to search through using the selection tool. Use the check boxes to select mailboxes and click “Add Selected” to add them to the list in “Currently Selected”. You may remove mailboxes from the “Currently Selected” list by clicking on the red X next to them.

You will see the mailboxes made available to you via GroupWise proxy rights (if the function is enabled in Retain), via the “Search All Mailboxes” right or via mailboxes you have been granted access to specifically.



Loading, Saving and Deleting Searches

The user may save searches for future use, and reload them whenever they are useful. These search queries may also be deleted freely.

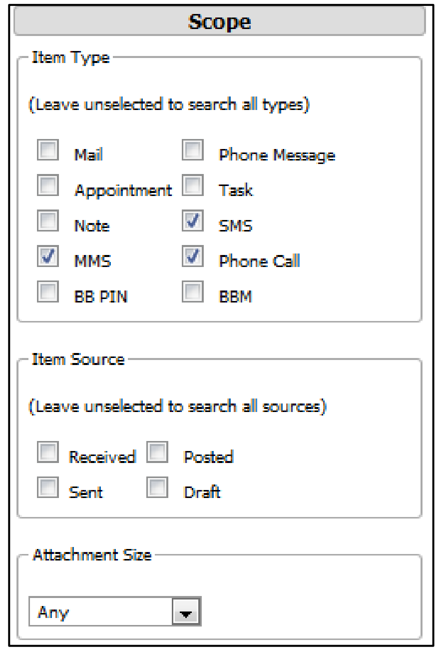


The icons (below the tabs) from left to right mean:

- Load
- Save
- Delete

You can save up to ten queries and you may delete queries you no longer want.

Scope Tab



This tab contains functions to further narrow what you're searching through.

Item Type

If no boxes are checked, you will search through every mail system item type. Otherwise, Retain will search through only those types of items you have checked off.

Item Source

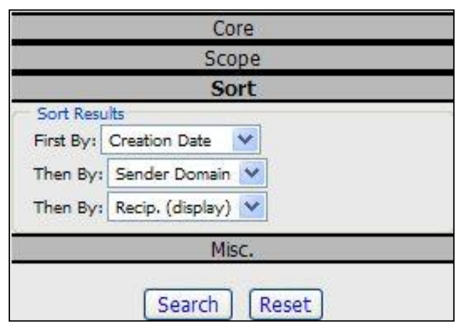
If no boxes are checked, you will search through every item source. Otherwise, Retain will search through only those items whose source matches what you have selected.

Attachment Size

When searching through messages, you can tell Retain to search through all messages regardless of the size of the attachments or whether to restrict your search to only those items whose attachments are within the size range you select.

Sort Tab

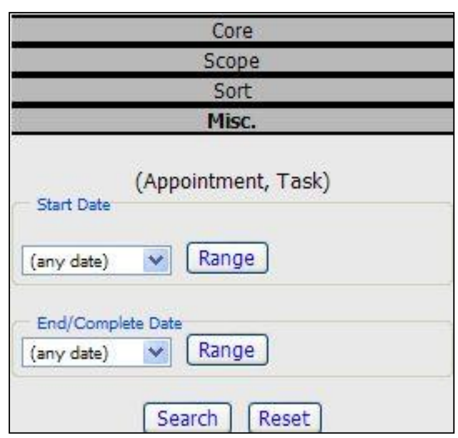
Choose how you want Retain to sort your search results.



You may sort your results by the date the items were created in the mail system, by the Subject, Sender, Sender's Domain, the Recipient's e-mail address, or display name.

Your sort may be up to three levels deep.

Misc. Tab



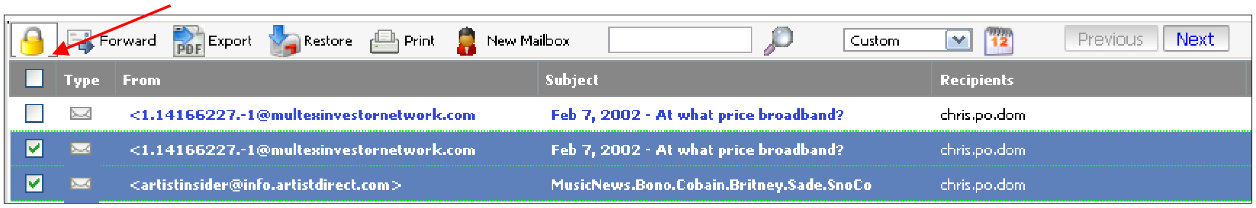
Choose your Date Range here. It is important to note WHAT date is being filtered here. It is NOT the same as the date range selector on the results window. The results window date range filters based on the date the item was created in the mail system.

In this case, it is for filtering appointments and tasks. So you are filtering based on the start/end dates of the item, regardless of when it was created in the mail system. For example, you might have created an appointment for yourself that will happen in three months. The creation date is three months away from the start/finish dates.

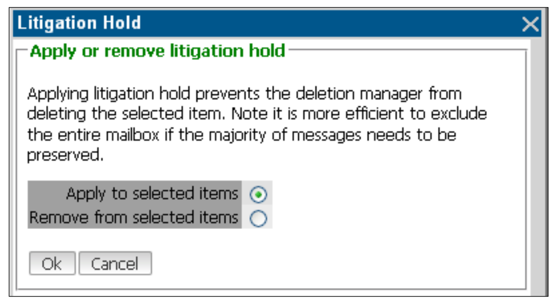
Litigation hold

Litigation hold is a feature which counteracts the deletion manager. To use the Litigation hold feature, users MUST have the litigation hold right granted to them in the Retain Server.

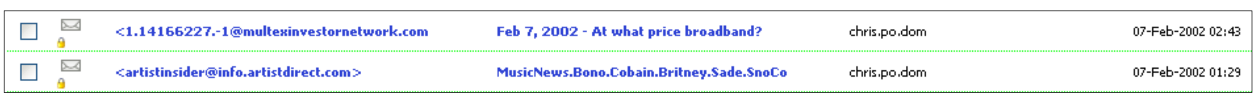
The deletion manager is how mail is expired out of the archive, and removed when no longer needed due to age or other circumstance. Litigation hold tells the system to ignore the remove command from the deletion manager; messages or entire user mailboxes with litigation hold applied will not have any mail removed from the system until the hold is removed.



To apply the Litigation hold to an item, select the item then select the padlock at the top of the browse window. The following window will be displayed:



Choose whether to apply or remove the hold from the selected items. The entire use mailbox may be excluded from a deletion job in the deletion manager.



Items that have a litigation hold active on them are marked by a small padlock in the interface. If a hold needs to be removed, selecting the item then the litigation hold button at the top will bring up the option to remove the hold from the selected items.

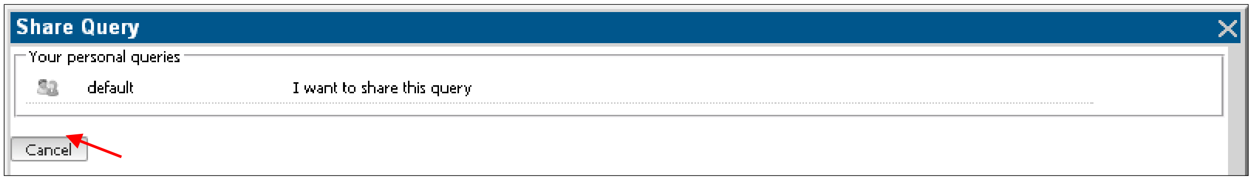
Shared Queries

Queries may be shared with other users in the system. Shared queries are still subject to the individual rights of any user that the query is shared with. A shared query shows the full results to the query but does not grant access to the messages. If a user is restricted from viewing the mail from another user, but has a shared query, they will be unable to access the messages outside their rights.

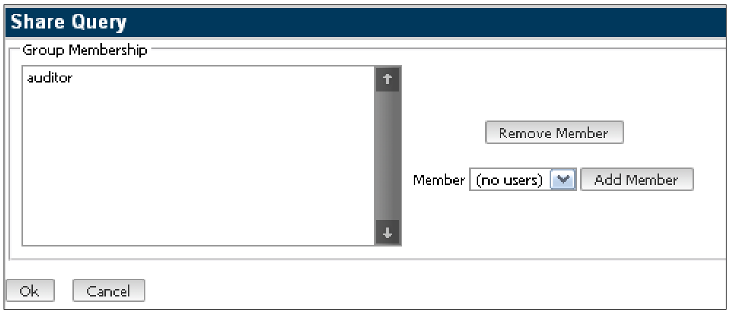
Any search may be saved and any saved query may be shared with other users. When a shared query is created, the creator decides which users to share the query with. Once a query has been saved by using the disk icon at the top of the search window, it can become a shared query.

Creating a shared query takes two main steps. A query must be shared, and then accessed by the user it was shared with. To share an existing query, select the sharing icon at the top of the search window. This icon looks like red and blue users. The icon is between the save, and the close icons.

After selecting the share query icon, a window displaying all saved queries is displayed.



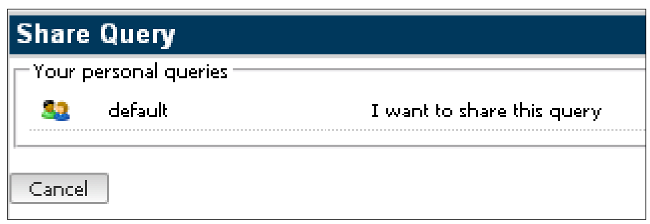
There are no queries shared in this window. The queries are listed, displaying name and description. If a query is to be shared, select the gray icon at the beginning of the saved query.



After selecting the shared query icon, the query creator must now select which users to share the query with.

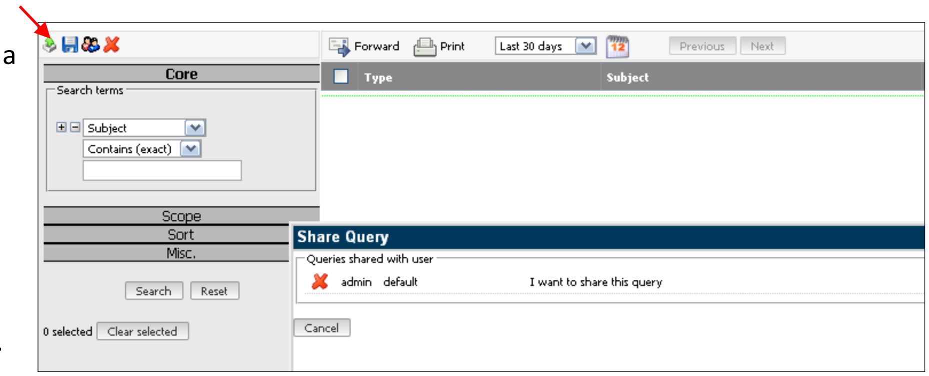
Use the drop-down menu and 'Add Member, Remove Member' buttons to populate the group the query is to be shared with.

Once the group has been selected, click 'Ok' to be returned to the Share Query window. If the share query icon is now colored instead of gray, then the query has been successfully shared, and the users in the shared group now have access to the query.



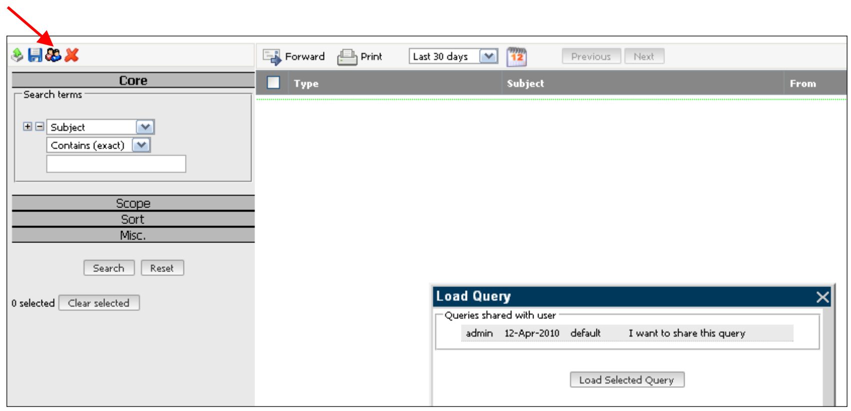
There is no limit to the amount of users that a query can be shared with. Adding users to an existing shared query group is accomplished by selecting the shared query icon and editing the existing list. The user which created and initially shared the query retains the rights to remove users from the shared query group membership or cancel the share altogether.

Accessing Shared Query



To access a shared query, a user which has membership in a shared query group logs into Retain and selects the Search tab. In the Search window, the user selects the Load icon at the top left of the search window. All saved queries will be displayed, and the query that was shared will be available to be viewed. Select the desired query and the 'Load Selected Query' button to load the search criteria. Clicking 'Search' loads the messages fitting the shared criteria.

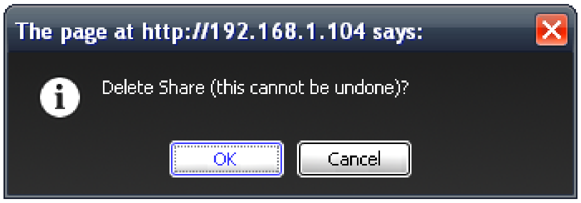
Removing a Shared Query



Users have the option to remove a shared query from their saved query list.

If a user desires to remove a shared query from their query list, it is accomplished through the 'Shared Query' window. Select the 'Shared Query' icon to view all queries that are shared, and that the user is sharing.

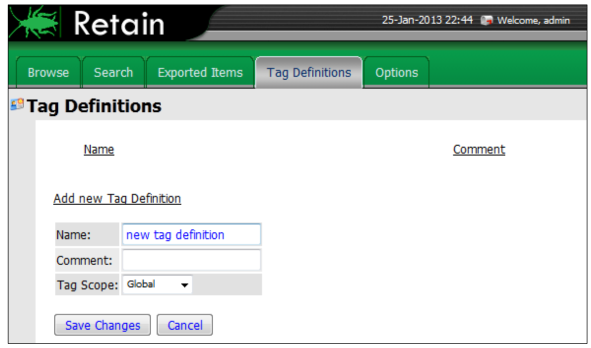
Selecting the red 'X' next to the offending query in the shared query window will remove the query and remove the user from the shared query group.



This action cannot be reversed, but the query may be re-shared.

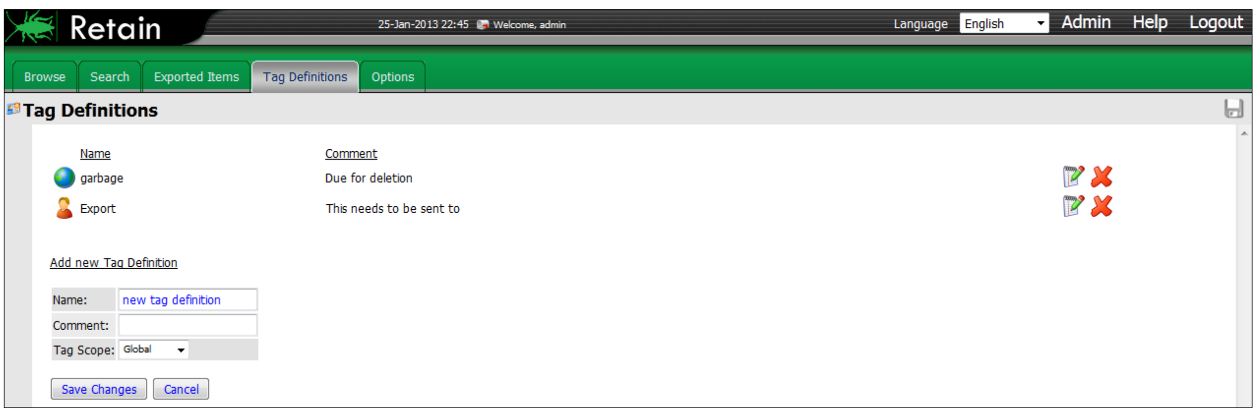
Tag Definitions

The Tag Definitions tab allows the creation and removal of Tags, their automatic comment, and name. Tags are an informative note which can be attached to any data item in the search messages interface. There is no limit to how many tags any one item may have applied to it, and there is no limit to how many tags a user may create. In addition, tags are also a serachable item, making this one of the most versitile ways to add long-term identification for items in the data store.



Before the tag icon will appare on the toolbar in the search interface, there must be at least one tag defined. To define a tag, enter the tag name and initial comment if desired, then, if the user has permissions to do so, define whether the tag is personal or global. Once saved the tag is available for use.

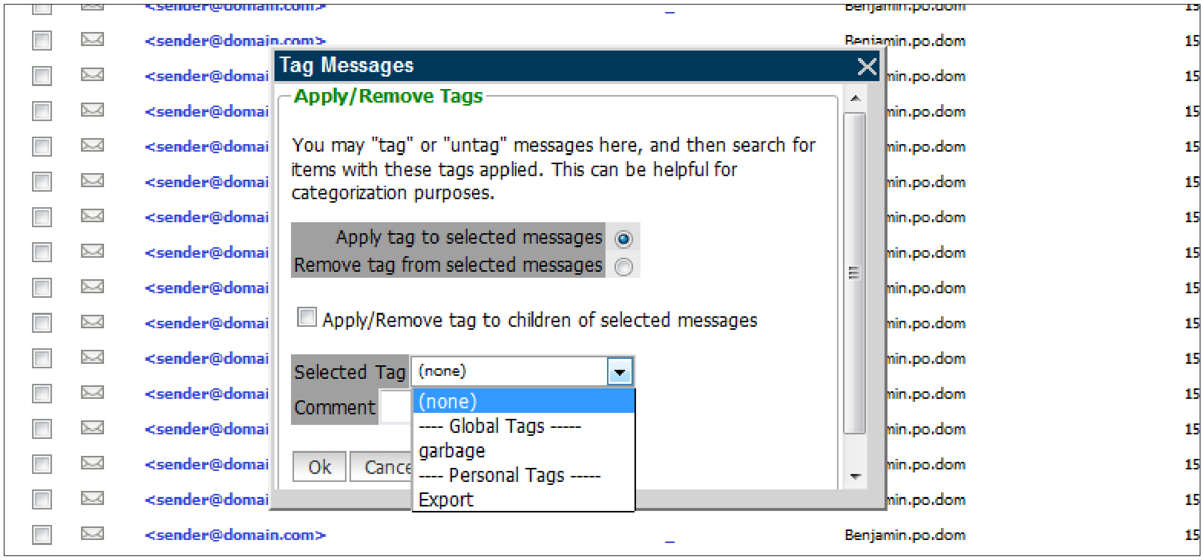
Global tags are tags that any user with the rights to see global tags will be able to view and apply.
Personal tags are limited to the user who created them. Only tags visible to users will be available to be searched for by that user.



Any tags created or subject to manipulation by the user logged-in will be displayed under this tab.

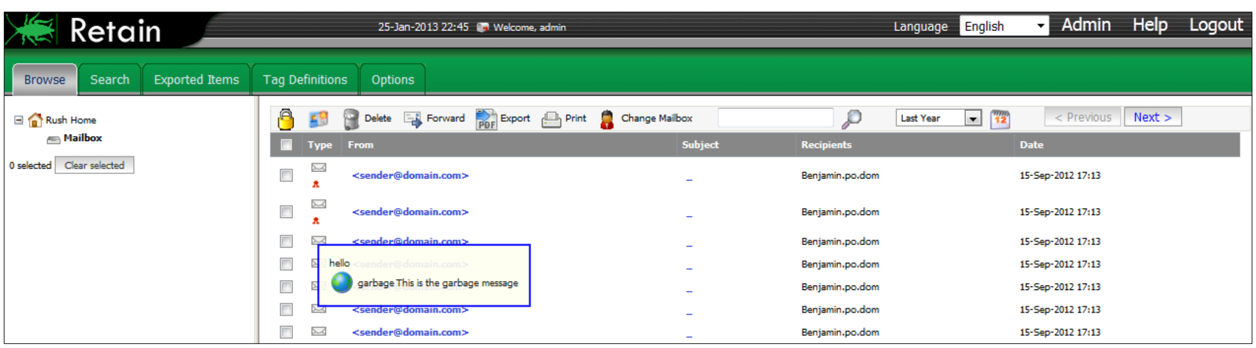
To apply a tag to a message or data item in the search messages interface, simply select the data item or items, and then click the ‘Add / Remove’ tag button in the toolbar.

Once the ‘Add / Remove Tags’ button has been pressed, the following information box is displayed:



All tags open for use by the user will be displayed, both global and personal. There is no limit to the amount of tags that can be applied to any one message. An additional comment may be added to the tag for the specific item or items selected. In addition, any associated ‘children’ messages or data items connected to the selected ones, may also be selected for tag application.

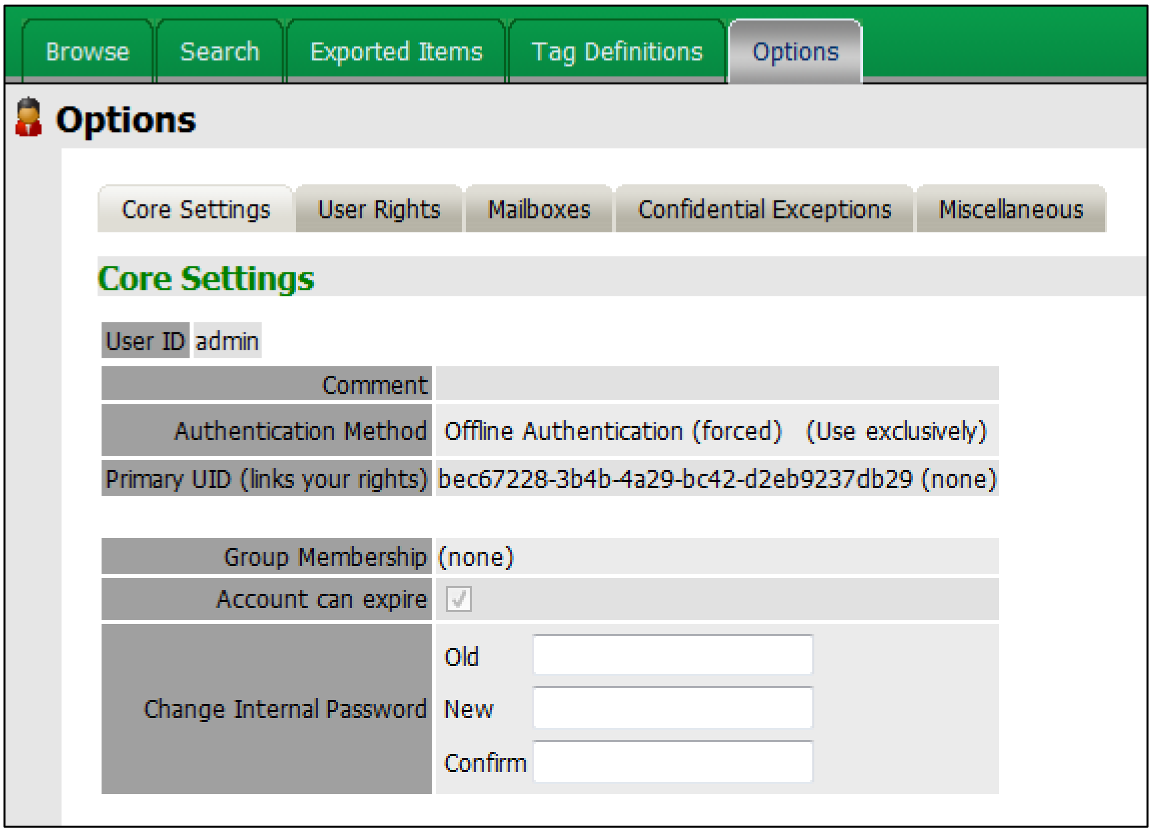
Once a message has one or more tags applied to it, a badge is displayed below the item icon in the window.



Hovering over the item’s tag badge will display the tag; the global or personal icon along with the name and initial comment.

Options Tab

The options section here is exactly like the section in the Administration | Users section. These settings here are specific to the currently logged in user. The current loaded user is shown next to "User ID" located below the Core Settings tab.

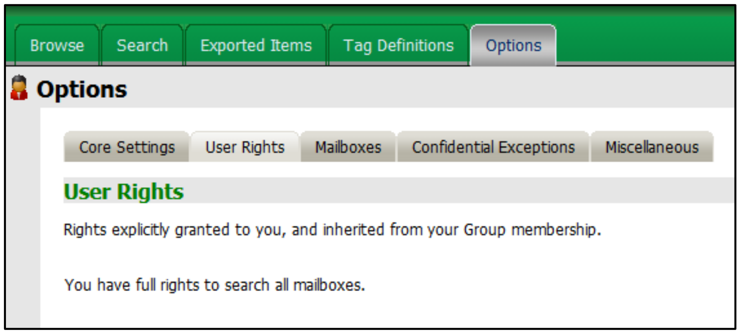


Core Settings

Among the information displayed is:

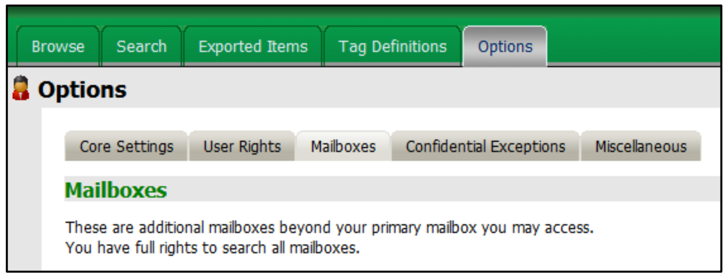
- Your User ID (internally generated by Retain)
- Your Group Membership (you cannot change that here)
- Your authentication method (you may change this if you have rights to)
- Your offline password if you don't use SOAP to authenticate
    - You may change the password only if you have rights to change it.

User Rights Tab



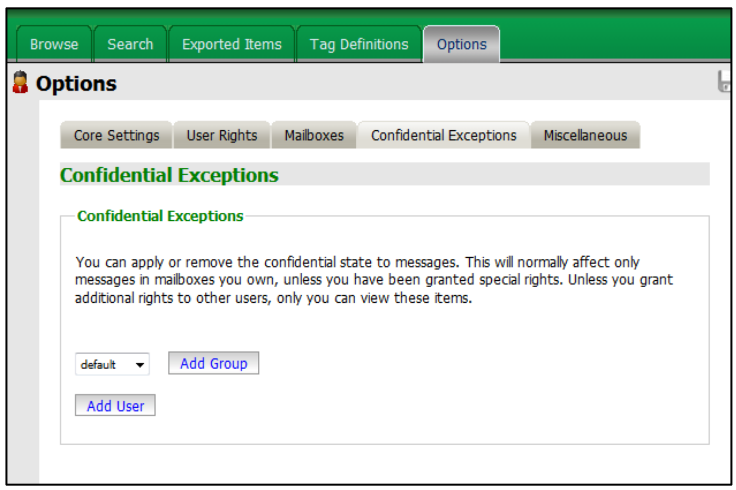
You're shown the rights you have within Retain on this screen. Available rights may only be changed by a user administrator within the Administration screen.

Mailboxes Tab



In this section, you're shown the mailboxes you have been given explicit rights to work in. By default, you have rights to only your own mailbox. If an administrator explicitly gives you rights to other mailboxes or you are a member of a group that has rights to other mailboxes explicitly, those mailboxes will be shown here.

Confidential Exceptions



When a user marks a message as 'Confidential' in the archive, the message becomes invisible to all except administrators who have been given the confidential right, or any user which is specified in the exception list.

The 'Confidential Exceptions' allows users to add any necessary exceptions to the confidential tagging. Confidential tagging may be applied to protect sensitive. However, sometimes this information may need to be viewed by others and instead of granting that user rights to see confidential items for all users, a user may apply that right to only their items.

A group or individual user may be added to or removed from the list.

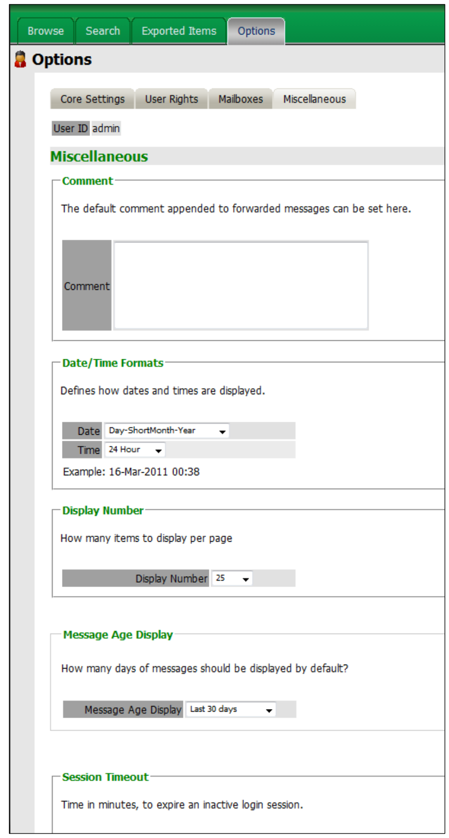
Miscellaneous Tab

This contains your display and session options.

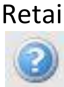
These work just as described in the user display options in the Administration screen.

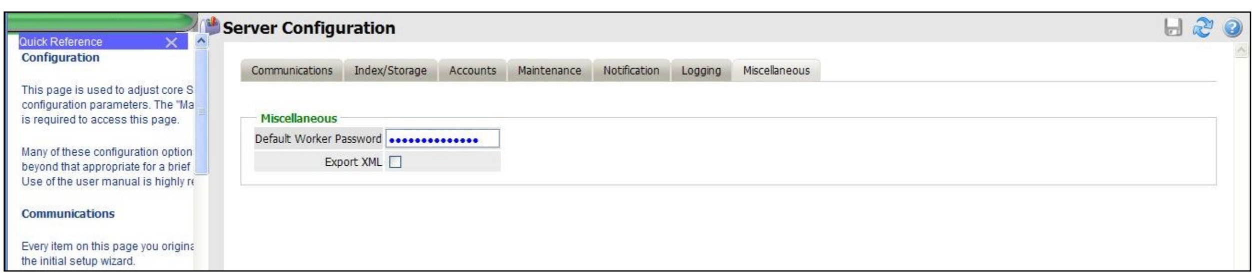
Options are:

- Comment — Default comment for forwarding messages.
- Date/Time Format — How you want your dates and times to be displayed.
- Display Number — How many items to display per page.
- Message Age Display — Default date filter for searching. It may be changed on the fly.
- Session Timeout — Inactive session timeout. Can be between 5 and 60 minutes.



Using the Retain Help System

Retain has context-sensitive help screens that appear in the left column when you click the help icon. ()



To view help, click the help icon on the right (the blue question mark circle icon) and the help will appear on the left.

Scroll through and read what you need. To hide the help and make the menus re-appear, click the X at the upper right of the help screen.

All topics in the main window are covered in help.

About and Diagnostics Page

There is a special page in Retain containing credits for those who helped with the project.

There are also valuable diagnostics on this page. When you tune the memory usage of the Retain components, you may want to refer to these diagnostics and statistics.

To get this page from anywhere in the administrative console of Retain, click on the GWAVA logo in the top left corner, or the 'about' link in the top right.

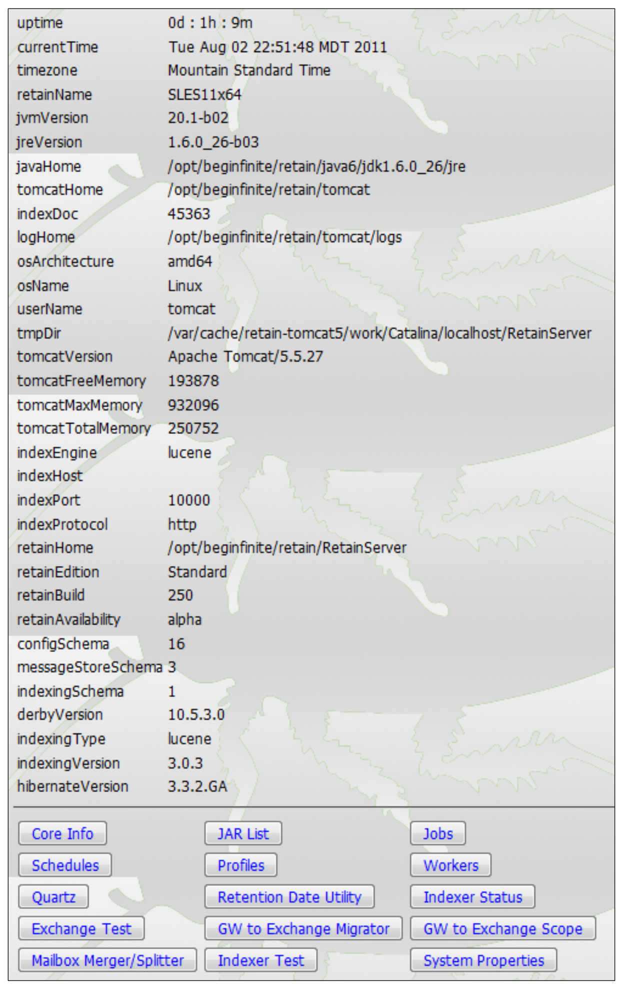
There are two parts to this screen. The credits part is at the top.

The diagnostics part is below.

Operational statistics are listed such as uptime, component version numbers, directory paths and memory statistics.

Below that, the buttons will give you more detailed diagnostic information. Generally, you will only use these at the request of technical support.

Please pay particular attention to the Tomcat memory statistics. This information is needed to fine tune Tomcat.



Diagnostic Buttons

In usual operation, none of these buttons will be used without instruction of support. The diagnostic buttons found on the diagnostics page are used in conjunction with support and can be dangerous for the system if used without understanding or instruction. The utilities contained here display or modify core settings and functions of the Retain Server. Mismanagement of these functions may render the Retain Server unmanageable and in a nonfunctioning state.

Core info, JAR List, Jobs, Schedules, Profiles, Workers

The **Core info, JAR List, Jobs, Schedules, Profiles,** and **Workers** buttons initiate a download of the configuration .xml for each of those categories. All configuration tied to those items which have been configured in the Retain Server will be contained in the downloaded .xml and can be used to examine recorded configuration.

Quartz

The **Quartz** button displays a page containing all information and configuration for the Quartz scheduler. These settings determine when jobs start, when maintenance is, and time in the system.

Retention Date Utility

The **Retention Date Utility** tests the retention and purge flags in the mail systems. It is set in UNIX time stamp format, and should not be used without express guidance from Support.

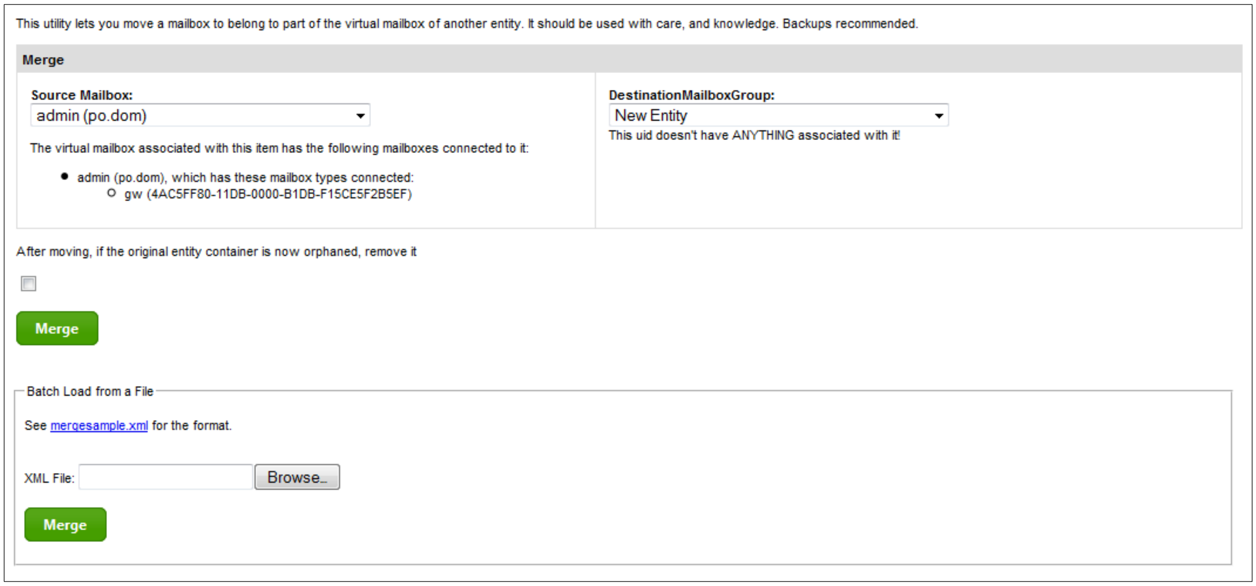
Indexer Status

The **Indexer Status** displays the current health of the indexer engine along with the total unindexed items and associated memory load. There is also an option to shut off or to turn on the indexer. As the indexer should be alive at 'on' at all times during normal operation, only use this utility under instruction from Support.

Exchange Test

The **Exchange Test** utility attempts to connect to and login to the specified mailbox in the Exchange mail system, utilizing current configuration from the Exchange module, if configured. This is used to ensure that sufficient rights and access is open to Retain in the Exchange system. A target mailbox different from the Retain 'service' account must be specified.

Mailbox Merger / Splitter



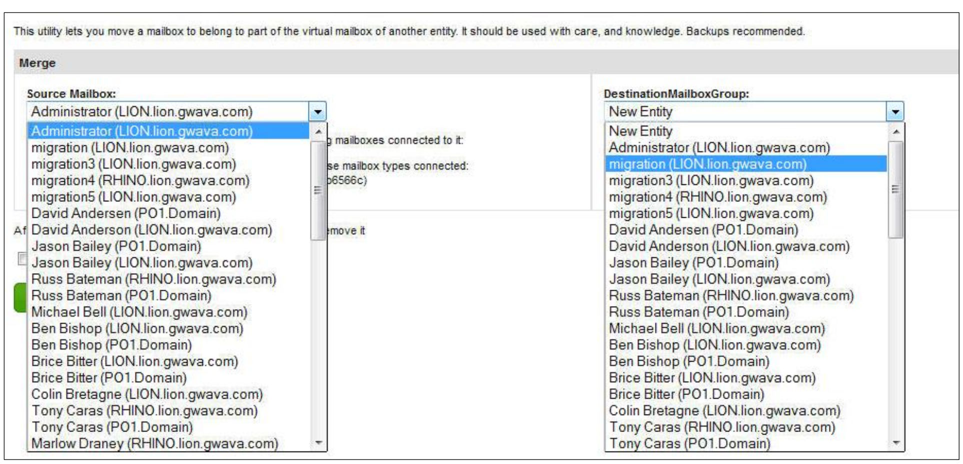
Mailboxes may be automatically merged by the Retain system if configured correctly under the Module Configuration | Mailbox Mapping options screen, but it must be done in correct order or the system will not recognize that a change has occurred and the merge will fail. Automatic merge can only be performed once.

Manually merging and splitting mailboxes is repeatable and is also the only way to undo a merge, automatic or otherwise. A batch load may be created and processed, but requires specific formatting, see the 'mergesample.xml' for format information.

Merging accounts creates a connection between two existing entities in the Retain database by merging their UID's in Retain, and allows a user with two differing email accounts, or one account repeated on two different systems, to manage their mail from within the same interface without having to search for and select a different account, or separately logging-in to two different systems.

To merge two addresses, first select the source mailbox and then select the destination mailbox. After the desired mailboxes have been selected, click the green 'merge' button.

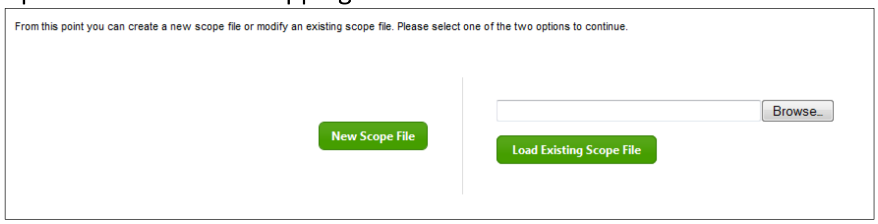
To remove currently merged accounts, select the account you wish to sever as the source mailbox and merge it to a 'new entity'. Because the merge utility relies on tying entities to accounts in the database, the 'new entity' simply unties the account



from any other connections. Tying a user to a new entity does not create any new, floating entities or make any changes in the mail systems; it only severs the selected account from previously merged accounts.

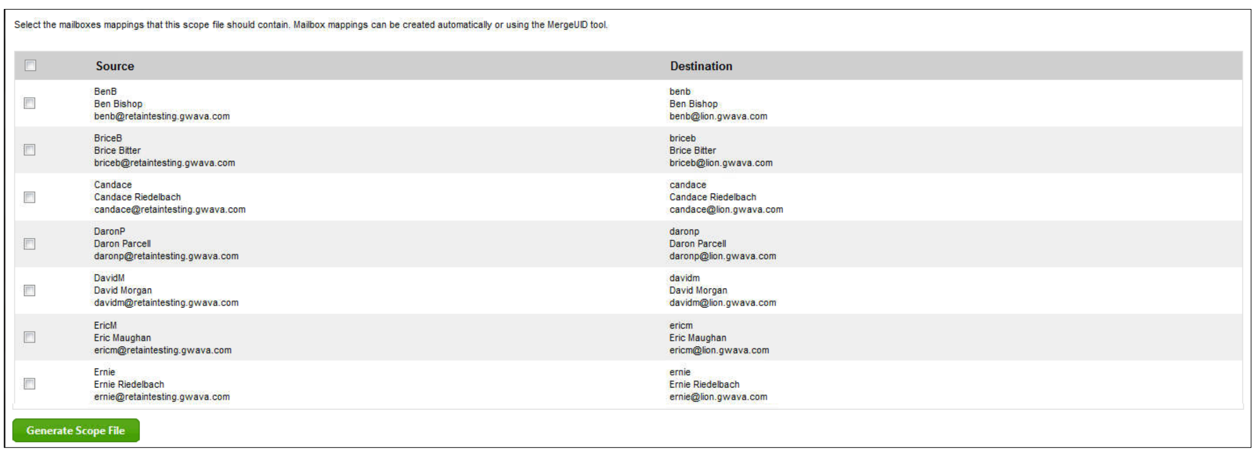
GW to Exchange Scope

The GroupWise to Exchange Scope utilizes mailbox mappings to direct data from the mailbox and is required for the Migration. The scope is used to specify which users are to be included in a migration job. If a user's mailbox data is desired to be migrated from GroupWise and placed into Exchange, they must be included in a scope file used by the migration.



Select 'New Scope File' unless a scope file already exists and is to be modified. After an uploaded file is loaded and modified, a new file will be created.

From the new scope page, users which have been merged are displayed below. For any users to appear, their accounts must first be merged.


Select the mailboxes mappings that this scope file should contain. Mailbox mappings can be created automatically or using the MergeUID tool.

	Source	Destination
☐	BenB Ben Bishop benb@retaintesting.gwava.com	benb Ben Bishop benb@lion.gwava.com
☐	BriceB Brice Bitter briceb@retaintesting.gwava.com	briceb Brice Bitter briceb@lion.gwava.com
☐	Candace Candace Riedelbach candace@retaintesting.gwava.com	candace Candace Riedelbach candace@lion.gwava.com
☐	DaronP Daron Parcell daronp@retaintesting.gwava.com	daronp Daron Parcell daronp@lion.gwava.com
☐	DavidM David Morgan davidm@retaintesting.gwava.com	davidm David Morgan davidm@lion.gwava.com
☐	EricM Eric Maughan ericm@retaintesting.gwava.com	ericm Eric Maughan ericm@lion.gwava.com
☐	Ernie Ernie Riedelbach ernie@retaintesting.gwava.com	ernie Ernie Riedelbach ernie@lion.gwava.com

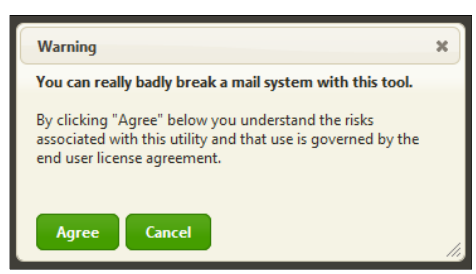
Generate Scope File

Select the desired users from the list by selecting the checkbox next to the name. A global select option is available at the top.

Once the desired users have been selected, click on the 'Generate Scope File' button to create and download the scope file.

GW Exchange Migrator

The GroupWise to Exchange Migrator is enabled via an additional license file. Because of the complexities of the Exchange environment and possible configuration options with Retain, it is recommended that you consult with your reseller or GWAVA Sales Engineer who can provide the license as well as assistance to ensure a successful system migration.



The process to migrate mail from GroupWise to Exchange begins with an existing Exchange system containing existing accounts equivalent to those found in GroupWise. The GW to Exchange migrator will not create accounts, it must have destination accounts to place the mail, and be told which types of mail, and which accounts to put it into.

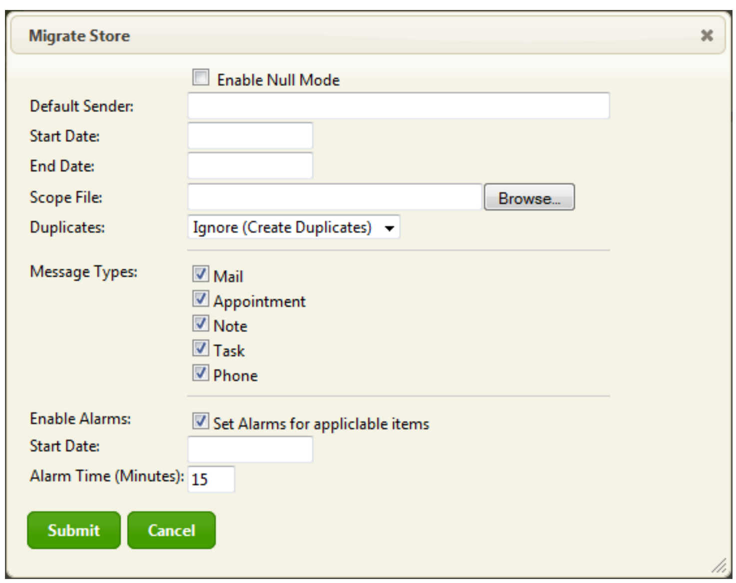
Migrating data from GroupWise to Exchange is not a straight-forward endeavor, as Exchange contains default settings which, at default, block messages from 'untrusted' source, messages with specific attachment types or attachments which are too large. (Default limit for Exchange is 10 mb.) Setting appropriate trusted message types, sources, and size settings in Exchange are the responsibility of the system administrator. GWAVA Inc. is not responsible for any data that is not migrated due to incorrect settings.

To migrate data from an existing GroupWise system into an Exchange system, several steps must be performed in correct order.

1. Configure and cache the address book for both GroupWise and Exchange modules.
2. Merge the virtual Retain accounts either manually or via the automatic merge though mailbox mapping
3. **Immediately** run an Address book refresh from the modules page. (If the address book is not re-cached *immediately* after an automatic merge, the merge will fail and addresses will have to be manually separated and re-connected. Forcing a failed automatic merge can be accomplished by contacting GWAVA Support.)
4. Create a migration scope profile
5. Open the migration tool and fill in the pertinent information
6. Run the migration

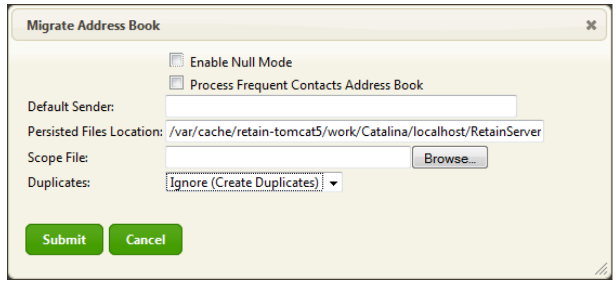
To initiate a migration, select the 'GW to Exchange Migrator' from the diagnostic page. (If your system license does not enable Migration, you will be notified; contact your Retain sales representative.)

The migration tool requires a scope, which functions as a profile for the migration specifying included mailboxes, types of mail to be migrated, and the applicable date range. When an appointment is migrated from GroupWise into Exchange, an alarm can be set in the Exchange system to notify the user of the active appointment. The optional start date creates alarms only for appointments after specified date.



When using the 'Migrate Store' option, only users specified in the scope will be migrated. Browse to the saved scope file, set the start and end date, (blank migrates everything), the message types desired, and then click 'submit' to initiate the migration. If a specific user is necessary for mail system operation, specify a default sender name.

Migrate Address Book migrates the users' personal address book for the users specified in the scope file.



Be sure to manage the duplicates accordingly, as the migration may be performed multiple times.

Indexer Test

The indexer test utility provides a simply and quick query to the index engine and database. This is used as a low-level diagnostic tool for Support and is best used in conjunction with Support. Normal operation does not require any use of this tool.

System Properties

The System Properties utility displays basic system information and settings about the Retain Server, host environment, and functioning parts.

Appendix A: Backing up Retain

There are a few areas of Retain that are important to backup.

- ASConfig.cfg
- License
- Indices
- Archive
- SQL Database

The storage directory and location holds all of these files, and the backed up versions of those that should not be backed up while in use. (To find your storage location, see the Storage tab under Server Configuration.)

Retain automatically creates a backup of certain files, you may specify the settings for the Lucene index backup under Maintenance. Retain will automatically backup ASConfig.cfg and Lucene Indices. (Exalead indices are **not** backed-up by Retain, as Exalead is a completely separate system and should be backed up individually.) These backups are located in the storage location, under the backup directory. The Archive and the License are kept in the storage location as well, though Retain does not create backups of these, so these require a manual backup.

The sensitive location to backup for Retain is:
<your storage location>/backup
<your storage location>/license
<your storage location>/Archive

Steps to back up the SQL database are dependent on the SQL database. See the recommendations of your SQL vendor to find instructions and backup procedures.

Fine tuning GWAVA Retain

Tomcat Memory Usage Tuning Overview

WARNING: *Failure to tune Tomcat's memory usage will guarantee failure of the Retain components and may lead to severe and irreparable data loss and/or corruption!*

The Tomcat servlet container is configured with parameters to indicate how much memory is available for allocation to web applications. Regardless of the amount of physical memory available in the server machine, Tomcat will never exceed these values.

Tomcat is preconfigured with extremely conservative memory allocation parameters– usually from 64 MB to 256MB RAM parameters. This is by design, to avoid taking away too much memory away from other server processes. Once memory is allocated by Tomcat, it is NEVER returned to the general server memory pool.

Two Critical Issues

However, Tomcat's conservative settings present two critical issues:

- The memory allocation is shared among all web applications running under the Tomcat instance. You **cannot** specify a specific amount to be reserved for one specific web application. This is the major reason it is strongly recommended that Retain components (especially the Server component) run on a dedicated Tomcat instance on a dedicated server -- Other web applications such as WebAccess, iManager, iFolder, etc., may consume too much of the shared resources.
- The preconfigured memory parameters may be sufficient for the Retain Worker components. They are definitely not sufficient for the Retain Server component.
  Failure to alter these parameters will guarantee a slow Retain Server, or severe unexplainable crashes and/or irreparable data loss. Recovery of information can potentially be impossible.

Hence, it is crucial that the administrator carefully examine and alter the memory allocation parameters on each server.

General Recommendations

The following are our general recommendations for the maximum memory allocation parameter. The initial memory allocation parameter may be anywhere from 50%-100% of these values. These parameters are discussed in more detail in the next section.

Retain Server Component

A minimum of 1 GB of RAM is recommended. For larger systems, 2-3 GB RAM may be fully warranted. Remember, if this RAM is in use by Tomcat, it is unavailable to other server processes – leave sufficient physical RAM for these. Of course, these others server processes are ideally minimal. Also, remember this memory is shared with other web applications.

Retain Worker Component(s)

The Retain Worker component(s) have been designed to be light weight. Nonetheless, a minimum of 64 MB RAM is recommended, and 160 MB is strongly recommended, to give room for future functionality.

Remember, if this RAM is in use by Tomcat, it is unavailable to other server processes – leave sufficient physical RAM for these. Also, remember this memory is shared with other web applications.

Tomcat Configuration Parameters

There are three significant parameters:

1) **Memory allocated upon Tomcat startup**
   - Indicates how much memory is immediately allocated and reserved to Tomcat upon startup. This memory will be in usage for the entire lifetime of Tomcat and never available to the other server processes.
   - Typically this is set to 50%-100% of the maximum memory parameter discusses below. It can be lower, but pre-allocating a sizeable percentage of memory ***enhances performance*** and reduces memory fragmentation.

2) **Maximum Memory available to Tomcat**
   - If the memory usage grows beyond the startup allocation, Tomcat will allocate additional blocks of memory in chunks as needed up to this limit. It will never return this memory to the general server memory pool. (Although memory internally will be freed and reused for Tomcat applications).
   - Tomcat guarantees that it will never exceed this memory allocation parameter. If Tomcat runs out of memory, it will try to reclaim unused memory via garbage collection. If this is insufficient, the web application will be denied the memory allocation. Unpredictable (but invariably unpleasant) results will then occur.
   - **This is the most critical parameter to tune.**

3) **Stack Size**
   - For each thread (which includes each and every concurrent user request), Tomcat will allocate stack space.
   - This value is typically measured in KB, and defaults to 512KB.
   - It is allocated per concurrent users, and is in fact far too generous a number in general. 1000 users for example would take 500 MB of RAM just for stack space, before the program even allocates memory to run!
   - Generally we recommend reducing this number to 128k-160k. Increase conservatively, in 64 KB chunks, if you see out-of-stack-space errors in the logs.

How to change memory values

Linux Embedded Tomcat Memory Tuning
For Embedded Tomcat which ships with Retain, Edit the following configuration file:
<<Tomcatconfigurationfilej2ee location>>
<</etc/opt/beginfinite/retain/tomcat/j2ee>>

Edit the following line with the appropriate parameters for your system:

CATALINA_OPTS="-Xms256m -Xmx1024m -Xss160k"

This line sets the initial memory pool at 256MB, the maximum at 1024MB, and the stack size at 160KB.

By default, the embedded Tomcat is pre-tuned for basic functions, with 1024MB as the default for the Retain Server, and 256MB for the Retain Worker. THIS WILL NOT BE ENOUGH IN A FULL PRODUCTION ENVIRONMENT. Please tune to fit your system needs.

Windows Embedded Tomcat memory tuning:

1) Go to the System Tray icon for Tomcat. (If using the embedded Retain Tomcat, launch tomcat5w.exe located in C:\Program Files\Apache Software Foundation\Tomcat 5.5\bin. Skip step 2.)
2) Choose configure.
3) Go to the Java tab.
4) Set the Minimum Memory (always used), Maximum Memory, and Stack Size.
   (Retain Tomcat is pre-tuned to 1GB for the Server, and 256MB for the worker, and 160K stack size.)

Checking memory

After logging into Retain Server, click the bug icon at the upper left. Among other stats, you'll see the tomcat Memory statistics. These are for all web apps, not just Retain Server.

UPGRADED SYSTEMS

If you upgraded, it is STRONGLY recommended to return any previous memory tuning back to normal for the original Tomcat while using the embedded Tomcat that comes with Retain. If you are not using the standard Tomcat for any other web resource, simply uninstall or completely disable the standard Tomcat installation.

Windows:
The embedded Tomcat installation overwrites the standard Tomcat installation, and any memory tuning you have previously completed no longer is in effect.

Appendix B – Troubleshooting for Common GroupWise Problems

General GroupWise Error troubleshooting can be effectively done by checking the GroupWise documentation. For any error code not found below, download and check the GroupWise documentation. (http://www.novell.com/documentation/groupwise.html select your GroupWise version and have a look into the Troubleshooting guide for the Error Messages.)
Or, the GroupWise online documentation is usually found at
wwwnovell.com/documentation/<groupwiseversion>/
i.e.
http://www.novell.com/documentation/gw8/
http://www.novell.com/documentation/gw7/

From the troubleshooting menu, select 'Error Messages'
Some common error codes are:

EA04

EA04: The response is too large, SOAP protocol error, or the POA received too much data at once. This error message is largely invalid and gets thrown due to a bug in the current (7.0.2) GroupWise Post Office Agent. Retain has been tested with multiple attachments, some even tens of megabytes in size, that it does get the entire attachment.

To change the setting, edit the POA startup file and add the `/soapsizelimit` variable. Please consult the Novell GroupWise online documentation for the syntax.

Example on NetWare: `/soapsizelimit-2048`

The real solution will be in GroupWise 7 SP3. One workaround is to set the chunking size limit to 2048. We will only take 1024 chunks, and this setting is sufficiently high to fool the POA into not throwing the message.

D712/D714

D712/D714 The administrator has disabled/expired the entire post office or a specific user database. Retain cannot log in.

D714 The Database is temporarily disabled. GroupWise believes a MOVE is in progress. The MOVE must complete before Retain is allowed to log in.

C05D

C05D Item store is missing from Database. A mandatory database file is missing. This implies one of two possibilities:

1) Significant database corruption in the user database, which may be fixed with GWCHECK, or
2) This account has never been logged into before. Until an account is logged into at least once from the GroupWise client, Retain cannot access it.

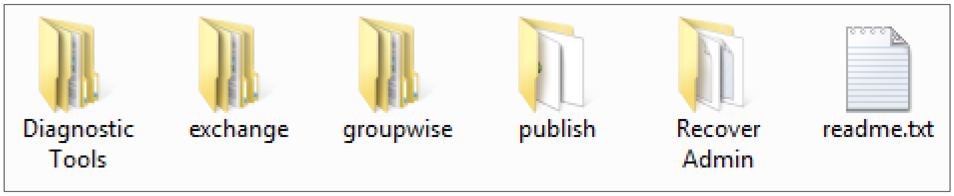
Other notes regarding GroupWise 7, SP 3 (7.0.3)

Retain cannot access mailboxes with either of the following set
- Limited client license

Novell will be addressing the limited client license issue in GroupWise 7 SP 3.

Appendix C – The Tools Folder

There is a TOOLS folder included in the Retain download package.
The tools are grouped into categories, diagnostic and Retain archive tools and platform specific:



GroupWise tools

GroupWise Archive Migration Tool

This migration tool is designed to import native GroupWise archives directly into Retain.
There are two modes:

1. Run at all workstations mode.
   From a command line, you'll run this and it will log into the users mailbox, and then open the local archive. It will then feed messages directly to Retain.
2. Centralized run.
   This only works if you have all archives stored at a central point.
   In this case, one can conveniently run all of the migrations from a single workstation, and not involve the users at all.

Archive Migration Tool

The Archive Migration Tool is for taking your existing native GroupWise archives and sending them to your Retain archive.

The directory contains 5 files:

1) The migration tool itself.
2) The migration tool configuration utility.
3) Two support DLL's and a readme file.

System Requirements

- A Windows XP workstation running GroupWise client 7.0.1 and up.
- Access to the archives you want to migrate.

Overview; Modes of Operation

The migration tool uses the GroupWise client to access the archives you want to migrate.

- In ***single-user mode***, the migration tool will access the mailbox of the logged-in GroupWise user and it will read the archives available to the GroupWise client and send them to the Retain Server you specify.
- In ***multi-user mode***, it will use the **trusted application key** to log in to the mailboxes of the users specified in a chosen **GroupWise distribution list**, attempt to access the archives defined in their mailbox and will send them to the Retain Server you specify.

How it Works

The migration tool does not access the archive files directly. Due to the way GroupWise stores its archives, you need the GroupWise client to read the archives and to hand the data to the migration tool. The migration tool then sends the archives to a Retain Server, much like a worker would.
In normal operation, a Retain Worker reads data from the live GroupWise system and sends it to a Retain Server. With the migration tool, the tool itself is a worker that reads the archived data from the GroupWise client and sends it to a Retain Server.

The migration tool reads the path to the archives as defined in the GroupWise mailbox that you're accessing. That path must be accessible by the workstation you're on. It will then ask GroupWise to open the archives and it will read the items in the archive and send them to the Retain Server you have specified.

If you run in single-user mode, the migration tool will access the mailbox currently logged into by the GroupWise client. If none is logged in, GroupWise will be opened and you will be asked to log in.

If you run in multi-user mode, the migration tool will open GroupWise, you can be logged in as any valid user, and it will use the trusted application key to log in to each user specified in a GroupWise distribution list, one at a time.

Prerequisites

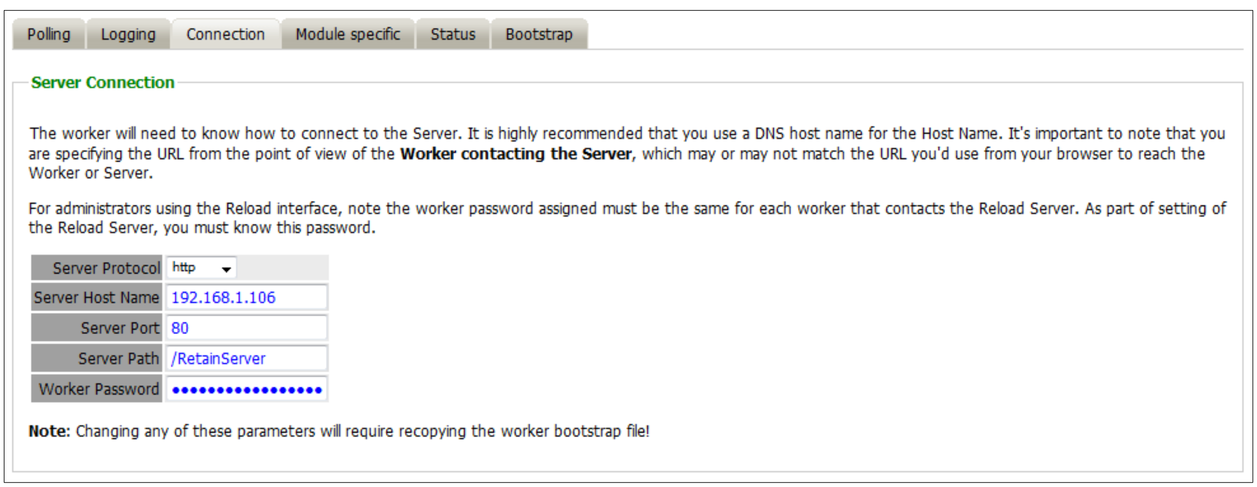
The GroupWise client on the workstation you're using MUST be able to open the archives you wish to migrate. The process depends on GroupWise being able to access these archives. If you're migrating the archives of another user, as you would be doing in multi-user mode, you MUST be able to access that user's archives from the workstation you're on.

It is not enough that the archives are on a network-accessible volume. GroupWise must be aware of the path to these archives and that path must be available from the workstation you're going to use for migration. Refer to the Error Handling section for important configuration.

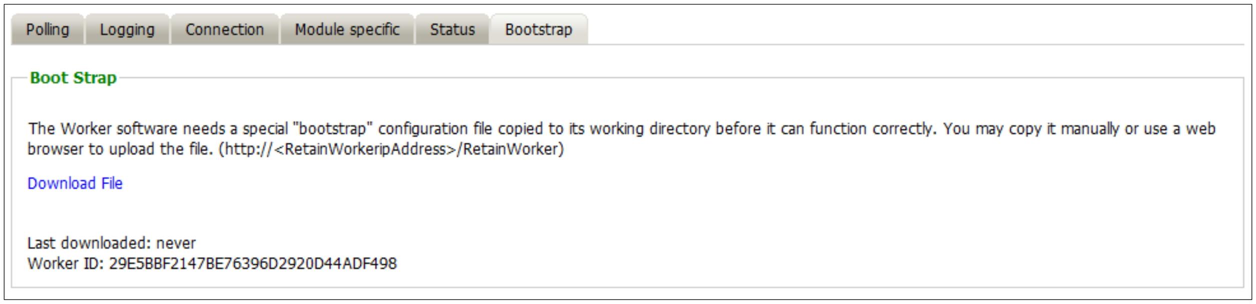
Setting It All Up

In multi-user mode, you can use one workstation to migrate the archives of multiple users. In so doing, you can migrate the data without affecting the user(s) in question. In single-user mode, you will run the migration tool on a workstation that has access to the archives you want to migrate (typically the workstation of the user whose archives you're migrating) and you'll migrate just one mailbox.

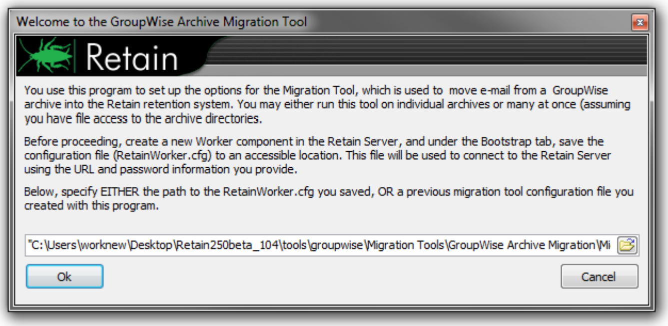
1) Copy the migration tool files to any directory accessible to your workstation.
2) Log in to the Retain Server you want to migrate the archives to.
3) Create a new worker. You're not actually installing a new Retain Worker anywhere; you're creating a new bootstrap file for the use of the migration tool so it knows which Retain Server to send the archives to. Be sure the settings listed are accessible and usable by the workstation where you will be running the migration tool. The migration tool will use these settings to log into the Retain Server.



4) Once you've saved changes, you will be able to save the bootstrap file. Save it in the directory of the migration tool.



5) Now start up the migration tool configuration utility. A window will open on top of the configuration utility requiring the location to find the bootstrap file you have just saved.



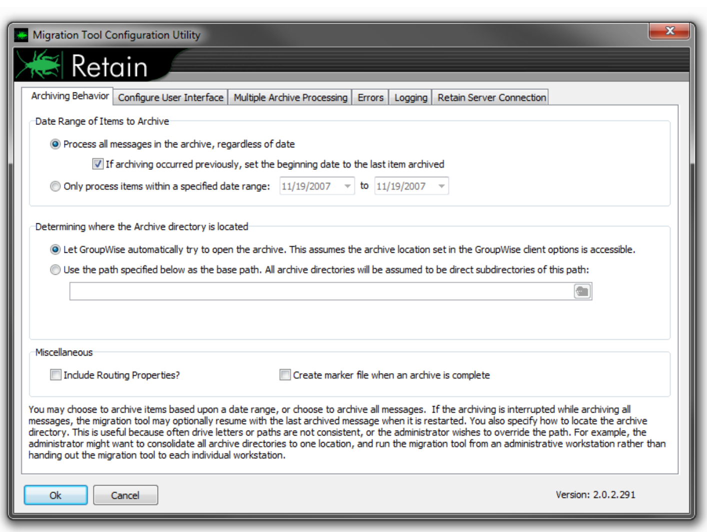
(This window will also accept saved configurations from previous sessions.)

Archiving Behavior

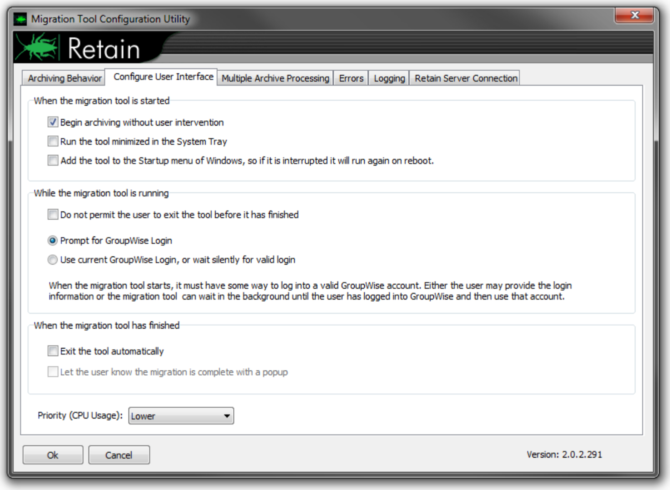
Date Range – limits or specifies specific mail to process based on a date range.

Archive Directory – The location of the archive or archives to be migrated. The default path is assumed unless selected to be specified.

Miscellaneous – contains the options to preserve the routing properties in the archive or to add a marker file when the migration is complete.



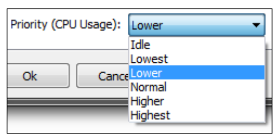
Configure User Interface



When the Migration Tool is Started - Begin without user intervention the archive process immediately begins without any prompts. Run minimized sets the migration utility to run the migration in the background while the workstation completes other work. The tool may also be set to run automatically on system boot, in case something interrupts the archive job.

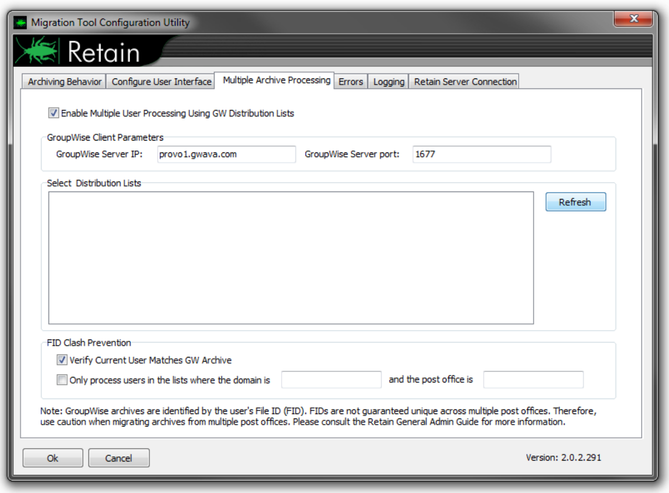
When Migration Tool is Running - Contains options to prohibit the user exiting the program before the archive migration is complete and GroupWise login settings. The tool must be able to login and gain access to the archives.

When the Migration Tool has Finished – Contains the behavior of the migration utility on completion; automatic exit, notification, or neither.



The CPU priority usage is also set here.

Multiple Archive Processing

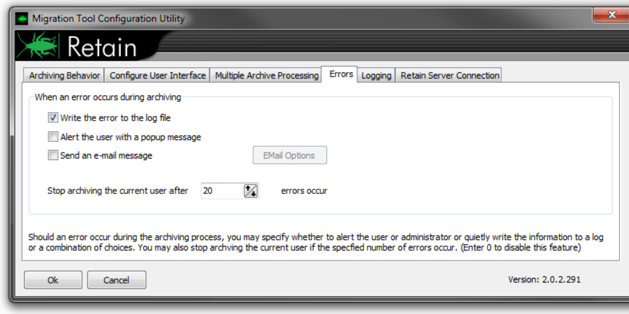


In order to process more than one user archive the option must be enabled at the top of this page and the users must be verified against the GroupWise system.
It is recommended to only process multiple archives from the same post office.

The Multiple User section only appears in **multi-user mode**. (If you click “scan multiple user archives”.) It displays the available distribution lists. The archives belonging to the users in the selected distribution list(s) will be migrated. If users from multiple Post Offices are to be migrated, employ some kind of FID clash protection by verifying archives or only processing users which can be verified by a specified Domain and Post Office, (specified in DNS:port or IP address:port).

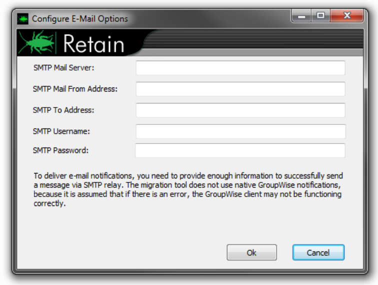
Errors
The error limit and actions taken when an error is encountered are specified on this tab.

Errors may be written to the log file, (specified in the next tab), sent in a pop-up message to the user, or sent as an email to the specified address.



The limit of how many errors may be encountered before the migration utility quits the current user is specified. A setting of '0' sets the limit to infinite. IMPORTANT! **By default, the current user will be skipped after 20 errors by default.**

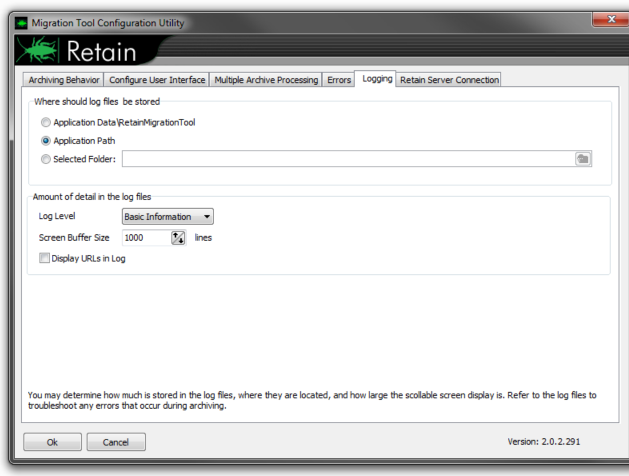
If an email is desired for each error encountered, email settings must be configured. Select 'Email Options 'and input the connection information, source address, destination address, and user login information for the SMTP Mail Server.



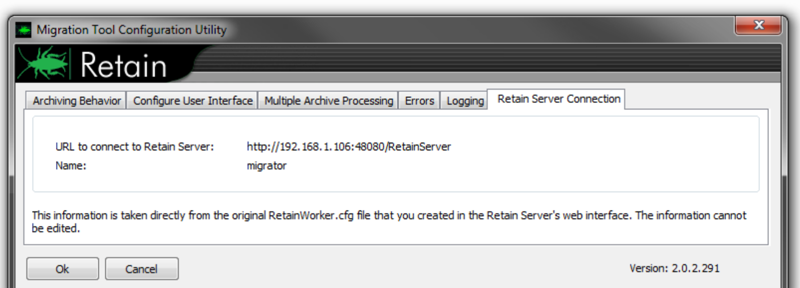
Logging
The location, logging levels, and buffer of the logging screen are all configured on this tab.

Where Should Log Files be Stored - A specified path, the path to the current location of the application, or a specified path must be selected.

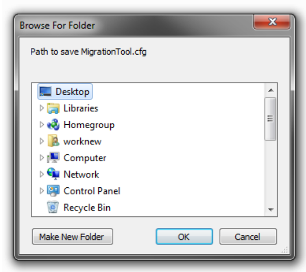
Amount of Detail in the Log Files – The logging level determines how much information is provided in the log files. Unless troubleshooting, log levels of 'normal' and 'errors only' are sufficient. The buffer size for the logging screen determines how much history the running log screen of the migration tool contains.



Retain Server Connection
This is an informational page showing the connection settings from the RetainWorker.cfg created in the Retain Server. If this information is incorrect, the Retain Server Connection settings must be modified under the worker configuration in the Retain Server, and a new bootstrap file downloaded for use.



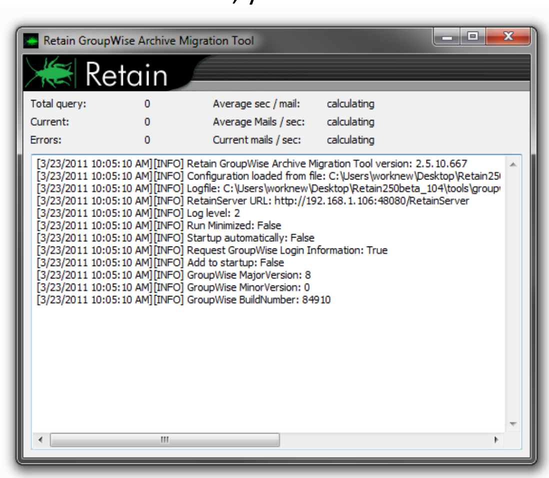
Once the configuration has been setup as desired, click ‘Ok’ and select the location to save the changes into a ‘MigrationTool.cfg’ file.



Running the Migration

The migration tool will use the configuration file to run the job as you have specified in the configuration tool. You may run this tool as often as you need to set up the migration job to your liking.

When the tool runs, you will see a screen like this:



You will see any errors in this screen and when the job is complete, it will say so.

For each user in a multi-user job, it will read the location of the archives from GroupWise and then it will attempt to open the archives. It is critically important that the workstation used for the migration can access the archive files.

Limit of 5 Concurrent Migrations

There is a maximum of 5 migrations permitted at any given time. For instance, if you’re running the migration tool from the workstations of your users, only 5 at a time can be migrated, the others will wait their turn. This is to prevent all the migration requests from overwhelming the server.

Other Notes

The migration tool may be deployed using management tools such as Novell ZENworks. This is one method to collect archives which have been stored on users’ workstations. Users may run the tool manually or it can be run automatically.

The Archive Plug-in

This is a simple C3PO plug-in for Win32 clients that allows you to

- add a Retain menu item for easy access to web archives
- hide current Archive options.

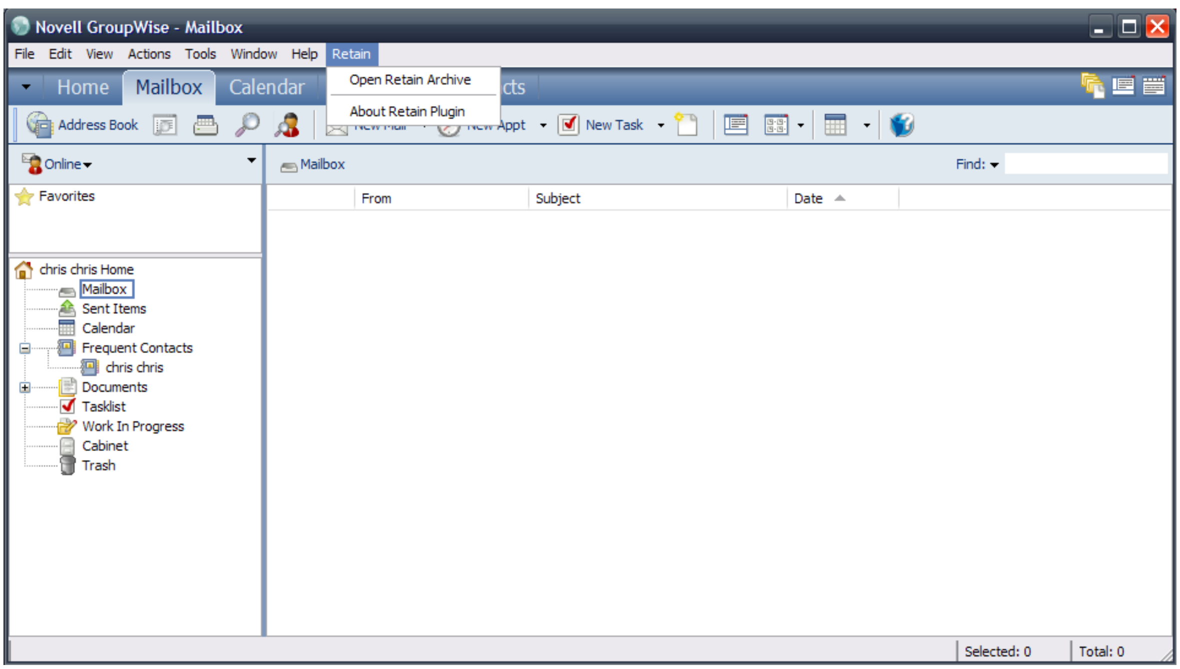
It can be run interactively or via command line. Run the program for the command line switches.

Blob Extraction Tool

This command line utility provides a quick way to extract the original contents of any compressed/encrypted blob in the system. This is for diagnostic and disaster recovery purposes. Simply type BlobExtractionTool at the command line for the usage options.

Single Sign On

The C3PO Plugin for Win32 provides single sign on functionality. To utilize the single sign on feature, the Win32 GroupWise client must have the Retain plugin installed. The Retain Plugin is located in the downloaded install source. (…/<Retain>/tools/Win32 Client Archive Plugin/Retain Archive Plugin.1.1.0.119.exe) The installer must be run on the machine where Single Sign On will be used. Single Sign On requires Retain Server 1.8x or later. Single Sign On integrates a menu option into the GroupWise Win32 client providing easy access to online archives. The Installation requires the specified address of the Retain Server.



Once selected, the Open Retain Archive option will sign the user into Retain using the GroupWise authentication active in the GroupWise client, providing a transparent login. As such, it is not recommended for use on public workstations.

The program may be run from command line, the options are:

- /url=URL (Provide URL to the Retain Server)
- /hidemenu (Hide standard GroupWise archive)
- /SILENT (Run without user intervention – requires /url argument.)

WebAccess

(Same as Single Sign On above)

Requires:

- GroupWise 8 or later
- (Installer only) Java 1.5
- Windows or Linux

NOTE: If you are running WASP2™ you must update to the latest version of WASP (Version 2.0.5) in order to continue using both WASP and the Single Sign On Retain Module on the same WebAccess server. If an earlier version of WASP is in use, it will be broken with the addition of the incompatible Retain WebAccess Single Sign On plugin.

The WebAccess module .jar file is located in the Retain install sources. After Retain has been downloaded and extracted, the .jar file can be found in the …/Retain180/tools/WebAccess plugin directory.

To install the module, run the .jar java executable file in an X session.

i.e.

On Linux:

java –jarRetain_setup_20091005.jar

On Windows:

double-click the file.

For NetWare or remote systems SEE THE FOLLOWING LINK:

http://support2.GWAVA.com/kb/?View=entry&EntryID=1608

Installing to a remote system **requires** direct file access.

The installer file may be run from a workstation fulfilling the requirements to install on a remote machine. To install remotely, WebAccess source directories must be exported and mounted to the workstation.

i.e.

(For Linux):

/srv/www/tomcat5/base/webapps must be exported and mounted via NFS or a SAMBA share

/var/opt/novell/ must be exported from server and mounted to /var/opt/novell on the workstation.

The final step to install the WebAccess plugin is to create two folders in the Novell folder structure. Retain cannot create folders or set permissions on the host system, but requires the folders to be created in the Novell directory structure to function.

Windows:

Two folders need to be created on the GroupWise server. From where GroupWise was installed, browse to:

…\GroupWise\webaccess\retain\templates\webacc

Create two new folders here:

mobile

simple

Restart Tomcat and the plugin installation is complete.

Linux:
Retain requires two folders to be created, as well as the permissions set to match, on the GroupWise server.

Browse to:
/var/opt/novell/groupwise/webaccess/retain/templates/webacc

Create two new folders here: 'mobile' and 'simple'
mkdir mobile
mkdir simple

Note the file permissions and owner of the 'css' folder, and change the permissions of the two new folders to match.

Restart Tomcat
rcretain-tomcat restart

Once Tomcat has been restarted the plugin installation is complete.

Once installed, WebAccess will add a new tab to the User client window called "Retain", which will sign the user into Retain when selected.

For a text-only or shell install on Linux:

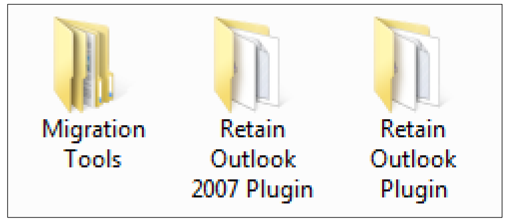
1. Copy the "WebAccess plugin" directory (or contents thereof) to the webserver where the WebAccess Application (the Tomcat servlet, not GWINTER) is installed.
2. Flag the .sh files as executable
    chmod +x *.sh
3. Run desired install:

./installtext.sh (For text mode only install)
./installgui.sh (If running X-windows system and want a graphical install)

(The folders described above must still be created on the GroupWise server.)

Exchange Tools

The Exchange tools folder contains the tools appropriate for the Exchange mail system: personal archive migration, and single sign on plugins.



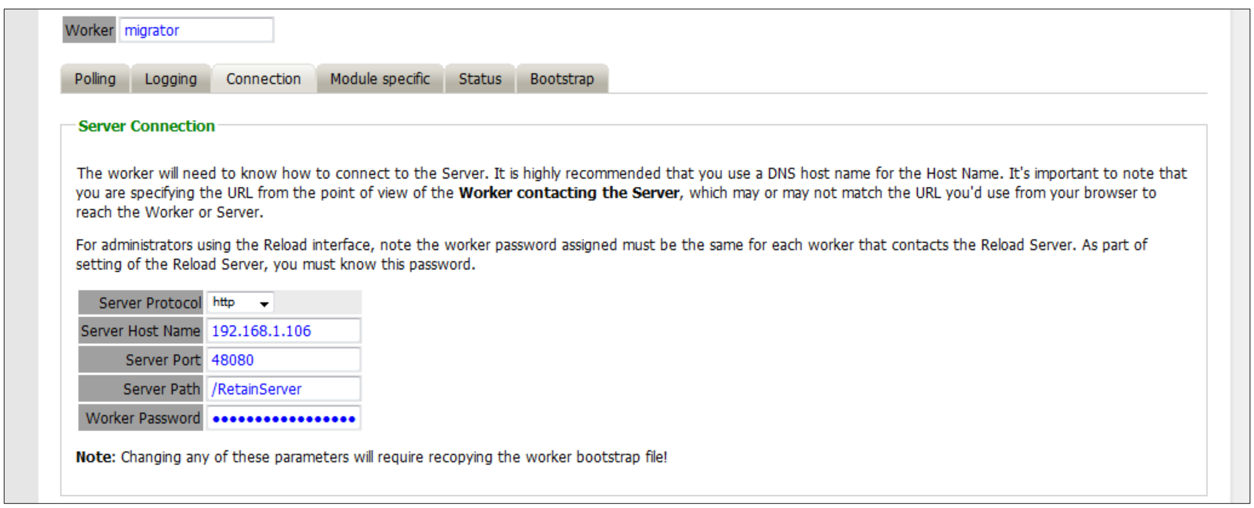
Exchange PST Migrator Migration Tool

The PSTMigrator is a Java utility used to input mail in the PST archives into the Retain system. The PST migrator interfaces with the Retain system through a worker configuration file to contact the Retain server and input the mail found in the PST archive to the Retain system.

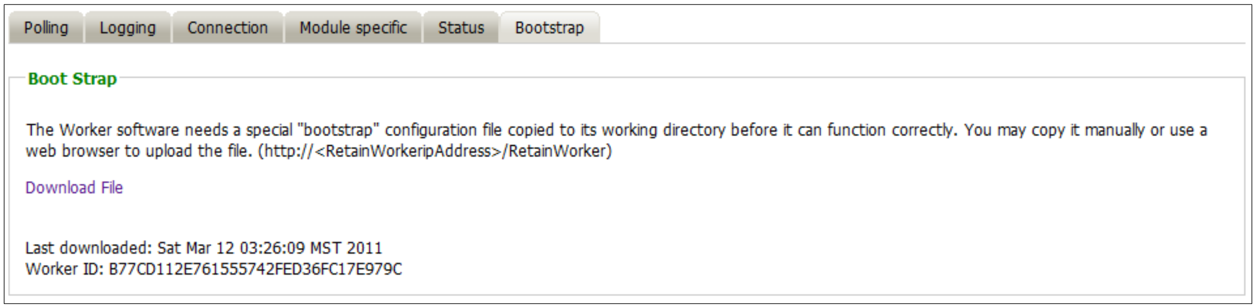
The PSTMigrator should be run on the local workstation where the Outlook PST archive file is located, and requires Java to be locally installed.

The PSTMigrator requires a Worker configuration and bootstrap file to know where and how to communicate with the Retain Server.

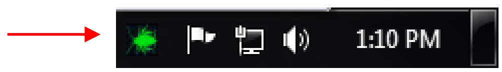
1. In the Retain Server management console, create a new worker, it would be appropriate to name it 'migrator' or 'pst migrator'. A general configuration is all that is required; no specific settings need to be changed from default, except the connection information if it needs to be modified in accordance to the needs of the local network. It is imperative that the PSTMigrator have an open connection to the Retain server. When the settings are correct, save the new worker.



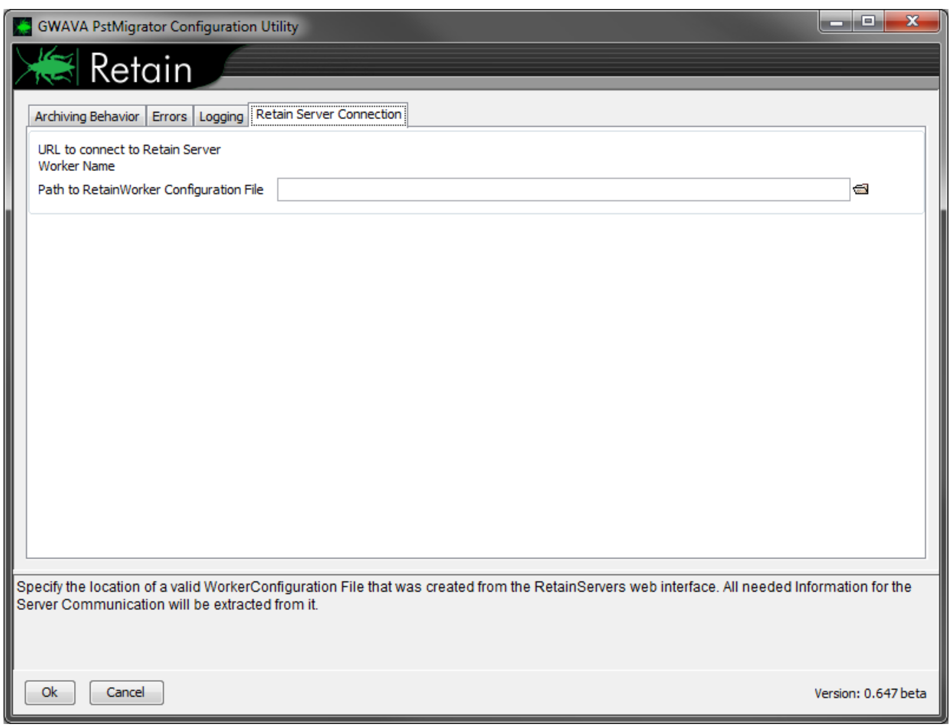
2. Download the bootstrap file.



3. Run the PSTMigrator utility on the Windows workstation containing the pst archive file. If Java is installed, the PSTMigrator.jar file can be run simply by double-clicking on the file.
   When initially run, the PSTMigrator is placed in the taskbar, and must be selected to be opened.

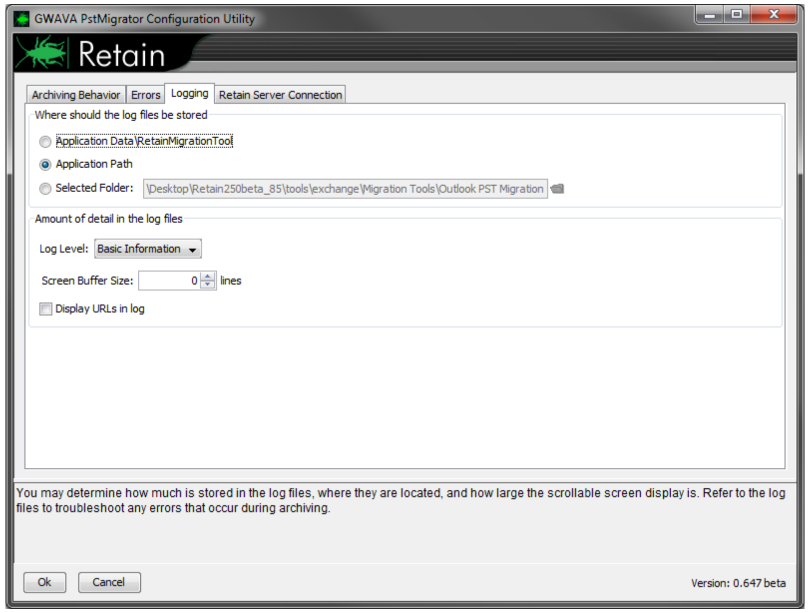


4. Upload the Worker configuration to the PSTMigrator.
   Right click on the PSTMigrator icon in the taskbar, and select 'configuration'.
   The initial screen of the migrator is opened to the Retain Server Connection tab, where the bootstrap file is specified.



Browse to the location of the worker configuration downloaded in step 2, and select the configuration.

5. Configuration logging, error reporting, and specify the pst archive file.



Logging

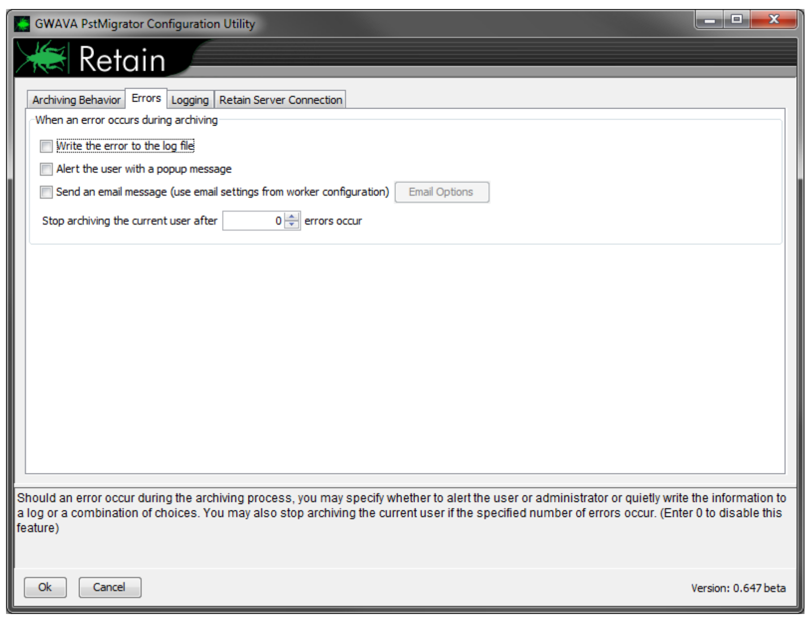
Log files will contain as much information as the administrator desires, from a normal or basic level, to diagnostic.

Select the path for the logging files, whether that is a custom file path, application path (stored in the same folder as the application), or with the application data, (in Retain).

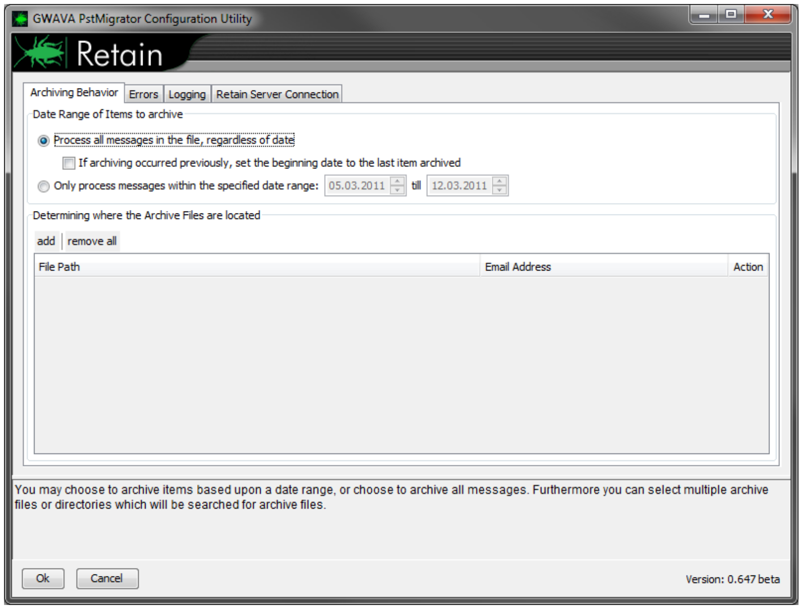
Errors

If an error is encountered, what the migrator utility does with that error is determined by the options configured here. The error may be logged, recorded in a popup message, sent in an email notification, or all three options at the same time.

An error limit may also be specified which determines how many errors the migrator can encounter before ceasing the migration job.

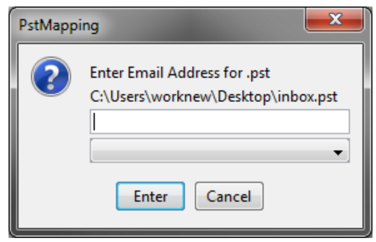


Archiving Behavior

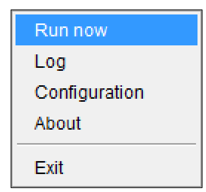


The Archiving behavior tab determines what is archived. If the pst archive file has been partially migrated at a previous time, then the PSTMigrator provides the option to only archive the parts which have not been previously archived.

The PSTMigrator also has the option to only migrate mail according to a set data range. The PSTMigrator will work on all archives listed in the Archive File window. To add an archive file to the migration list, select 'add' and browse to and select the desired pst archive file. After selecting the archive file, the migrator will attempt to access to the archive.



The PSTMigrator may require the email address of the source account in order to achieve access to the archive. Provide the source address.



6. Migrate the pst archive.

   Selecting 'Ok' does not initiate the migrator, it only sets the configuration. To start a migration job, right click on the taskbar icon and select 'Run now'.

7. Wait for the migration to finish.

   The migrator will run as a background service and complete the entire list of archives. If configuration needs to change between archives, migrate the archives separately with configuration changes in-between.

Single Sign On

Single sign on for Exchange comes in two different versions: one which plugs into the Outlook client, and one that works with WebAccess on the Exchange server. Select the version which fills the appropriate need.
Single sign on creates a new entry in the user interface which opens a new window directly into the user's personal Retain archive. This eliminates the need to log into Retain separately from the User's normal mail client.

Exchange Server WebAccess install

The WebAccess plugin installation is simple; run the installer on all applicable Exchange servers and follow the prompts.
The installer prompts for install location and for the URL of the Retain server.

IIS must be restarted. The installer offers the ability to restart IIS automatically.

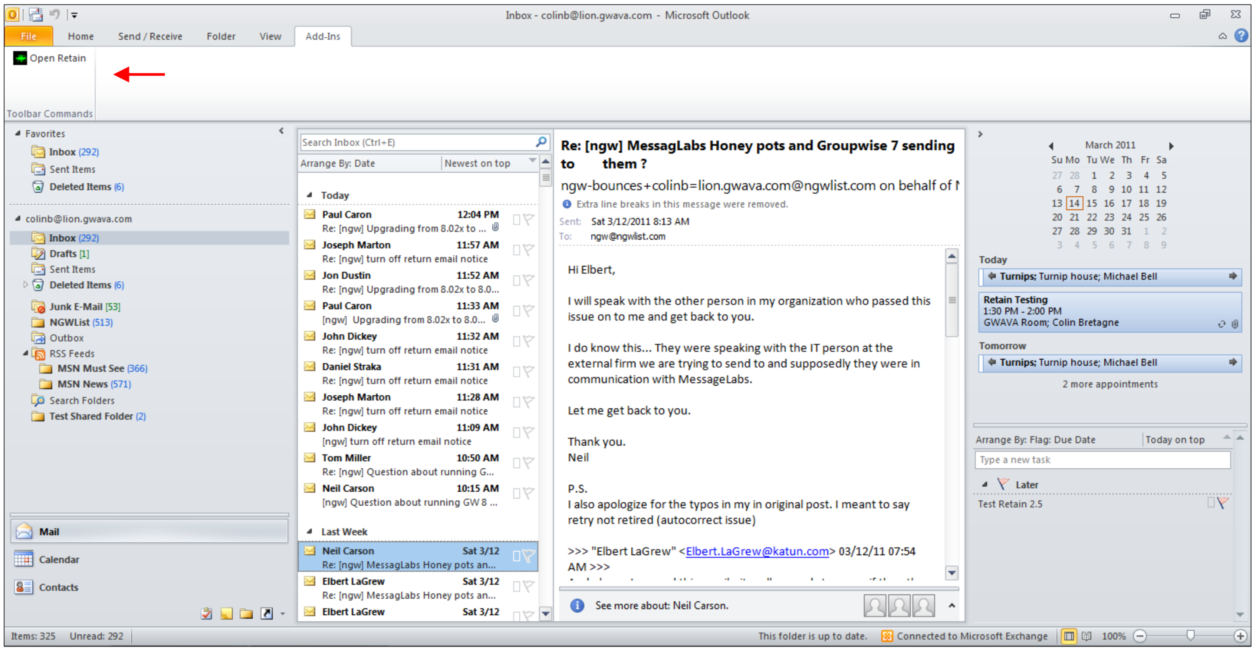
Outlook Plugin

(NOTE: Trial versions of Outlook have plugins disabled; the Retain outlook plugin will not work on trial versions. Outlook 2007, 2010, and 2013 are supported)
The Outlook plugins are essentially the same thing; Single Sign-on plugins for Retain which allows Outlook users to connect to the Retain archive in simply by connecting to their accounts in the Exchange system. Be sure to install the appropriate one for your system.

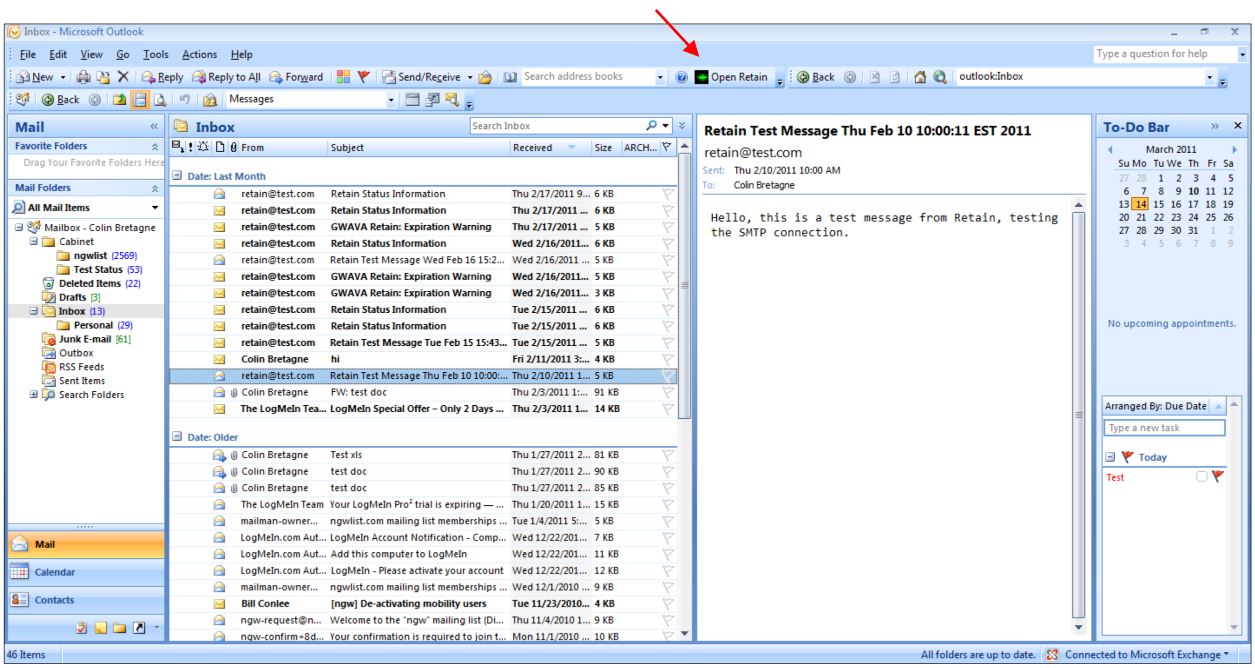
The module requires Outlook configured and currently running, authenticated to and part of Active Directory. For the plugin to work correctly, **administrator rights are required during insta**ll.
Installation is simple, run the setup.exe installer and follow the prompts. Running the setup.exe installer will download and install all necessary and appropriate files and run the .msi as appropriate. An Internet connection to the target workstation is required to download and install the necessary files, (32-bit or 64-bit as appropriate).

Uninstallation is achieved through the Control Panel | Uninstall or Change a Program utility in Windows.

Accessing the plugin is different in each version of Outlook. The Retain plugin under Outlook 2010 is found under 'Add-ins', where Retain has a toolbar button, 'Open Retain'.



In Outlook 2007, the option adds a toolbar button. To access the archive, select the 'Open Retain' button from the toolbar.



Recover Admin
This is an emergency tool you can use if you happen to lose your admin account/password.
This utility will let you create a new admin.
Consult the readme file for further information on its use.

Appendix D – Reload Integration

GWAVA Reload and GWAVA Retain perform very different functions. Retain is an archiving product whose main feature is the storage of data in one place for later search and retrieval. Reload is a Hot Backup, Quick Restore and Push-Button Disaster Recovery product whose main feature is the storage of instances of GroupWise post offices for the purposes of restoring items to their original location in their original form or providing disaster recovery of domains or post offices.
So, why would you want to integrate Reload and Retain?

1. Reload is very good at moving data efficiently from point A to point B.
    a. It copies your post office data in its original form.
    b. It can make what is effectively a full backup by moving and storing as little as 12% of the total amount of data in the post office.
    c. By having the backed up data available in its original form, it can serve as a data source for Retain.
    d. Reload's backups are available the moment the backup job is complete.
2. Retain moves a lot of data and needs strong network links to do so rapidly.
    a. An archiving job moving "everything" will move all of the data. This may seem self evident but when you combine Reload with Retain, you can achieve the same thing by moving only 12% of the data.
    b. If you don't integrate them, you will pull data twice over the link – once for Reload, and once for Retain. On top of that, if you don't have Reload and you only have Retain, you will definitely have to move your data twice.
    c. By integrating Reload and Retain, you can centralize your archives and ensure good backups and achieve a single data pull.

A Brief Review on How Reload Works

No Helper Software Needed.

Reload runs on a Linux server. It does not use agents or helper software on the source post offices to work. In other words, no agents or TSA's are required. Reload simply connects to the server where a post office or domain is stored and then copies the data to its backup storage location.

Backups are instantly available.

Because the data is copied in its original format, the data becomes available as soon as a backup job is complete by simply running a post office agent (POA) against it (for post office backups) or a message transfer agent (MTA) (for domain backups).

Backups Have Little or no Impact on Users.

Because Reload does not use the Post Office Agent to make backups, there is very little impact on users. The POA will continue to run and service users as normal. Reload also does not use TSA software or helper agents on the live post office server. Backups can be made while the users are logged in and working.

Reload Leverages GroupWise's Architecture to Save Bandwidth.

A GroupWise post office is composed of databases and overflow files. Databases contain users' mailbox layouts and indexes and other databases contain users' authentication information. For any GroupWise item exceeding 2KB in size, such as e-mail with attachments, overflow files are stored, commonly called BLOBs (Binary Large Object).

While the contents of the databases changes almost constantly, the BLOBS are static. Therefore, in a Standard Backup, Reload grabs the databases in their entirety but only those BLOBS that have been newly created since the last backup.

Generally, the BLOBs take up almost 90% of the space occupied by the whole post office. Therefore, with a standard backup, Reload can get away with copying only 12% of the data – the databases and only those BLOBs which have recently been added. For those BLOBs that have been backed up in prior backup instances, Reload links to a master backup directory, taken the first time a backup was run, using a Linux feature called symbolic links. A symbolic link is like a Windows shortcut except that it looks, feels, and acts like the real thing.

This is how Reload can achieve VERY fast backups. In addition, using Reload to move data will save tremendously on network bandwidth compared to traditional backup systems which grab all of the data.

Backups Can be Made of Backups Allowing Centralization and Redundancy

Reload was made to backup live post offices and domains and it can also make backups of other Reload backups. The following two cases can help illustrate how useful this can be:

Consider client "A" who has two physical locations, one post office in each. This client wants redundant backups – a primary backup plus a secondary in case the primary fails.

This client installed a Reload server in each location. The servers backed up the local post office in addition to making a backup of the Reload server in the other location. Thus, each Reload box effectively had backups of both servers.

Consider client "B" who has one central data center and four branch offices. This client wants the head office to have backups of all post offices in all locations.

Branch offices 1, 2, and 3 have fast WAN links to head office but branch office 4 has a very weak connection to head office. However, branch office 4 has a strong WAN link to branch office 2.

So the client installed a Reload server in each office and one in the head office. The Reload server in the head office was set to back up the Reload servers in branch offices 1, 2, and 3. For Branch office 4, the Reload server in Branch office 2 was set up to back up the data from the Reload server in branch office 4 and then the head office was set to back this data up from the Reload server in branch office 2.

Thus, backups can make as many hops and can be backed up in as many places as you need.
Using the ability to backup one Reload server with another, you can achieve data centralization and redundancy. The redundancy also gives you the ability to use Reload for off-site disaster recovery.
Additionally, for client "B", their old backup system moved all of the data every day. Using Reload, they managed to cut their network traffic by 88%.

How Retain Takes Advantage of Reload's features

Consider client "B" from the earlier example who has four branch offices and a head office. They want their Retain Server to be located at head office. So they need to centralize their data.
Without Reload, they would have Retain Workers on the branch office POA servers and the data would be sent over the WAN links. For a data collection involving "everything", all data would surely saturate the WAN links.
Plus, their backup/restore software would use the WAN links too, if they were centralizing their backups.
Adding Reload to the mix, they are able to achieve huge bandwidth savings and performance gains.
Reload would be set up to centralize the data to one Reload server in head office, saving immediately 88% of their bandwidth compared to their existing backup/restore system.
Next, A Retain Worker would be set up on the central Reload box to draw data from all backed up post offices.
One Retain Worker can only run one job at a time, so the post offices would be archived one at a time.

Multiple Workers on One Server

It is possible to install more than one Retain Worker on one server but this would double the hardware requirements, Tomcat memory tuning, and is limited to Linux as the platform OS. This option is built into the Linux installer and is activated by using the 'addworker' switch to the install command. (I.e. ./RetainInstall.sh addworker)
You would normally only add additional workers if you wanted to dredge more than one post office at a time.
On a Reload server, it might not be so time critical to dredge the post offices on it since there is no impact on the end users. On top of that, Reload has a special feature made especially for Retain, a special post office agent that stays up all the time, except to move to the latest backup. This way, it is always available to Retain.
So you will have to decide if it is acceptable to have the post offices dredged one at a time or if you would prefer to dredge many at a time. To do many at a time requires multiple workers.

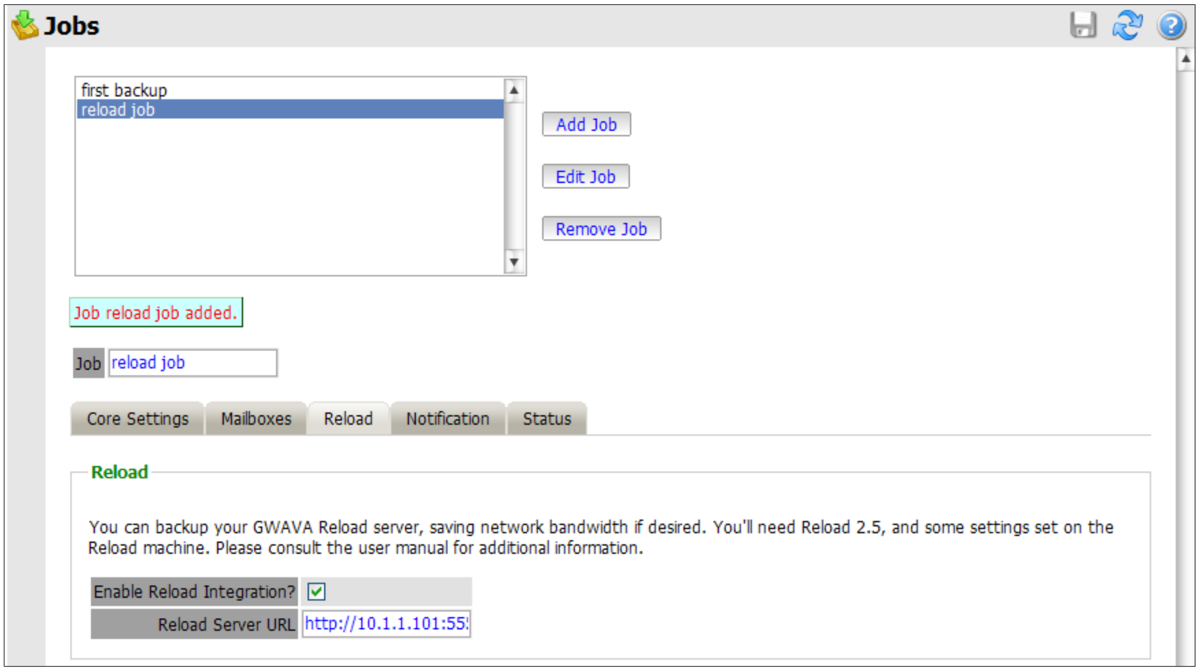
Timing

It's important to time the data collection on Retain so that the Reload backup will be complete long before the Retain job is scheduled to start. This is set in the schedule section under the Data Collection menu in Retain.

Retain Settings

The three tasks to configure Retain to work with reload are to assign the reload password for the worker, assign the running jobs to use the Reload integration, (this setting is found in the Jobs configuration page in the Retain management console), and configure the Profile to use the Item store flag for duplicate checking.

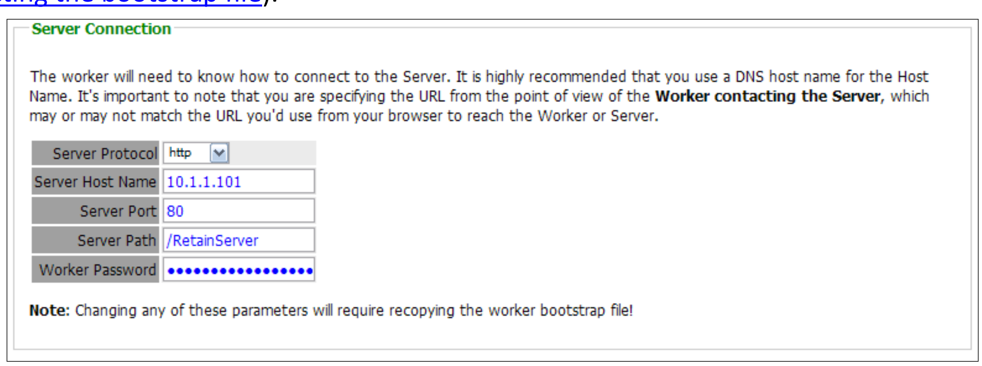
Enter the management console, and select Jobs from the Data Collection menu.



Create or select a job which you desire to use against the Reload system, and select the Reload Tab. You must select the Enable Reload Integration option, as well as supply the correct connection address for the Reload Server URL. (Both IP address and DNS name will work, but DNS is recommended wherever possible.)

Set the rest of the Core Settings, Notification, and Status as you would normally for your Retain system, but note that in the Mailboxes section you MUST assign the mailbox that Reload is backing-up. Save the changes.

To specify the Reload –Retain password to the worker, open the specified worker in the worker settings page, and click on the Connection tab. Specify the new Worker Password by entering it into the provided field and then click 'Save changes' in the top corner of the page. **You must re-upload the bootstrap file to the worker after creating a new password.** (See the worker section to get instructions on correcting the bootstrap file).



How to Setup Reload to work with Retain

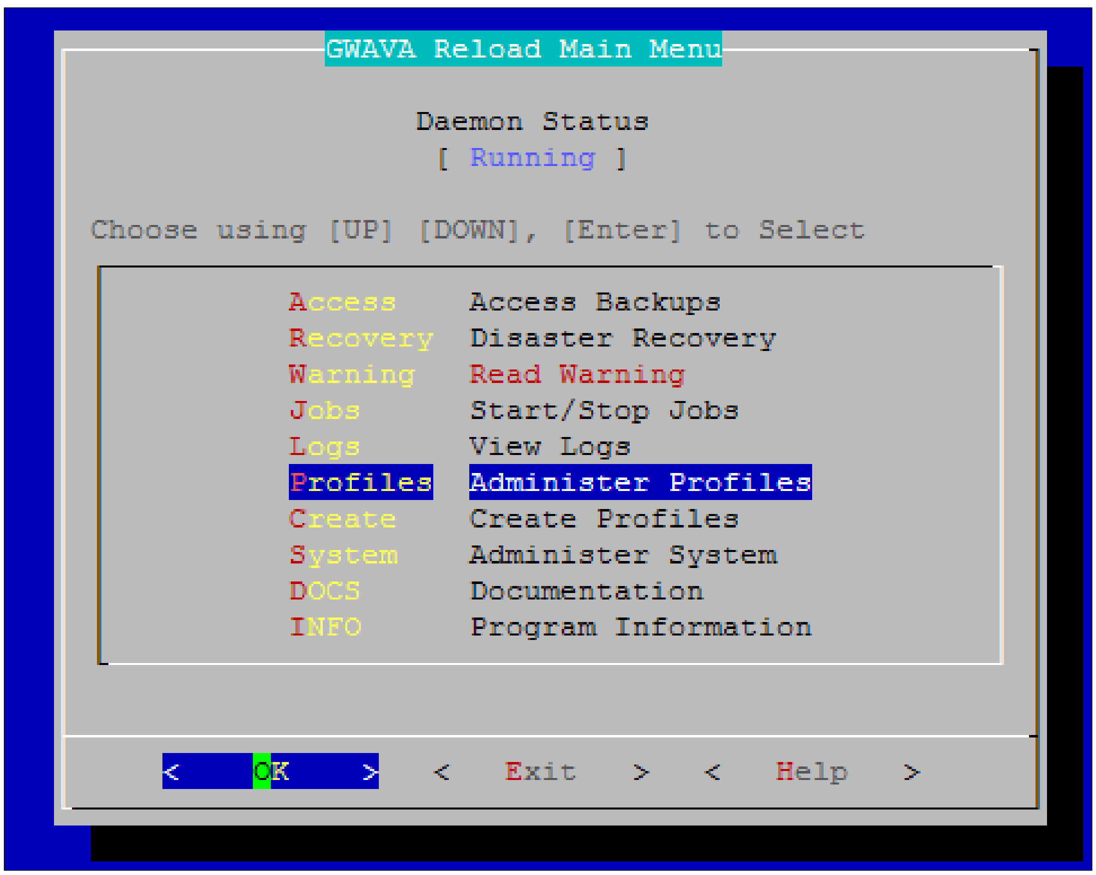
This part assumes that you have already set up and configured one or more Retain workers to collect data from your Reload box.

First, Reload must be set up so that the backups are available. There is a special feature in Reload for this. It calls up a post office agent that stays up all the time and it only goes down long enough to change to the most recent backup. So it will always be there with very small interruptions as the POA is brought down then up.

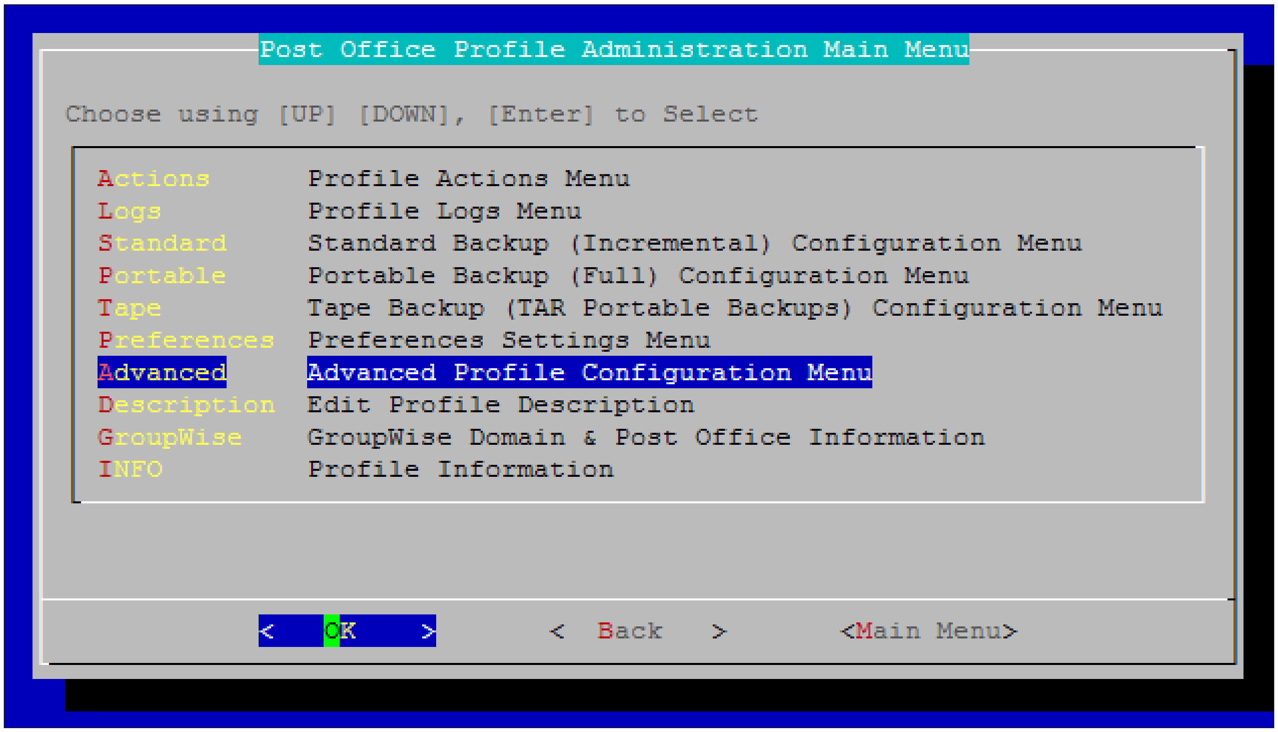
Setting up Reload is done on a Profile-by-profile basis. Each post office that you set up for Retain to dredge from must be configured within the profile configuration menu.

1) Start up Reload's Administration menu.

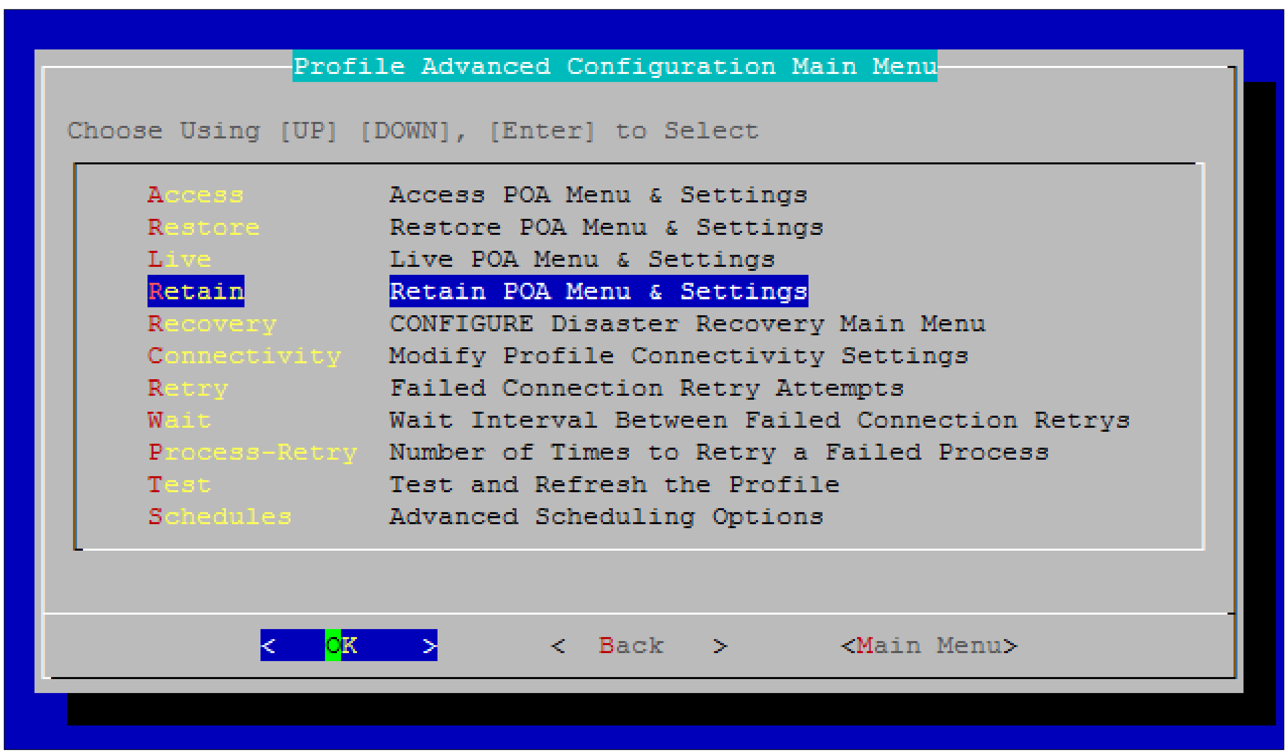
2) From the main menu, choose Profiles – Administer Profiles.

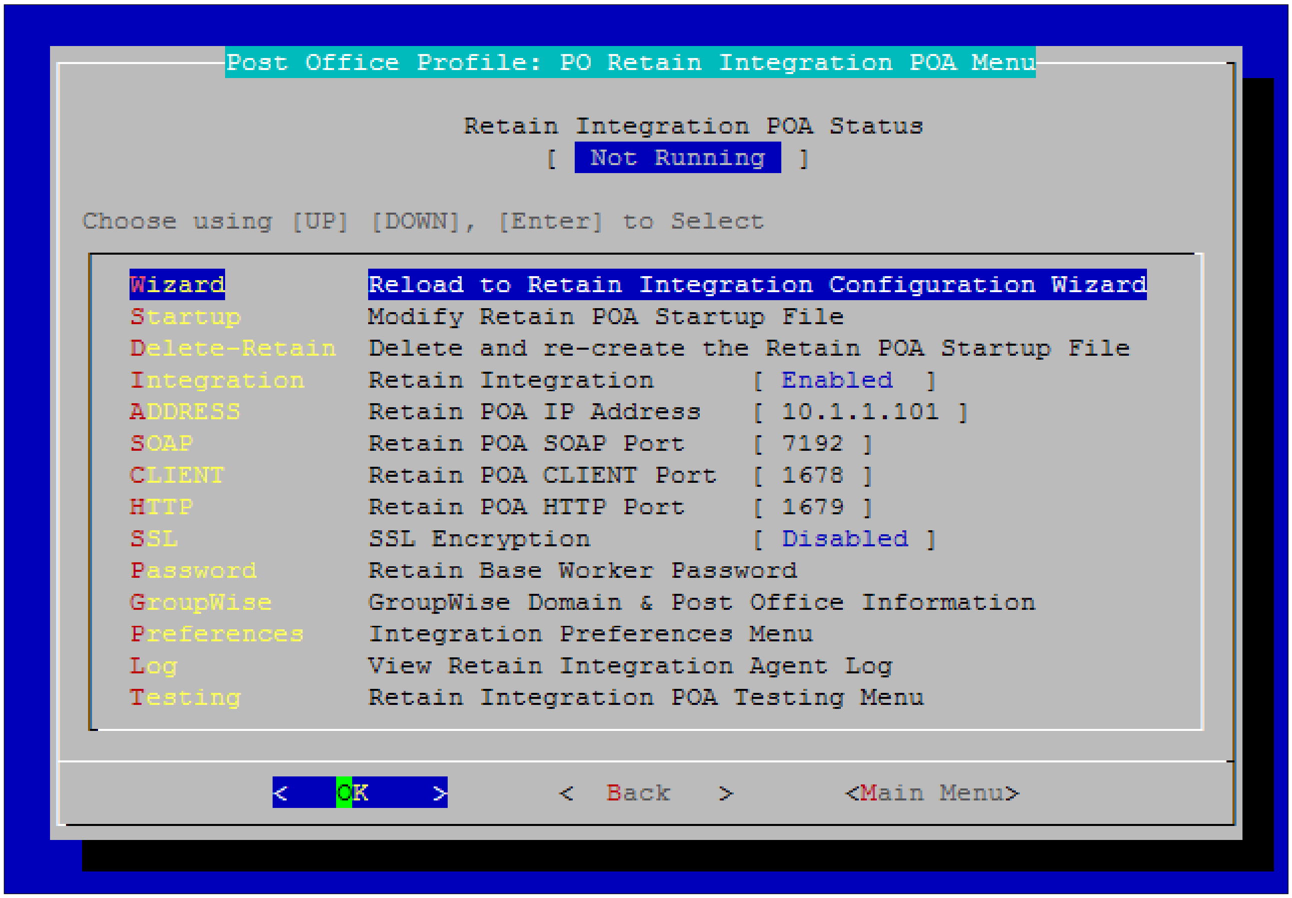


3) Choose Advanced Profile Configuration Menu



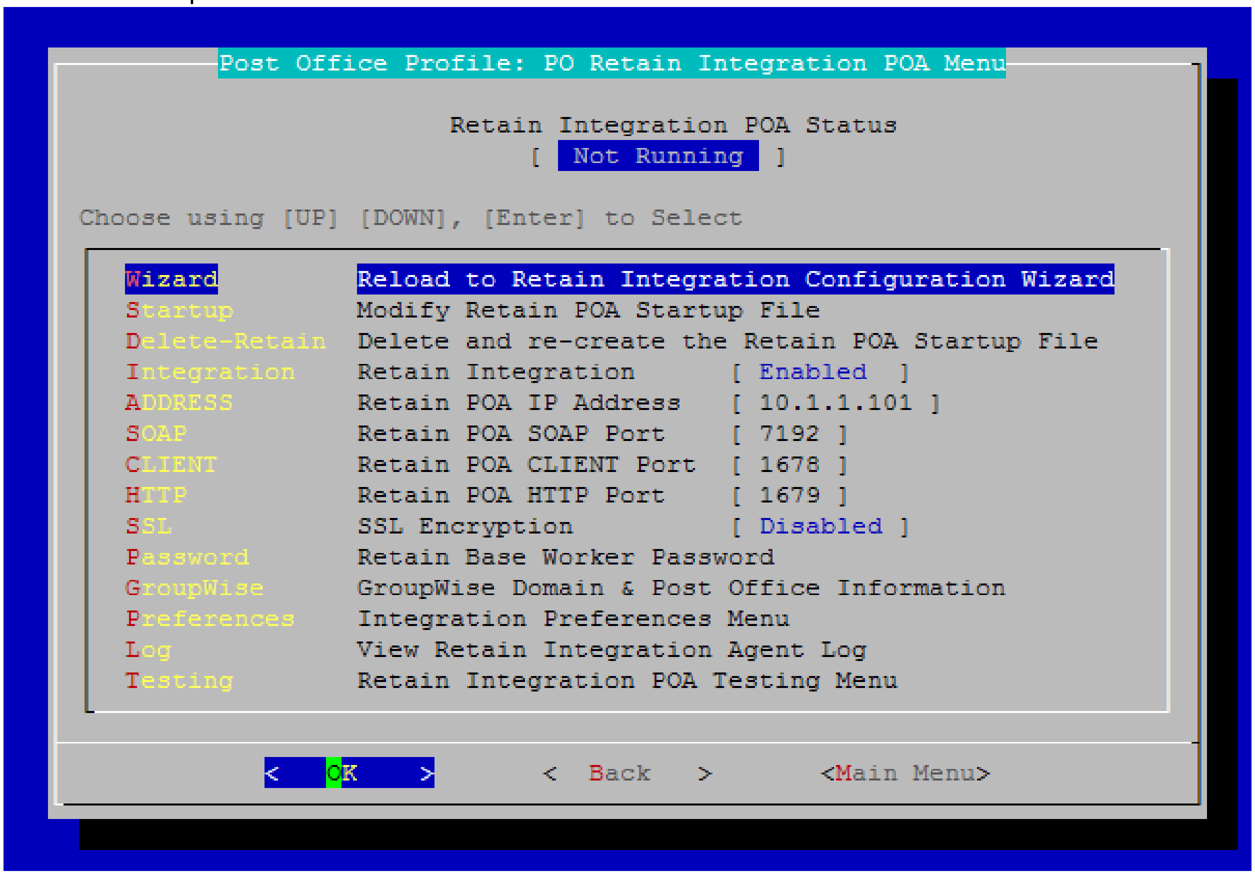
4) Choose Retain POA Menu & Settings





Now it's worthwhile examining this menu. It contains all the settings you will need to make the Retain integration work. This will be a new post office agent running and it will not interfere with the POA being used to access, backup or disaster recovery. Thus, the settings NEED to be different. The easiest way to start is to run the wizard.

Here is another shot of the configuration screen after running the wizard. You will see sample settings and the menu options will be described below.

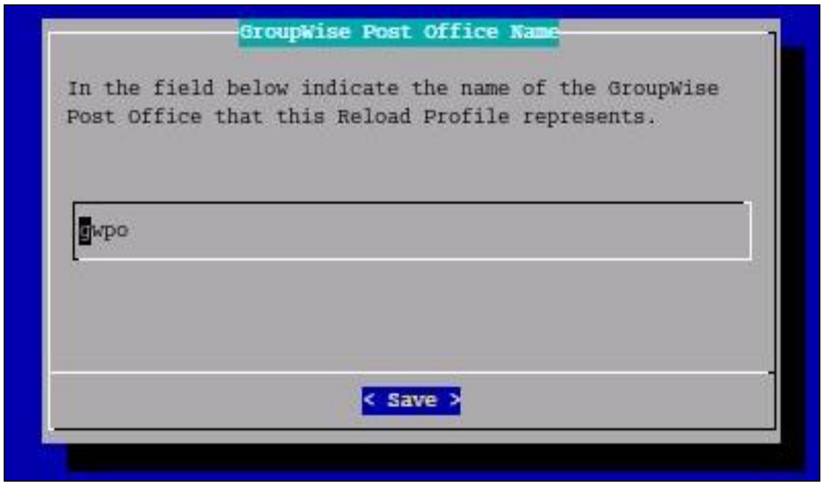


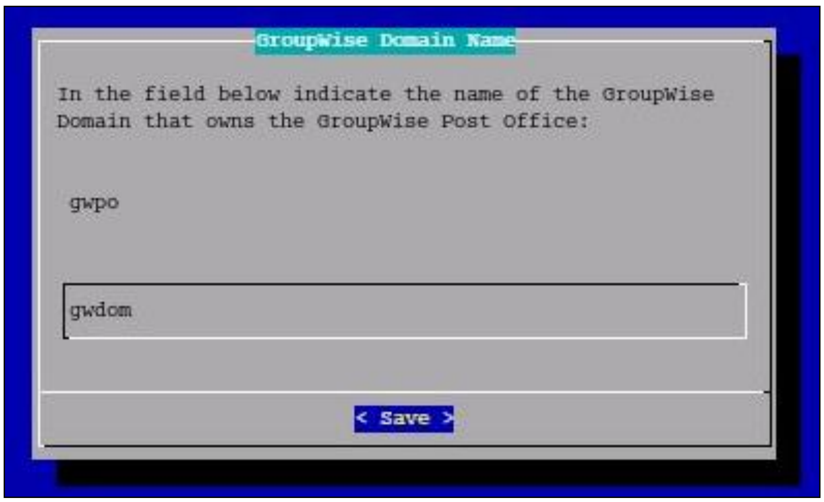
At the top, the status of the Retain Integration POA is displayed.

- Wizard: Run the configuration wizard.
- Startup: modify the startup file for the POA if you want to make specific changes to it.
- Delete-Retain: delete the startup file if you want to start fresh and configure from default.
- Integration: Enable or disable the Retain Integration
- Address: The IP address this POA will listen on.
- SOAP: The SOAP port this POA will use.
- CLIENT: The port that a GroupWise client may use to access this POA.
- HTTP: The HTTP port for this POA.
- SSL: Enable or disable SSL (Generally keep SSL Disabled)
- Key: A password Retain will use to access this POA.
- GroupWise: Specify the domain name and post office name for this POA.
- Log: View the Integration Agent Log.

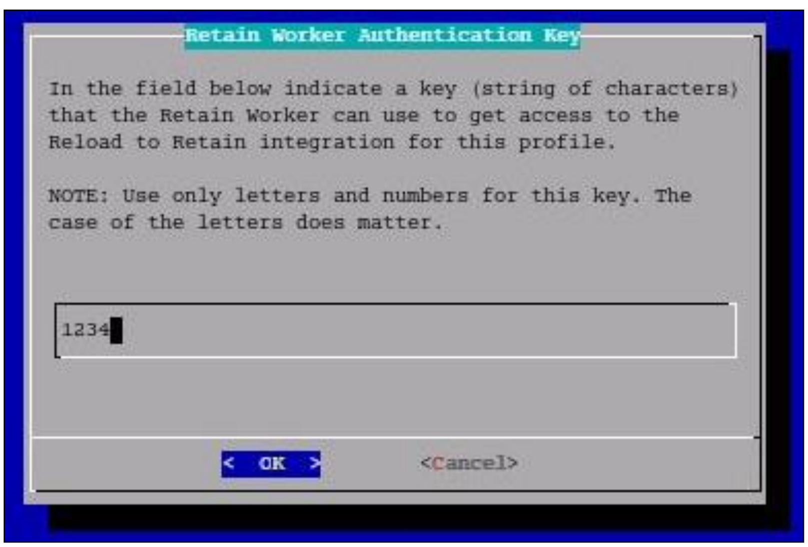
The wizard will be shown below.

1) Run the Wizard

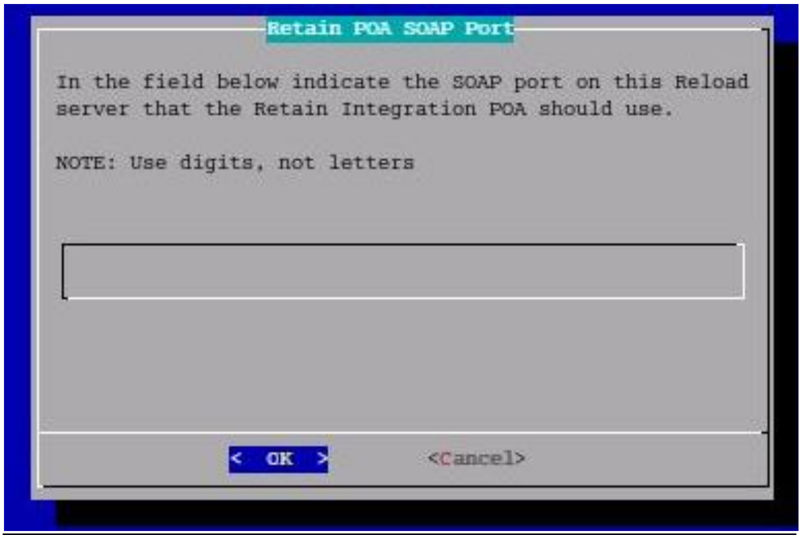


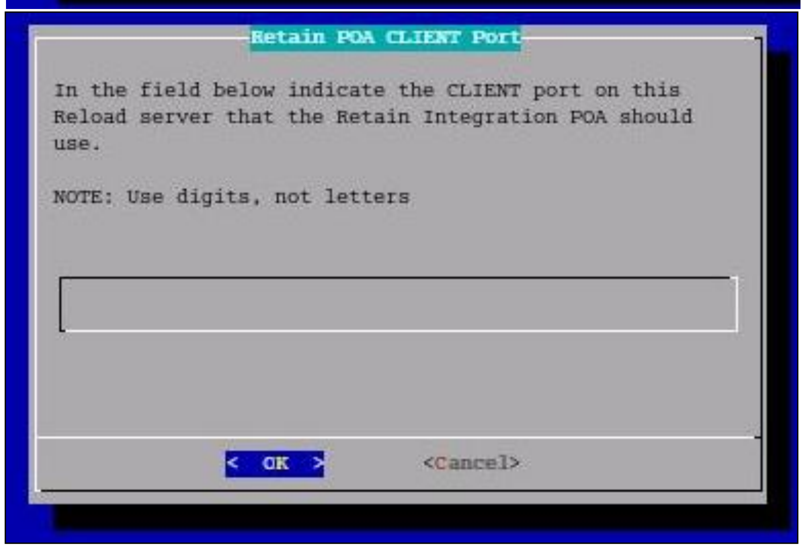


2) Enter the name of the post office and domain.

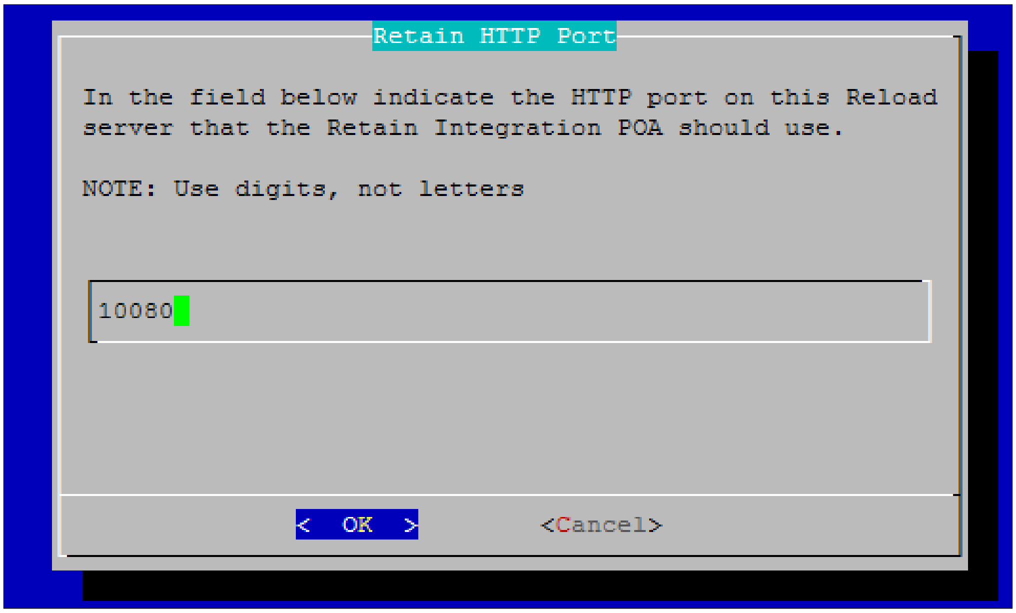


3) Choose an authentication key that Retain will use to access this POA. **This must match the password you assigned to the Retain Worker.** (See the Retain Settings)





4) Specify the IP address and SOAP port for this POA. **Be sure it is unique.** Some will choose one IP for the whole box with different client ports and SOAP ports for each POA. Others use the same ports but the IP addresses are different.



5) Choose the HTTP port for this POA.

Because Reload is creating a faux POA for Retain to archive mail from, the Reload POA must be on a different or unique port, so there is no conflict with your original POA. If your Reload installation is on a separate machine from your POA, any port will do, but if it is the same, pick a port that you know is open, different from the live system.

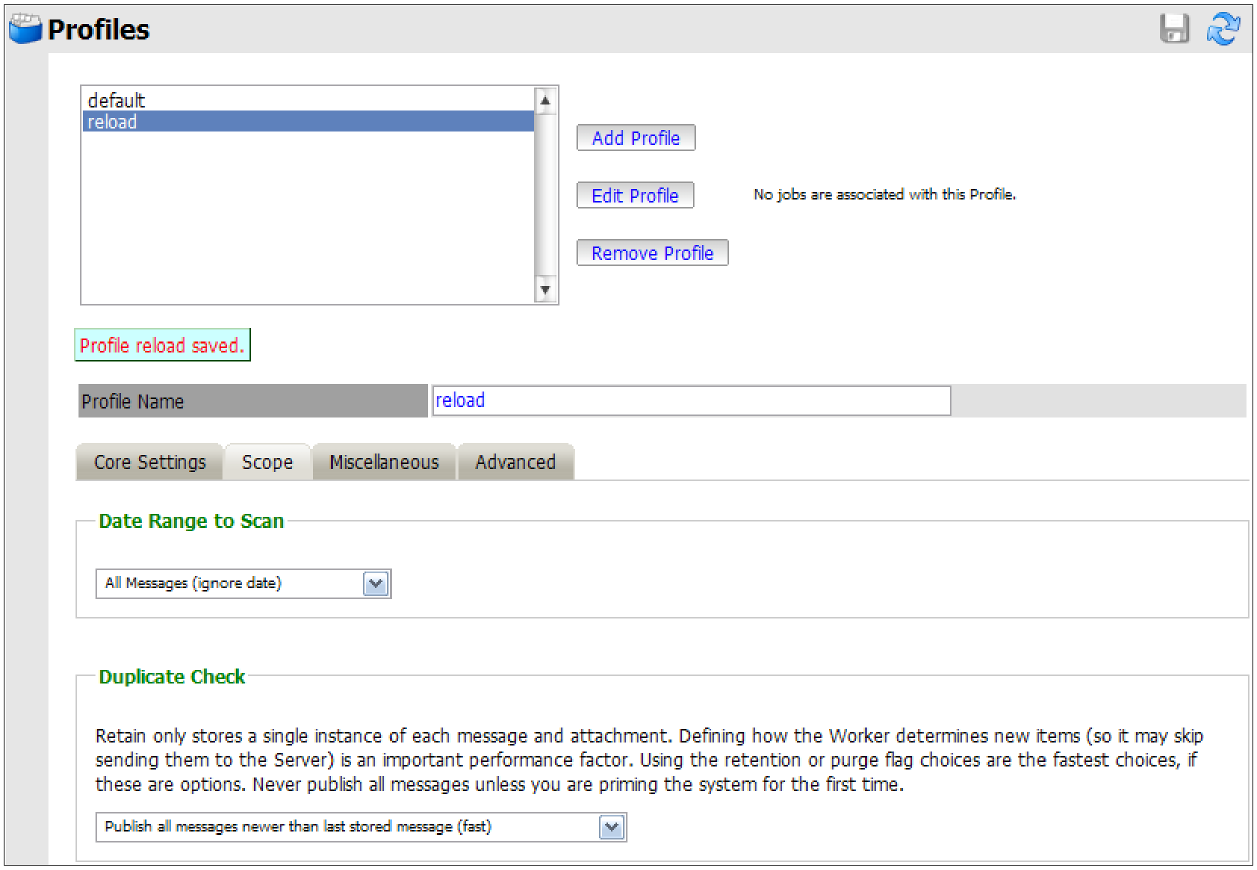
Retain will pull all necessary connection information from the Reload server. There is no need to enter these settings into the Retain Server.

Now that you have set up the basics, you may edit the POA startup file in case you wish you change any other settings, (Retain.poa), or you can re-run the wizard from step 1.

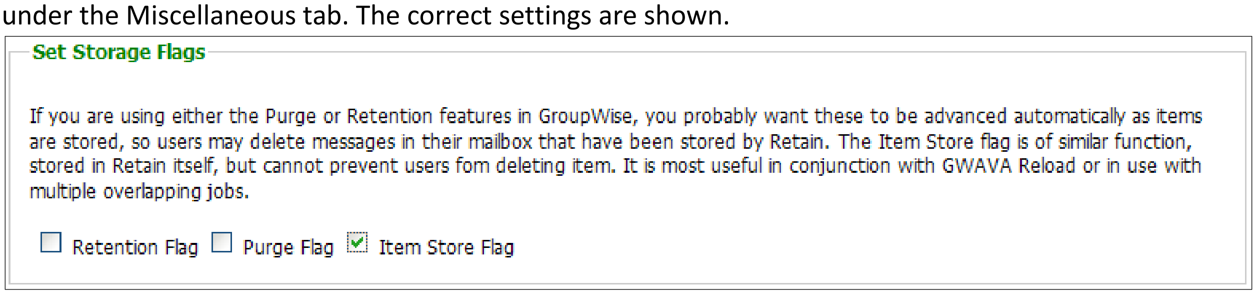
IMPORTANT Notes for the Integration

Retain

Because Reload essentially creates a snapshot of the Post Office, the duplicate checks that Retain can use are very limited. The retention flag and purge flag will not function as they are kept within GroupWise and would be changed back as soon as Reload creates a new backup. **The Item Store Flag is the only duplicate check that is internal to Retain, and is the ONLY duplicate check ability that will work when Retain archives against a Reload system.** Again, the retention and purge flags will not work but the item store flag will. Be sure your Retain Profile matches this setting.

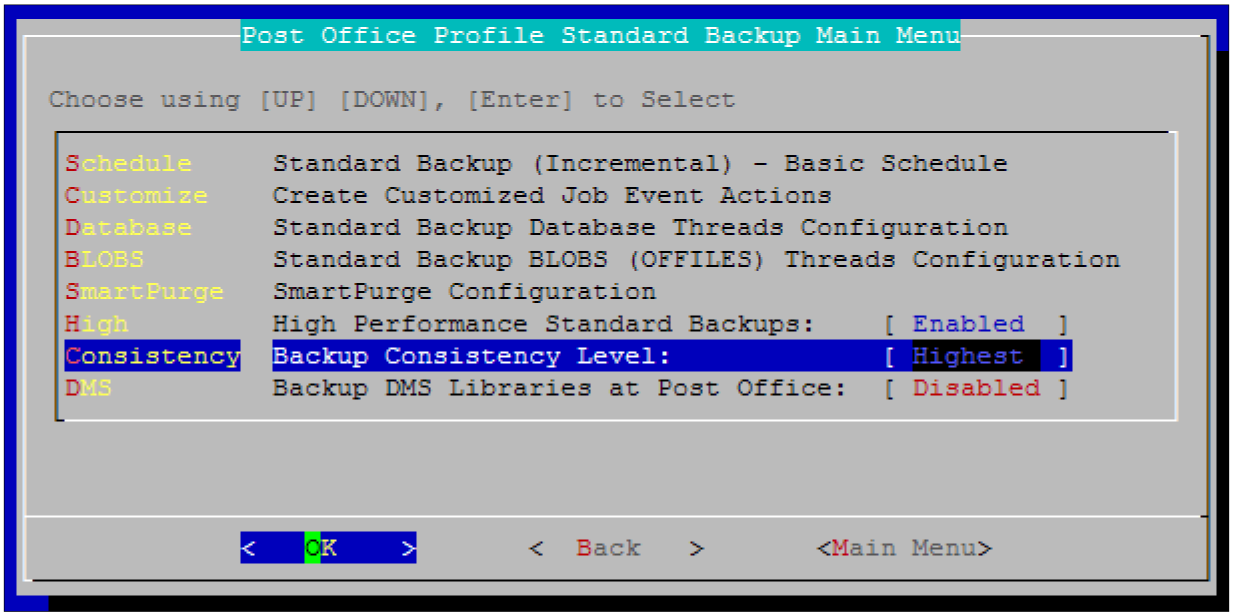


The item store flag is set in two places: Duplicate Check under the Scope tab and under Set Storage Flags under the Miscellaneous tab. The correct settings are shown.



Reload

To mitigate the chances of getting Retain Worker archive errors while working against a Reload POA, it is *STRONGLY recommended* ***that Reload is set to create highly consistent backups.***
This setting is located at:
Main menu > Profiles (Administer Profiles) >Standard (Standard backup (incremental) Configuration Profile) > Consistency (Backup Consistency level): Set to highest.



This is enabled by default for new installs of Reload 2.5, but will have to be manually enabled on systems that are upgraded to Reload 2.5 You want a highly consistent backup, to make sure that you have all the blobs associated with the database. Database is picked-up first, so the blobs that are referenced in the database will be consistent with the current backup.

Appendix E – Migrating Retain to a new Server or Platform

Migrating Retain between different platforms is possible, though time consuming. Retain can also be migrated between 32-bit and 64-bit systems. Migrating or moving the Retain Server can be complicated, because the different Retain components that connect to theRetain server by IP address, file paths mapped in the system, and the unique server identification which allows access to the data storage are all tied to the originalRetain Server. The important variables for theRetain Server are found in the ASConfig.cfg file. The connecting components will need new bootstrap files. In a migration, all these variables must either be corrected, or copied to the new system for the migration to be a success.

There are **no guarantees** when migrating a server. **BE SURE TO CREATE A FULL BACKUP WHEREVER POSSIBLE BEFORE STARTING THE PROCEDURE.** SQL databases and data storage systems are not supported or administered by GWAVA Inc., and are the responsibility of the local system administrator and the customer.

Regardless of the source and destination platform, the main steps will be the same. The steps for migrating aRetain Server are:

1. Create a backup of the server, data store, and database.
2. IF the SQL database is housed on the source Retain Server, copy or migrate the SQL database to its final destination in accordance with recommended practices for the respective SQL system. Setup the SQL server and get it running on the destination machine.
3. Download and install Retain. After Retain has been installed, shutdown Tomcat.
4. Copy the data store to the new destination. The data store consists of more than just the storage directory. The data store contains the configuration database, indexes, backups, license, and the archive, (if not on a SAN). If migrating to Linux, the ownership and execute rights to the data store **MUST** be changed. If ownership execute rights are not set correctly, the Retain Server will not function correctly, and will generate inexplicable errors. Commands are:
```
chown –R tomcat:www  <storage_directory>
chmod –R u+rwx <storage_directory>/*
```
5. Open the ASConfig.cfg file from the old server with the text editor of choice. (Text editor must be able to view .xml files.) The following file paths which were mapped for the original server must be corrected for the new server:
```
<serverID>unique_server_ID</serverID>
```
It is ESSENTIAL that the ServerID setting be identical to the original server ID, or the migration will fail.
```
<basePath>/retain</basePath>
 <archivePath>/retain/storage</archivePath>
 <xmlPath>/retain/xml</xmlPath>
 <indexPath>/retain/index</indexPath>
 <backupPath>/retain/backup</backupPath>
 <licensePath>/retain/license</licensePath>
 <EBDBPath>/retain/ebdb</EBDBPath>
```

Ie. If migrating from Windows to Linux, the `<basePath>` would need to be changed from: `<basePath>C:\retain</basePath>` to `<basePath>/retain</basePath>`

6. When the ASConfig.cfg file has been modified correctly, copy the modified file into the destination server. ../RetainServer/WEB-INF/cfg
   Once the file has been copied into the new server, start Tomcat.
7. Verify that theRetainServer is working. If it is not working, view errors and double-check the settings in the ASConfig.cfg file.
8. IF the final destination server has a different IP address than the original RetainServer had, all workers and stubbing servers must be reconfigured by re-uploading new bootstrap files for each one. If this step is not completed, the workers and stubbing server will not have contact with the Retain Server, and will not be able to function. See 'correcting the bootstrap' in the worker section.

The process should be done with extreme care and attention to detail, if not under the supervision and by the guidance of Retain Support. Completing ALL steps for your system is extremely important. If there is a problem call support and/or revert to the backup made in step one. Correctly following these steps will result in a fully functioning system on a new platform.

Appendix F – Switching the Indexing Engine

Switching between indexing engines is possible, though frequent changing is not recommended as it is a time consuming process. This guide assumes that the system will be switched from Lucene to the more robust Exalead indexing engine, though the process is nearly identical for the switch back to Lucene, it simply requires selecting 'lucene' instead of 'exalead' when the options are provided, as the positions of Lucene and Exalead are reversed when switching from Exalaed to Lucene.

Switching the indexer to Exalead

The Exalead indexing engine is not required, and the system can be switched from Lucene to Exalead at any time. However, the index engines are not compatible with each other and have no way to export the indexes between them, causing a need to re-index the entire mail archive each time the index engine is changed to ensure full coverage. Re-indexing the archive will take substantial amounts of time, and switching the indexing engine should only be run during a 'quiet time' when there are no jobs scheduled to run.

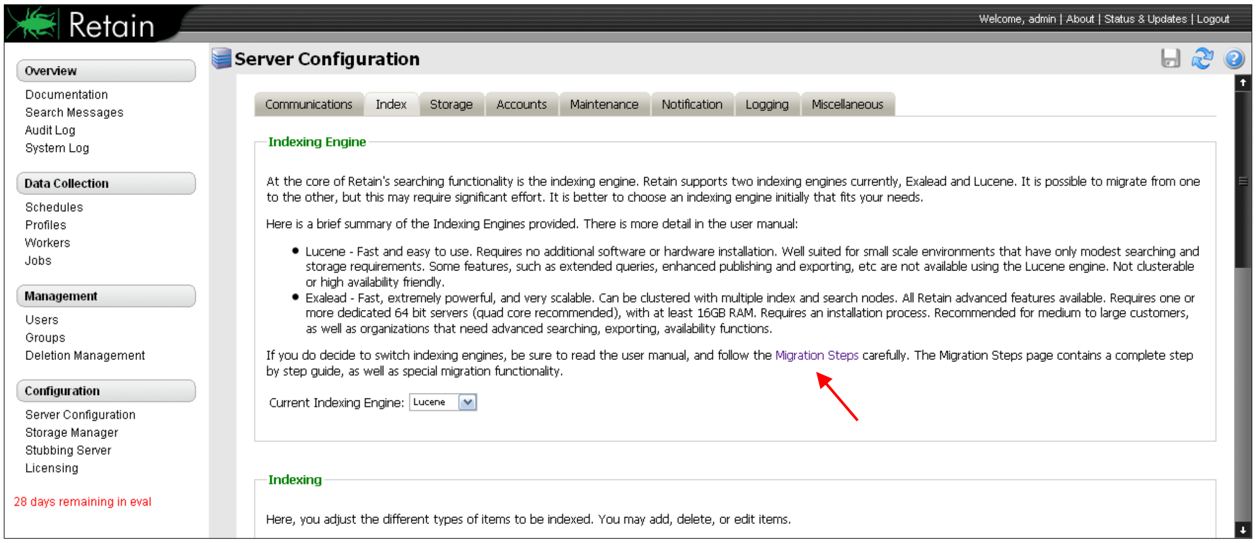
Exalead allows much more flexibility and options in searching and scaling. However, Exalead does require a separate physical machine with robust hardware. For a full list of Exalead requirements and install instructions, see the Exalead Install document. Switching to the Exalead indexing engine will cause some server downtime.

Before you begin the migration to Exalead for the indexing engine, you must first have Exalead installed and working. Log into the Retain Server management console as Adminitrator, and ensure that:

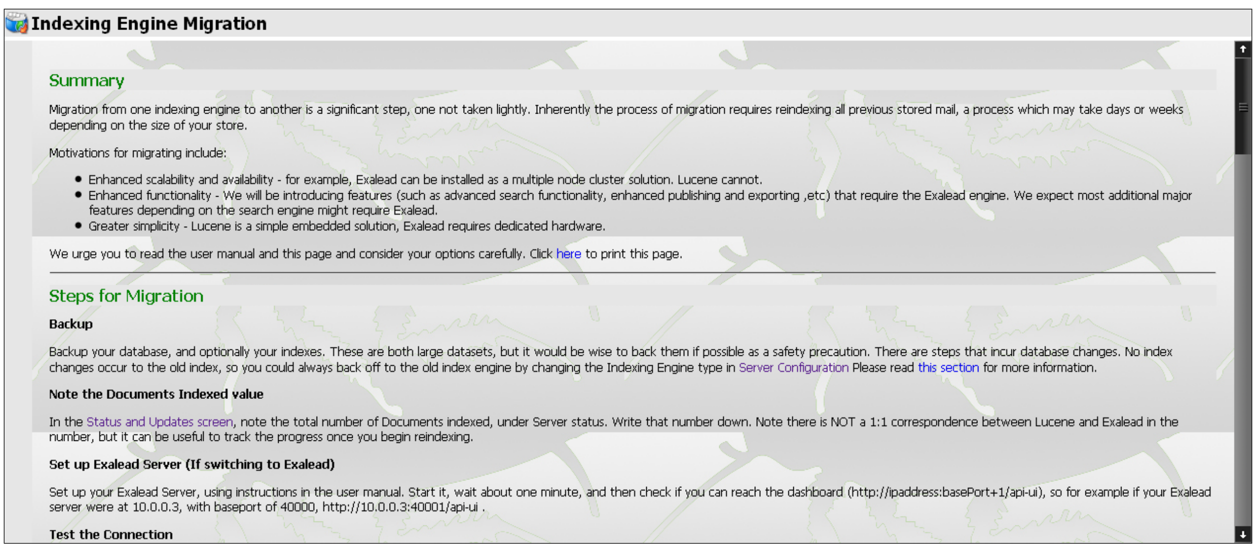
- The Retain System has been backed-up.
- Exalead serer has been Installed, setup, and is accessible .
- No deletion manager jobs should be running, or set to run.
- Indexer status is set to '0'. On Retain Server status page, the "Total emails in memory queue awaiting indexing" should show '0'. If this is not set to '0', and no job is running, contact support before performing the index engine migration.

From this point on, actual changes will be made in your Retain Server system. To change the index engine, perform the following steps

1. As admin, log into the Retain Server management console and browse to the **Configuration | Server Configuration** page and select the **Index** tab and click on the 'Migration Steps' link to spawn the migration steps window.

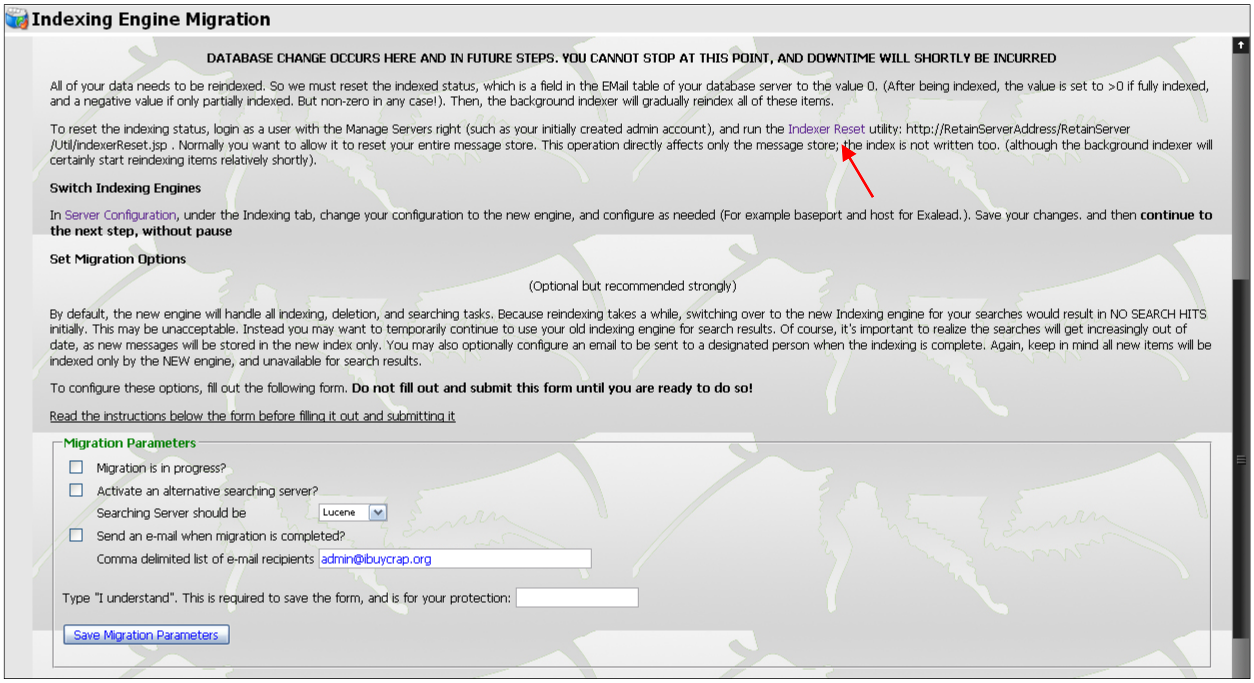


Open the migration link in a new window or tab.



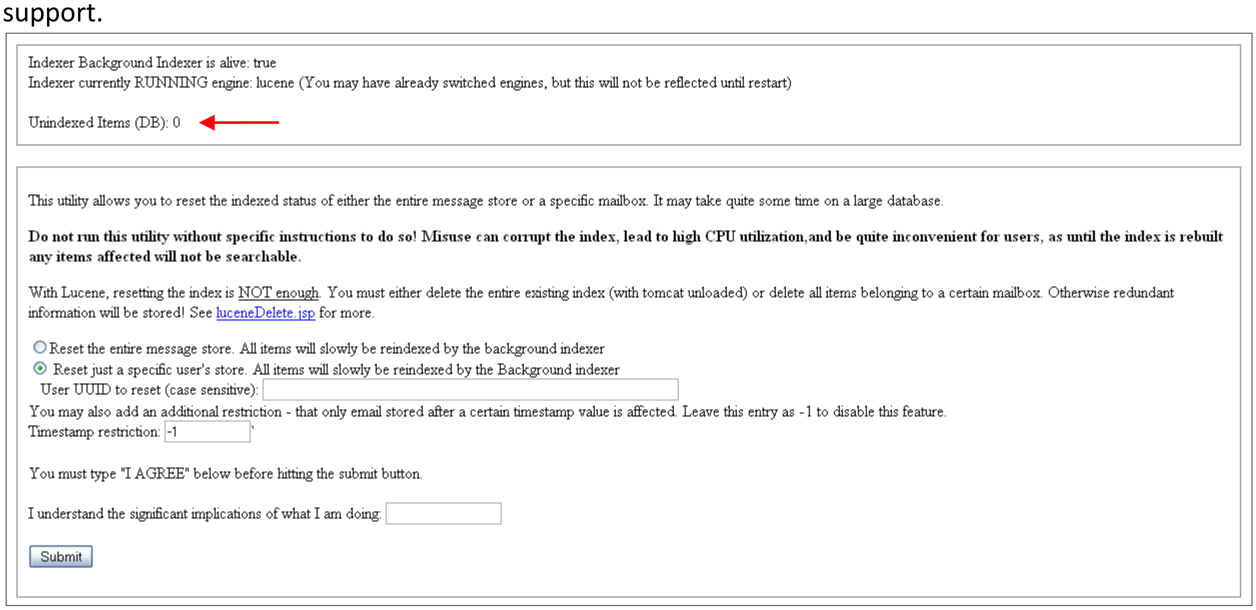
This window has links and information on the migration as well as the migration settings further down the page. LEAVE THIS PAGE OPEN.

2. Scroll down the page to the link to the Indexer Reset page.



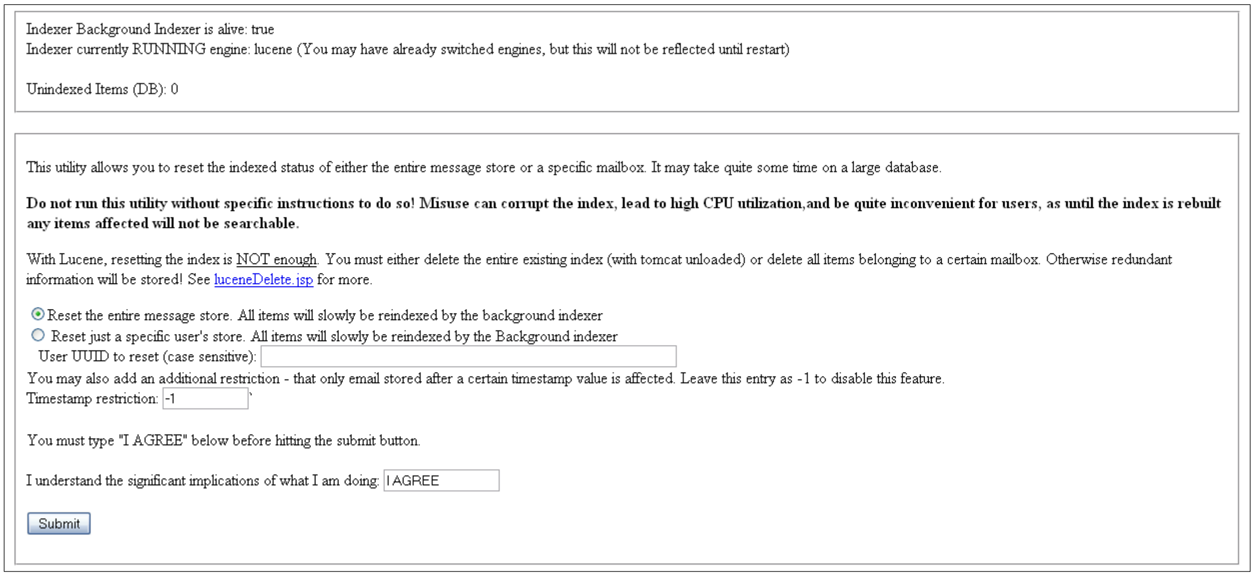
Open the link in a new page or tab. http://RetainServerAddress/RetainServer/Util/indexerReset.jsp

By default, the Indexer Reset page should look like the picture below. (Pay attention to the Unindexed Items (DB): number. It should read '0'. If it does not, do not proceed unless under the instruction of support.



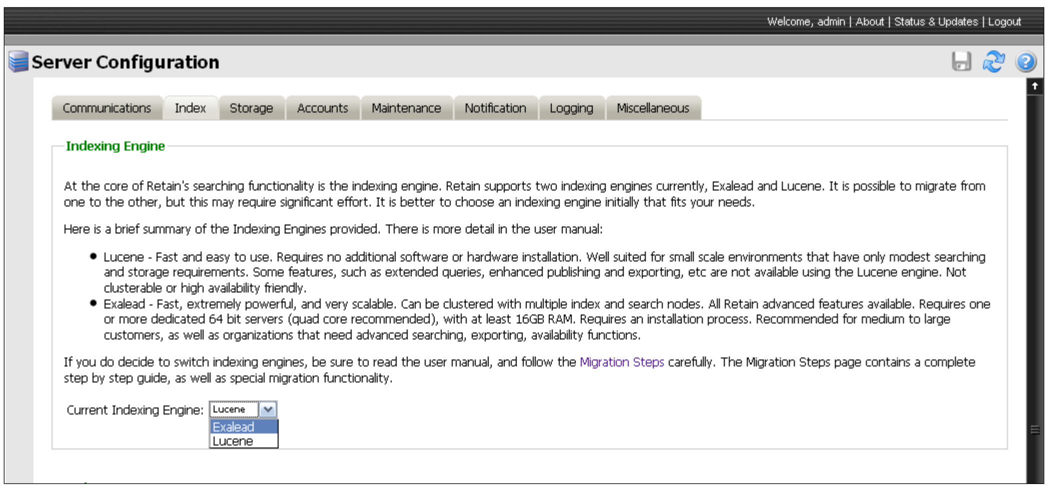
The next few steps need to be performed with little time delay between them. No more than a couple minutes. If not switched soon, the indexer reset switch will cause Lucene to re-index, instead of causing Exalead to index the message store, resulting in empty search results when switched to Exalead and slow responses due to Lucene re-indexing the message store. Read through the next steps and decide settings before proceeding. These steps must be completed in the order specified.

3. From the Indexer Reset page, Select **Reset entire message store**. Type "**I AGREE**" in the dialog after reading the warnings. Select **Submit**.

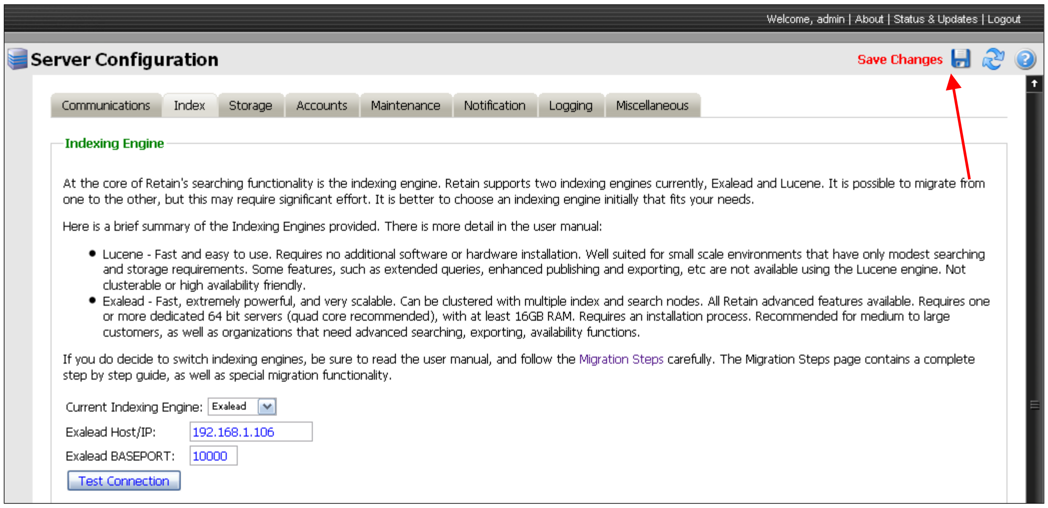


Proceed **without delay** to the next steps

4. THIS STEP MUST BE DONE QUICKLY AFTER RESETTING THE INDEX. Go the server configuration in the Retain Server admin page, and switch indexer engine to 'exalead'.



After selecting Exalead as the indexing engine, input the connection information (IP address and base port, the default base port is 10000).



After all changes have been made, select the **Save Changes** button.

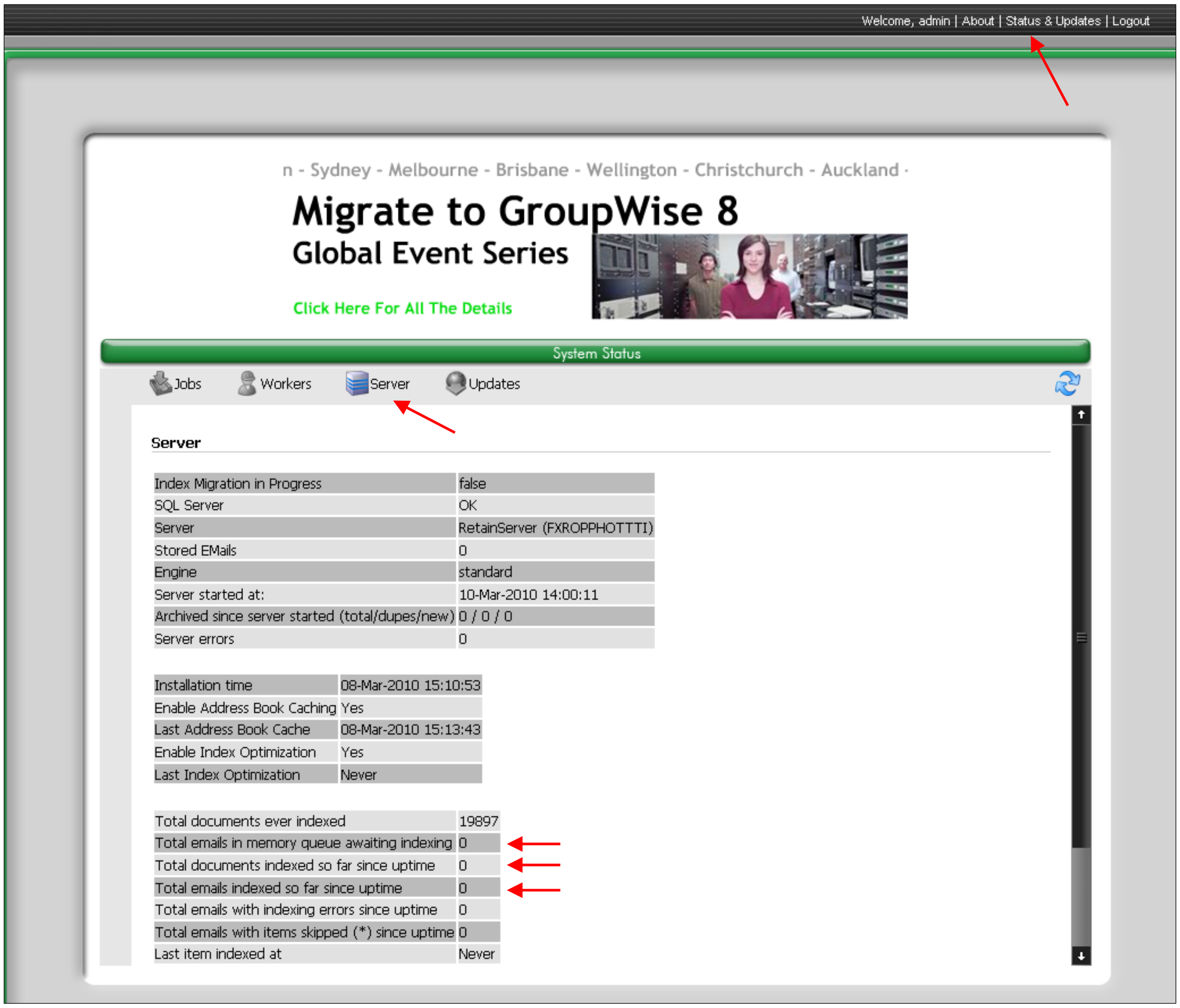
5. Go to the **Migration Steps** page and Select, migration in progress, and select to **Send an e-mail when migration is completed**. Specify a destination address.

6. Activate an alternative searching server if desired.

While Exalead is indexing the archive, there will be no mail in the index to be searched through. Depending on how much mail is in the archive, the indexing operation may take a very long time. To have the searching features of Retain available while the archive is processed, specify a separate searching server. In this case, it would be Lucene. The only downside to this operation is that any new mail added to the system during the indexing operation will not be added to the Lucene index, and will not be available to search until Exalead has finished and the search engine has been changed to Exalead.

7. After the settings are correct, type "**I understand**" and select **Save Migration Parameters**.
8. Restart Tomcat on the Retain Server system. When Tomcat starts back up, the settings will be cemented and the archive will be re-indexed into Exalead.

   During the indexing process of Exalead, the statistics of the Retain Server Status and update page should rapidly increase. It is one way to monitor the progress of the migration. (The screen shot shown is before the migration is started.)



9. When the migration compete email arrives, return to the Migration Steps page and unselect the **Migration is in progress** setting, type **I understand,** and **Save Migration Parameters**.

Even though Lucene has been unselected, it will still exist with all the indexes until removed. Again, Re-indexing may take a long time depending on the hardware of the Exalead system, the size of the archive, and the speed of the connecting network. Allow for plenty of time for the indexing to be performed. Time may range from several days to several weeks for extremely large systems.

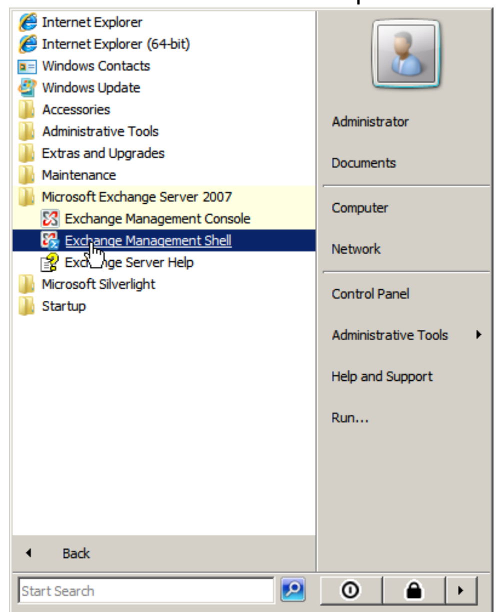
Once it has been determined that Lucene is no longer wanted or needed as a backup for the system, to save system disk space, the Lucene index should be removed from the system. This is not a necessary step, though it does free up system disk space that currently holds duplicate data that now resides in the more robust Exalead system.

To remove the Lucene Indexes, login as admin to the Retain Server, open a new window or tab, and browse to http://Retain_Server_Address/RetainServer/Util/luceneDelete.jsp to remove the users one by one according to UUID. The lucene delete page is also linked form the **Indexer Reset** page. To manually delete the Lucene indexes, remove the contents of the <storage area>/index directory. There should also be a copy of the index directory in the backup folder of the storage area. This measure is not required and

Appendix G – Exchange Permissions required for Retain

Exchange settings

To connect with exchange, Retain needs a user with appropriate rights. This can be accomplished by using an existing user, or by creating a new one. It is recommended to create a new user for Retain archiving. If creating a new user, ensure that the user is an active user account and that the password does not change to ensure Retain will be able to access mail without changing settings. This user is sometimes called a 'service account'. Retain calls this user the 'global catalog user'.



The user created or used for Retain must be a "mailbox-enabled user" with read access to see all other users, groups, resources, and Exchange Servers in the Exchange Forest. The user will be utilized by both the Retain Server and Worker for LDAP lookups in Active Directory. The Retain user also must have Exchange impersonation rights to every mailbox user on every server in the organization to be archived. The Retain user MUST NOT be a member of any Exchange Administrator group, as Exchange denies impersonation rights for all administrator accounts.

Additional permissions need to be added to the user created for Retain. The quickest way to add these rights is through the Exchange Management Shell. After creating the new user in Active Directory, open the Exchange Management Shell.

Grant Impersonation Permissions to the Retain user.

The commands required are different depending on the version of the Exchange Server. Exchange 2010, and 2013 require only one command per Exchange system to be issued, whereas Exchange 2007 requires the commands to be run on every Exchange server in the Exchange system to grant required permissions. If the Exchange system contains mixed 2007, 2010, and 2013 servers, the different commands must be completed on one server of each type.

Exchange 2010 and 2013 command:

For Exchange 2010 and 2013, the only command necessary for impersonation permissions is:

```
New-ManagementRoleAssignment –name ImpersonationAssignmentName
–Role ApplicationImpersonation –User ServiceAccount
```

Where the 'Name' is a name chosen by the administrator and the 'ServiceAccount' is the name of the Retain user.
For Example:

```
New-ManagementRoleAssignment –Name impersonation-retain
-Role ApplicationImpersonation –UserRetain
```

If additional Exchange servers are added to the system after running this command to grant rights to the 'retain' user, the command must be run again to grant rights to the new server.

Exchange 2007 commands:

('Retain' is the name of the Retain user, or Service Account below)

```
Get-ClientAccessServer | Add-AdPermission -UserRetain
-ExtendedRights ms-Exch-EPI-Impersonation

Get-MailboxDatabase | Add-AdPermission -UserRetain
-ExtendedRights ms-Exch-EPI-May-Impersonate

Get-MailboxServer | Add-ADPermission -userRetain -ExtendedRights
Send-As, Receive-As, ms-Exch-Store-Admin
```

Room and Equipment Resources

To archive Room and Equipment Resources, or to restore them, the Retain user, or Service Account, must also have delegation rights. These commands must be issued manually for each Room and Equipment or resource mailbox on every relevant server. This is required for both 2010 and 2007.

These commands must be issued:
('Retain' is used here as the name of the Service Account, or Retain user, and the 'Mailbox Database' should be changed to the appropriate name.)

(NOTE: every time a new Room and Equipment or resource mailbox is added, the first command must be re-run.)

Exchange 2010 and 2013 commands:

```
Get-Mailbox –ResultSize Unlimited –Database "Mailbox Database"
| Add-MailboxPermission –User "Retain" –AccessRights FullAccess

Add-ADPermission –Identity "Mailbox Database" –User "Retain"
–ExtendedRights Receive-As

Add-ADPermission –Identity "Mailbox Database" –User "Retain"
–ExtendedRights Send-As
```

Exchange 2007 commands:

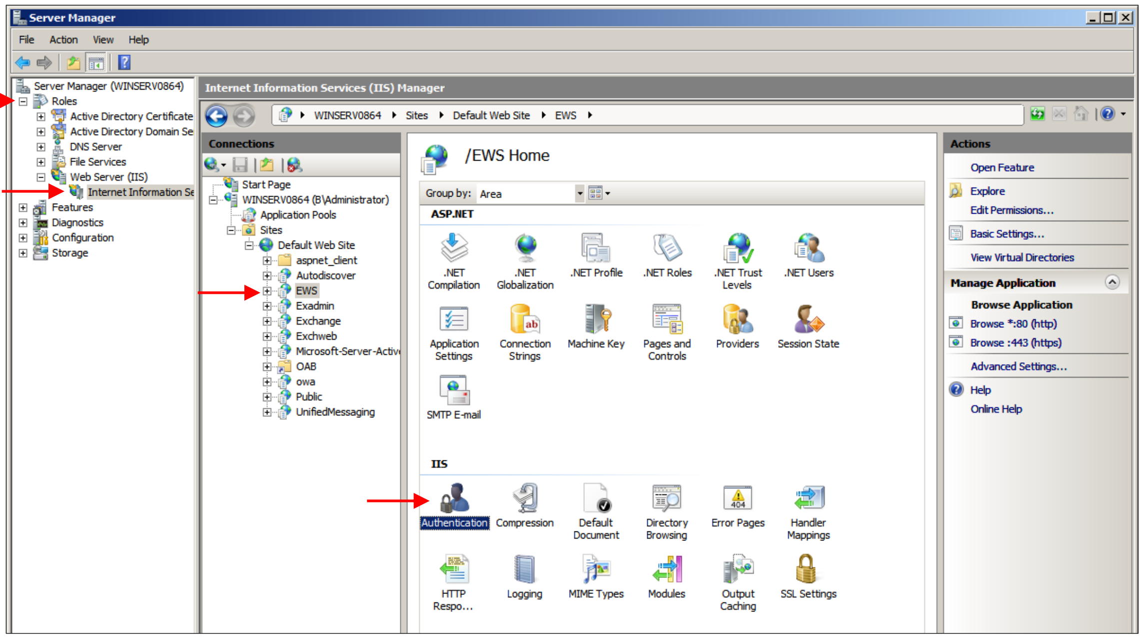
```
Get-MailboxDatabase | ForEach-Object {Get-Mailbox -ResultSize
Unlimited -Database $_.DistinguishedName | Add-MailboxPermission
-UserRetain -AccessRights FullAccess}

Get-MailboxDatabase | ForEach-Object {Add-ADPermission -Identity
$_.DistinguishedName -UserRetain -ExtendedRights
Receive-As,Send-As}
```

Authentication Methods

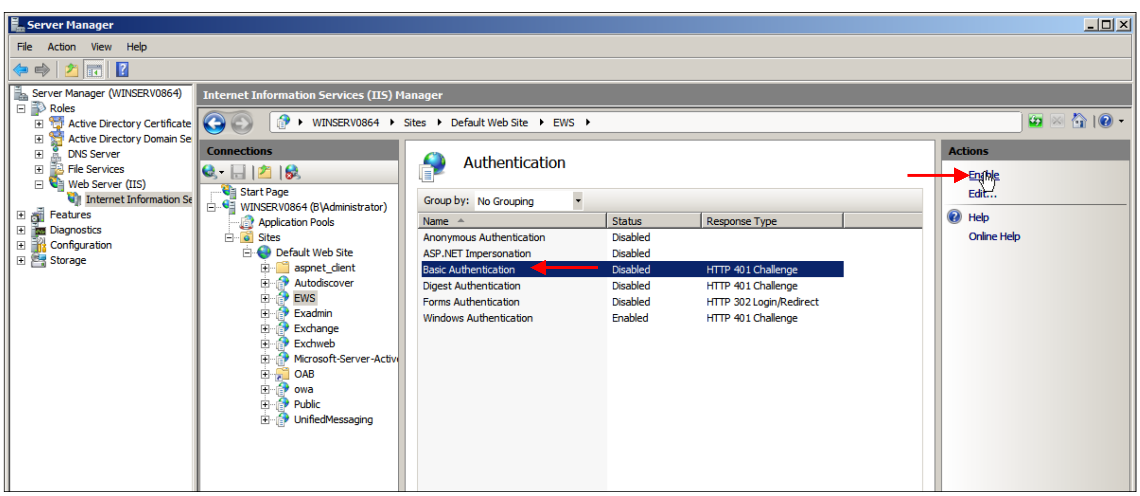
Retain requires Basic Authentication to be enabled on EACH CAS Exchange server in the system. Open “Server Manager” on Exchange server.

1. In left pane, expand “**Roles**”, expand “**Web Server (IIS)**”, select “**Internet Information Services (IIS) Manager**”.

2. A new “**Connections**” pane opens, expand your Exchange server object, expand “**Sites**”, expand “**Default Web Site (Multiple Protocols)**”, select “**EWS**”.



3. Under heading “**IIS**”, open “**Authentication**” icon



4. Select “**Basic Authentication**”, click “**Enable**” in right pane.

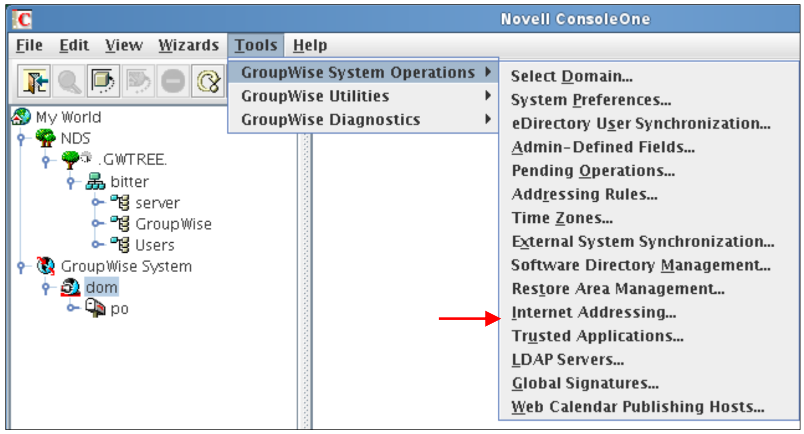
You can now close “Server Manager”.

Appendix H: Trusted Application Key Creation

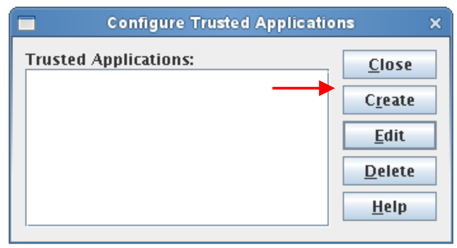
There are two ways to create a Trusted Application key: through ConsoleOne in GroupWise 8, or via utilizing a Trusted Application key generator on a connected and authenticated win32 workstation.

Trusted Application Key creation through Console One for GroupWise 8

ConsoleOne with GroupWise 8 supports the native creation of a Trusted Application Key. To create a trusted application key for Retain, select the GroupWise system from the system tree and select **GroupWise System Operations| Trusted Applications…** from the '**Tools**' menu.

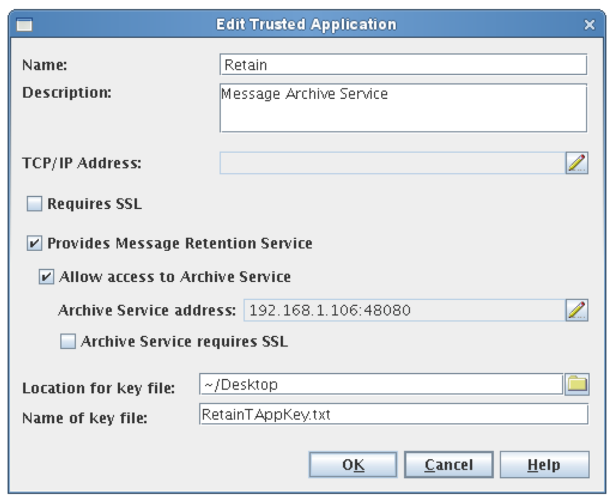


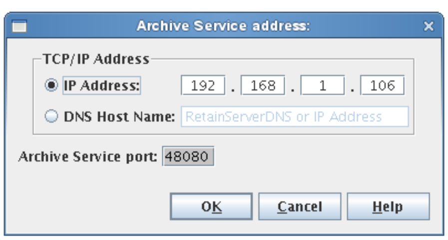
The Configure Trusted Application window will open, displaying any and all trusted applications currently listed in the system.



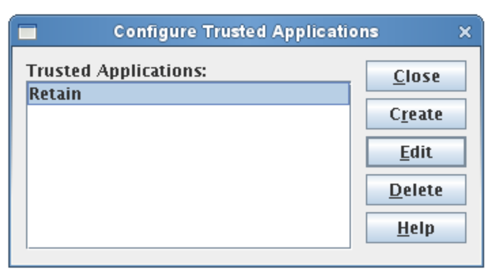
From the Configure Trusted Applications window, select 'Create'.

Enter the Name and description of the Trusted Application, in this case, 'Retain'. The name and description may be anything desired. Check the 'Provides Message Retention Service and 'Archive Service Address' and provide the IP address or DNS name to the Retain server and the port: 48080





The location for the key file and name may be anything desired, but the key file is saved in plain text, so add the .txt extension or open with an editor. The key may be copied and pasted into the Retain interface, or entered manually. The key file may be saved for records or discarded. The new Trusted Application Key is active and now appears to be edited, removed, or removed and re-created.



GroupWise Trusted Application Key generator

IMPORTANT Information about the Trusted Application Key generator:

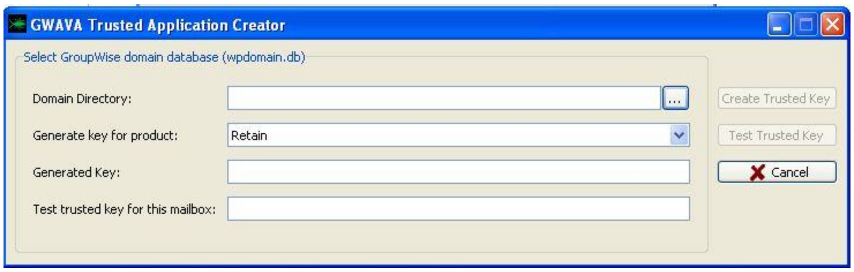
- The Trusted Application Key generator must be run from a win32 or compatible system.
- **You must use the program included with Retain.** The program included with other GWAVA products won't work for Retain.
- Your workstation must have the Novell and GroupWise clients installed.
- You must be logged in as the ADMINISTRATOR of the PRIMARY DOMAIN.
- The Trusted App Generator requires access to the domain database; in Linux this requires a SAMBA share or equivalent.

Note: The Trusted Application Key takes a few moments to propagate through the GroupWise system and therefore it may not be ready for testing or use immediately after you've generated it.

From the GroupWise Module page, select the link to download the Trusted Application Key generator, and select 'run', or run a previously downloaded and saved copy.

1) Click RUN to download and run the Trusted Application Key generator.

2) Follow the wizard. Click Next.

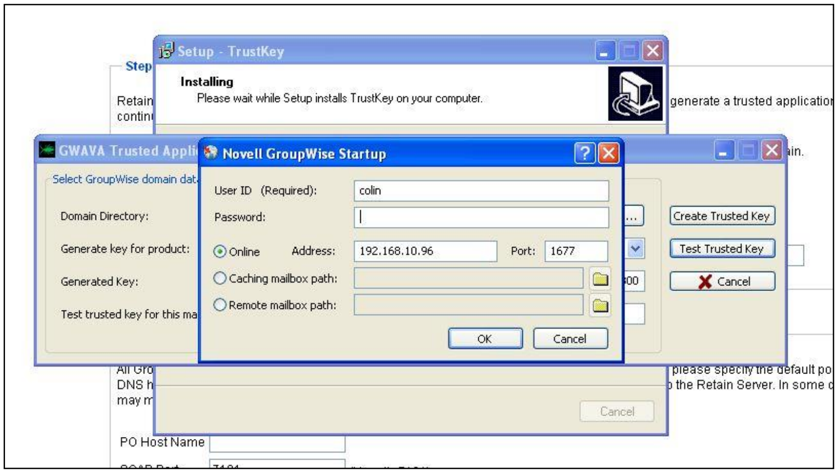


3) Find your GroupWise domain database. Click on the "…" button.

4) Once you have found your domain, click "Create Trusted Key".

NOTE: Please allow a few moments for the Trusted Application Key to propagate through the GroupWise system before testing it. You may proceed without testing the key but if you want to test it, please allow the time for the key to propagate through the system.

5) When the key has been generated, enter the name of a valid user on your post office and test the key by clicking "Test Trusted Key". You will be asked to log in to GroupWise for this user.



6) Once your login was successful, you know that both your trusted application key and the SOAP mechanism are working properly. The trusted application key is now copied to your clipboard so you can paste it to the Retain configuration page.

Appendix I Mobile Registration Email variables

The Retain registration email template, (…\RetainServer\WEB-INF\classes\config\mobile\registeruser.html), has many variables which allow for a customization of the registration email. There are a few variables which must remain unchanged, but the rest may be removed or modified, as desired, to adapt the email to any organization.

This is a quick description of the different variables, and which can be modified. They are distinguished by double brackets "[[" and "]]". The Retain Server code that sends out the email sets these variables with the product specific and user specific information.

Typically, only #1 will want to be changed – for use in mobile device management software.
If an admin wishes to make the registration email to look like it is coming from their company, they should modify #'s 1-2, 6-9. However, variables 6-9 may be simply removed if the admin doesn't want users to know what they are using.

1. your install location – This is typically the main variable to change. This variable is not included by default in the email to allow admins to utilize mobile device management software to push the Retain app to devices. It may be included in the email and filled in with the app's location so it can be manually downloaded to devices.
2. product – This is automatically filled out with the Retain product name. Admins may set this to be the company name. This variable is used in the subject and the body of the email message.
3. retainheader – This is automatically filled with the Retain product logo. Admins may set this to any branding or company image file. This must be an image file.
4. name – Each user's individual username will be input here. This should not be changed.
5. gwavaURL – Automatically filled-in with a link to the GWAVA website.
6. gwavaURLLabel – This determines text displayed for the gwavaURL link.
7. productNameURL – This is automatically filled-in with a link to the product website.
8. productNameLabel – This determines text displayed for the productNameURL link.

The registration code and information in that variable MUST NOT CHANGE. This information is generated by the device management page when the device is added.

The following variables MUST NOT CHANGE.
DO NOT MODIFY THE FOLLWING:

enrollmentCode: This is generated when the device is created on the device management page.
tenantid: This is static number for retain. Displayed on the mobile page from Module Configuration.
email: This is from the Device Management page.
name: This is from the Device Management page.
endpoint: This is the address of the Retain Server
rouerURL: This is pulled from the mobile page of Module Configuration.
activateHREF: This is an identification string, a link specific to the user and installation.

Appendix J Secureline Server Configuration

Retain requires the CellTrust Secureline server to create log files for the worker to access, digest, and send to the Retain Server for storage. To configure the Secureline server to create these files requires the scheduled run of a Gwava Report script, a tool provided by CellTrust.
The script may be scheduled through the quartz scheduler.
To configure the quartz scheduler to run the GwavaReport script, navigate to the /opt/PM/bin directory and run the start_sched_client.sh script, then follow the desired prompts.

For example:

```
[root@dev04120lv bin]# ./start_sched_client.sh

Hi, welcome to PrimeMessage Scheduler configuration utility
You will be prompted to enter different values. Every time you finish to
enter something - just hit "Enter". You can quit any time - just enter single
'q' charachter in the beginning of the line.
GOOOOD LUCK!

Select operation ( 1 - add job; 2 - remove job; 3 - pause job; 4 - resume
job; 5  - current jobs):
1

Enter job name:
GwavaReport
Enter job class name ( omit ".class" part ):
GwavaReportJob
Please select Trigger type( 1 - Simple, 2 - Cron):
```

At this point, select whether you want to use a Cron configuration for the triggers or a simple type – this is an example using the simple type:

```
Please select Trigger type( 1 - Simple, 2 - Cron):
1
Enter delay ( in seconds ) before first execution:
30
Enter number of executions ( 0 for indefinite ):
2
Enter interval between executions ( in seconds ):
30
Enter job additional params ( String or int only)
When finished, enter empty line for attribute name

Enter attribute name:
```

The GwavaReport has no quartz attributes, so hit enter, then ctrl-c to exit the script

Schedule the report to run as often as desired according to traffic and desired archival.

Once the report tool has run, it will place the necessary log file in the /opt/PM/scheduler/external directory. The files here are required by the Retain Worker. The Retain Worker required direct file access to these files. Whether by export or by local access, configure the CellTrust Secureline module with the location of these files, the file location must be from the worker’s point of view.