



GWAVA Reload 3

GroupWise Disaster Recovery

Contents

Introduction	9
Minimum System Requirements	10
Calculating Disk Space.....	11
Installation	12
Licensing.....	13
Logs	17
Administration	20
Reload CONSOLE Administration.....	21
Issues with VNC Client Sessions	22
Reload Administration from Mobile Devices.....	22
Understanding Reload Post Office Profile Backups	25
Job Preference	26
Access Mode – All Post Office Platforms	26
Restore Mode – NetWare or Windows Post Offices (Not Linux Post Offices).....	27
Standard (Incremental) Backups.....	28
Portable (Full) Backups	29
Expire-Portable Full Backups	30
Tape Archive Backups	30
Determining Disk Space Needed for Backups.....	31
Integrating Third-Party Backup Solutions with Reload.....	32
Backup Schedule Times.....	32
Creating a Reload Post Office or Domain Profile	33
Share Creation	34
Linux.....	34
Windows	35
Profile Creation	36
Creating a Remote Reload Profile for a Reload Post Office or Domain Profile on a Different Reload Server.....	38
Basic Reload Post Office Profile Configuration	40
Overview	40
Access-Backups	41

Configure - Access Backup Preferences	41
Access Mode - through the Access Mode POA.....	41
Auto-Reload Restore Area Access – Linux Post Offices Only	42
Restore POA Configuration	43
Managing Port Conflicts.....	44
Modifying a Reload Profile’s Restore POA Startup File	44
Creating a GroupWise Restore Area for use with Reload – NetWare and Windows Post Offices	44
Steps to create and use a Restore Mode POA.....	45
Creating a GroupWise Restore Area for use with Reload – Linux Post Offices	46
Disaster Recovery POA Configuration.....	50
Managing Port Conflicts.....	52
Modifying a Reload Profile’s Disaster Recovery POA Startup File	52
Load.....	53
Configure Disaster Recovery Failover Settings	55
Disaster Recovery Migration Settings.....	56
Configure Disaster Recovery Failback Settings	57
Standard.....	57
Schedule.....	58
BLOBS Threads	58
Database Threads	58
SmartPurge Configuration	58
DMS - Backing up Document Management Libraries	59
Customize.....	59
Advanced.....	60
Configuring Portable Backups.....	62
Schedule.....	62
Customize.....	63
Retention	62
Expire Action - Delete or Archive	62
Configuring Archive Settings.....	62
Specify Archive Path.....	63
Configuring Advanced Archive Settings.....	64

Advanced.....	64
Tape Backups	65
Schedule.....	65
Customize.....	66
Create Tape Archive (TAR) Files	66
Expire Old Tape Archive (TAR) Files	67
Specify Tape Archive (TAR) File Path	67
Configuring Advanced Tape Settings	67
Configuring the Reload Agent to “push” a *.tar file to another server	68
Configure Reload to push the *.tar file to a Windows server that is running Veritas.....	68
Build TAR Before Moving to TAR Path	68
Restore Mode – through the Restore Mode POA.....	Error! Bookmark not defined.
Final Notes on Configuring Reload Backup Jobs	Error! Bookmark not defined.
Job	69
Logs	70
Profile Preferences.....	70
Error and Warning thresholds.....	71
Advanced Reload Post Office Profile Configuration	71
Help	71
Managing Port Conflicts.....	Error! Bookmark not defined.
Modifying a Reload Profile’s Disaster Recovery POA Startup File	Error! Bookmark not defined.
Load.....	Error! Bookmark not defined.
Retain Integration	72
Retain Settings for Reload Integration.....	79
Reload Integration Preferences Menu.....	82
Connectivity	84
Working with a Reload Profile for a GroupWise Post Office That Has Moved to Another Server Platform	84
Configuring the Reload Agent For Failed Connectivity	84
Retry.....	84
Testing a Profile	84
Advanced Scheduling	85

Using the Reload Run Job Creation Utility for Enhancing Reload Backups for Disaster Recovery Applications.....	85
Domain Database Profiles.....	87
Understanding What a Domain Database Profile Does.....	87
Accessing a GroupWise Domain Database Backup.....	87
Basic Reload Domain Database Profile Configuration	88
Overview	89
Actions	89
Logs	89
Schedule.....	89
Retention	90
Expire Action - Delete or Archive.....	90
Preferences	91
Error and Warning thresholds.....	91
Specify Archive Path.....	91
Configuring Tape Backups.....	92
Schedule.....	92
Create Tape Archive (TAR) Files	92
Expire Old Tape Archive (TAR) Files	92
Specify Tape Archive (TAR) File Path	93
Configuring Advanced Tape Settings	93
Customize - Job Event Actions	94
Advanced Reload Domain Database Profile Configuration	94
Disaster MTA Menu & Settings.....	95
Modifying a Reload Profile's Disaster MTA Startup File	96
Load.....	96
Recovery.....	98
Connectivity	98
Working with a Reload Profile for a GroupWise Domain That Has Moved to Another Server Platform	98
Configuring the Reload Agent for Failed Connectivity.....	98
Retry.....	98

Testing a Profile	98
Disaster Recovery.....	98
Disaster Recovery.....	99
Reload Web Administration Method.....	99
Reload Console Administration Method.....	99
Reload Mobile Administration Method	100
Configuring Disaster Recovery Actions	100
Migrating Data Back to a Live Server	103
Disaster Recovery and Internet Mail	104
Upgrading Reload Software	104
Upgrading Reload Through Reload Administration	105
Upgrading Reload from a Command Line Session.....	105
Upgrading Reload from the Reload Web Administration.....	106
Upgrading Reload Automatically	106
Uninstalling and Re-installing Reload With the Reload Upgrade Tool	106
Reload Web Administration.....	107
Monitor	108
Disaster recovery Plan	108
Status Recipient-	109
Post Office profile	109
Domain Profile	109
Profile Monitor.....	111
Overview	112
Configure.....	113
Reload Web Administration Preferences.....	114
Job Handling Preferences.....	115
Reload Mailer Preferences, Help & Troubleshooting	115
Daily Status Report.....	116
Error Notification	117
Warning Notification.....	118
Job Completion Notification	118
Event Log.....	119

Agent Log	120
Profile page	121
Overview	122
Access Backups	127
Disaster Recovery.....	128
Tools menu.....	130
Documentation	130
Download Logs.....	130
Upgrade.....	131
License.....	131
Reload Quick Tour.....	132
Custom links.....	132
APPENDIX A.....	133
Restoring an Entire GroupWise Mailbox	133
Appendix B	133
Reload and Post Offices That Use LDAP.....	133
Reload and Post Offices That Use LDAP and SSL	134
Appendix C	134
Configuring Redline Integration.....	134

Intended Audience

This manual is intended for IT administrators in their use of Reload. It includes installation instructions and feature descriptions.

Technical Support

If you have a technical support question, please consult the GWAVA Technical Support section of our website at <http://support.gwava.com/>.

Sales

To contact a Beginfinite sales team member, please e-mail info@gwava.com or call Tel: 866-GO-GWAVA (866-464-9282) in North America or +1 514 639 4850. Suite 500, 100 Alexis Nihon Blvd., Montreal, Quebec, H4M 2P1, Canada.

Copyright Notices

The content of this manual is for informational use only and may change without notice. Beginfinite Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation. GroupWise® and SUSE® are registered trademarks of Novell, and copyrighted by Novell, inc. All rights reserved. GWAVA is a registered trademark.

Overview

Reload is a disaster recovery, hot backup, and quick restore system for Novell GroupWise. Reload integrates with GroupWise post offices and domains on NetWare, Linux and Windows to provide reliable backups. All the mail in those backups can then be examined using any Novell GroupWise client. Reload backs up post offices and domains from GroupWise 6.5 or greater. The Reload Server must run on the Novell Linux server platform. Specifically, Reload only runs on these platforms:

SUSE Linux Enterprise Server 9 – 32-Bit
Novell Open Enterprise Server (Linux Kernel)
SUSE Linux Enterprise Server 10 – 32-Bit or 64-Bit

Licensing

Reload is licensed per user. Reload will operate as a demo for thirty days for testing purposes. A demo license file (reload.pem) must be obtained separately from the Reload software download. The demo license file can be obtained at:

<http://getreload.gwava.com>

After 30 days, the demo license will expire. You will then be required to purchase a license for the appropriate number of users on your system.

Introduction

Reload is a Disaster and Recovery solution for GroupWise mail systems that provides live backups and recovery for GroupWise post offices and domains. In the event of a disaster where the post office or domain is unusable or lost, Reload can provide a temporary post office and domain for the GroupWise system to run off of, making messages flow seamlessly, even in a crisis.

Reload performs this function by creating backup copies of the post office and domain databases, which it then can load with GroupWise agents. Reload also can load access mode, or restore post office agents against the any post office backup, allowing users to transparently restore deleted or lost mail to the live post office, directly from the user's GroupWise client. With Reload, losing mail in a system is no longer a crisis, and in most cases, not an inconvenience.

Multiple Reload servers can also be tied together to add multiple redundant layers of protection for complete offsite backups of the GroupWise message system.

Reload only runs on the Linux platform and requires certain settings in ConsoleOne as well as on the host machine for both the GroupWise system and the Reload Server. Reload does not require eDirectory or any TSA components.

Setting-up Reload can be an intimidating process, but this guide will walk you through the process. There also is online documentation, an extensive knowledgebase, video documentation, full support, and consulting services available to aid you in customizing and perfecting your Reload system.

Reload backs up the GroupWise system according to a profile that the user specifies, which tells Reload what to backup, where it is located, and where to store the data. The Profile can also keep track of disk space and when to expire the backups it creates. After the initial backup, each successive backup takes an average of 12% the full size of the live post office, also saving network and disk resources.

The basic steps to setup a functioning Reload system are as follows:

1. [Install Reload](#)
2. [License Reload](#)
3. [Create backup Profile\(s\)](#)
4. [Run a Job](#)
5. [Configure Disaster Recovery](#)
6. [Test Disaster Recovery](#)

(It is also recommended to setup Reload's [warning and error threshold monitoring and alerting](#) message service.)

After the initial setup and test, the base of your Reload system is setup. If you wish to configure the access and recovery modes for the Reload POA's, you may do that at your leisure. It is best to review the entire guide to familiarize yourself with the system in order to plan where your Reload Server will go, and which features you wish to implement.

Minimum System Requirements

Supported OS's:

- SUSE Linux Enterprise Server 9 (SLES9) 32-Bit
- Novell Open Enterprise Server Linux kernel (OES)
- SUSE Linux Enterprise Server 10 (SLES10) 32-Bit or 64-Bit.
- The Reload server only supports the Intel Platform x-86 Platform

The Reload server must be run on the Linux platform, but it backs up GroupWise post offices on NetWare, Linux or Windows platforms.

Memory

Two gigabytes of available RAM should be sufficient for most environments. More memory is helpful.

CPU Speed

The faster the better; SMP is not to be considered a requirement, however testing of Reload 2.0 on SMP has shown that Reload is benefited by SMP.

Network

Reload servers should be in close network proximity to the GroupWise servers that are being backed up with Reload. If a Reload Server and some GroupWise post offices are on a Gigabit switch, it would be best to have a network card in the Reload server that supports a Gigabit speed.

Disk Space

The disk space may reside on the Reload server or on a SAN. The requirements of the disk solution are as follows:

- The disk solution should always be mounted for use with Reload.
- The disk solution should be formatted with a Linux based file system, specifically a file system that supports symbolic links.
- If the disk is not a SAN, but a NAS solution for example, the mount should be an NFS mount. No other protocol other than NFS.

Calculating Disk Space

Disk space must be carefully considered for each Reload Server. When the Reload server reaches the error threshold for disk space, it will no longer create backups. Make sure the target system has plenty of space to accommodate the needs of your Reload backups.

The Reload server requires the following disk space per profile:

- Initial backup: 100% of the size of the post office.
- Then for each week (on average) that will be retained as a Reload Portable Backup (full backup): 250% of the size of the post office.

A 100 gigabyte post office, for example, would require 500 GB of disk space to retain two weeks of portable backups.

For a detailed explanation of how much space will be needed, and how to calculate space for your system, see the following link: <http://support.gwava.com/kb/?View=entry&EntryID=514>

For a profile retaining three weeks worth of data, you must calculate 4 portable backups, because the 4th portable backup must be created before the oldest portable backup can be expired.

Disk speed directly impacts Reload performance. A disk that is tuned for fast writes to disk is highly recommended and will improve performance.

When considering disk space requirements, also take into account future growth of GroupWise post offices, and the space that will be required to sustain that growth.

If Reload runs out of hard disk space, backups will no longer be created. A Reload profile may have a threshold of days to keep in the portable backup set, so that it does not exceed the specified amount. This can help prevent systems from running out of disk space.

This setting is found in the Reload console administration under Profile | <select desired profile> | Standard | Advanced | Limit the Number of Standard Backups. Enable the option and the system then asks for a threshold value. The value is in days.

If there is more than sufficient space for the Reload system, it is preferred to keep this option disabled, to maintain full and consistent portable backups. **Remember to take Post Office growth and the host Operating system into account while calculating disk space needs.** The setting is found in context on [page 43](#).

Installation

Reload installation is straightforward and simple. The installation file is an .RPM file, the preferred installation method on the Novell Linux platforms. Locate the install file:

```
beginfinite-reload<some version number>.rpm
```

DO NOT INSTALL Reload FROM YaST. Install Reload from within a terminal session. Installing Reload from YaST will not work correctly. To install the Reload package, do the following: Assuming the *.rpm file is found in the path: /tmp

1. Open up a terminal window on the Linux server. This can be done either at the Linux server, or from a remote session via SSH or VNC.
2. Make sure to be logged in as root
3. Install the *.rpm with the following command:

```
rpm -ivh /tmp/beginfinite-reload<version>.rpm
```

For example:

```
rpm -ivh /tmp/beginfinite-reload-2.0.000-1.rpm
```

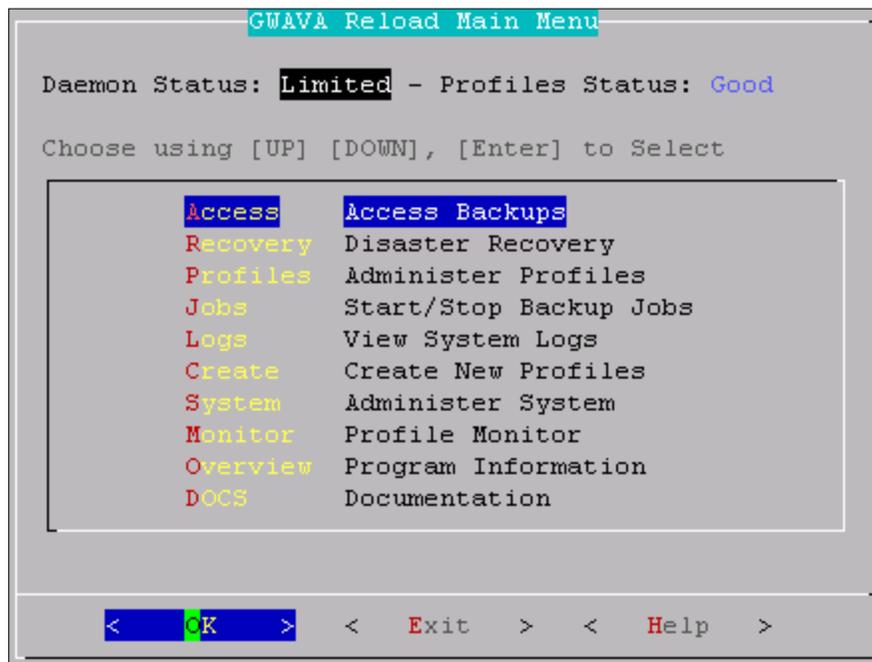
The Installation performs the following tasks:

- Installs the Reload System software to the path: /opt/beginfinite/reload
- Creates initialization scripts to start the Reload server on server bootup
- Creates various Reload initialization scripts such as "reload, reloadadd, reloadm, and reloadj" in the /usr/sbin directory, so that they are available to the Linux administrator "root".
- Sets up a default Reload System configuration
- Starts the Reload Daemon
- If needed, the installation also installs the GroupWise DBCOPY and GroupWise Agent packages, unless these packages have been installed before, or if the installation determines that other GroupWise agent software is already installed.
- If the Reload server has a connection to the Internet and can browse the web, then the Reload server will attempt to install a piece of software called Xdialog. The Xdialog is used to view Reload log files in a graphical user interface. It cannot be bundled with Reload, because of licensing issues, so Reload downloads it to the Reload server if the server has a connection to the Internet. Xdialog is not required.
- Installs a Reload Administration icon to the root user's Xwindows desktop. If you are in an XWindows type session, you should see an icon on the root user's desktop. This icon is compatible with a basic GNOME or KDE installation. The icon is for convenience, and may not work in all Linux desktop environments. The command to start Reload Administration from within a terminal session is:

```
reload
```

Licensing

When Reload is first installed, it does not come with a "license file". Without a license file installed, the Reload Daemon is running in "Limited" mode. So if you run Reload Administration, the Daemon Status may indicate: "Limited", as shown.



The Reload system will not function until a license file is obtained. The license file is named:

reload.pem

The Reload System Daemon looks for the license file in the directory:

/opt/beginfinite/reload/license

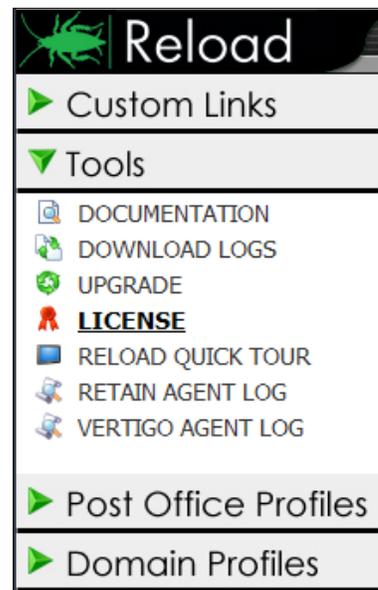
The license file can be either manually copied to the above directory, or it can be uploaded to the Reload System via the Reload Web Administration. If the license file is manually copied into the reload license directory, it must be named reload.pem, and the reload daemon must be restarted for the license to be recognized.

Example: if the server were at the IP address of 10.1.1.100; to access the Reload Web Administration type the following in a web browser:

<http://10.1.1.100:5555>

Follow the link **Tools | License**, to put the **reload.pem** license file in place. A temporary reload.pem file can be obtained from:

<http://getreload.gwava.com>



Once a valid license file is uploaded, the Reload Daemon will consume the new License file, and immediately give the Reload System full functionality.

If the time on the Linux server running Reload is incorrect (specifically the date reflects sometime in the past), you may see an error on Reload Web Administration home page in the “License Expiration Status” field. After receiving a License error, you may need to wait for a couple of minutes for the ‘License Expiration Status’ to indicate the problem with the License file. To configure the time on the server, see the “Reload Server Time Synchronization” section with regards to NTP configuration.

Post installation tasks

Reload connectivity to NetWare GroupWise Post Offices.

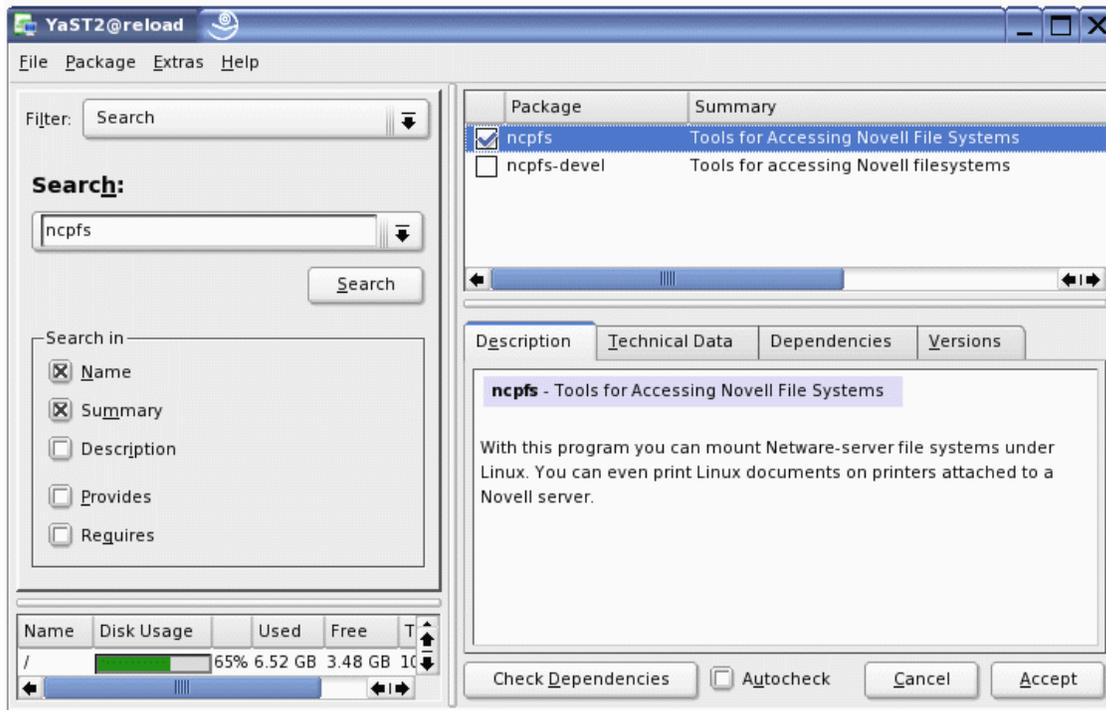
If the Reload server is backing up GroupWise post offices on a NetWare server or a cluster resource, then the NetWare connectivity package called “NCPFS” must be installed. The Linux-based ‘Novel’ client that is commonly used is not sufficient. The NCPFS package can be installed from YaST. To see if NCPFS is installed on your Linux server, use the following command in a terminal session:

```
rpm -qa | grep ncpfs
```

If the ncpfs package is installed, there should be a response similar to:

```
ncpfs-2.2.4-25.1
```

If you get nothing back from the above command, then NCPFS is not installed and needs to be installed through YaST. Start YaST and search for “ncpfs”. Once it is located, install the package.



STOP! Do not install any of the GroupWise Software Components mentioned in this section, until you have read the entire section. Most customers will not need to install any GroupWise Software Components.

Reload must have the following two GroupWise Software Components in order to run:

- GroupWise DBCOPY
- GroupWise Agents

The Reload installation routine will attempt to install the GroupWise DBCOPY and GroupWise Agent packages. The installation routine will not install these packages if it detects that there is a directory called

```
/opt/novell/groupwise/agents/bin
```

If the server has never had GroupWise for Linux packages installed, then there is a good chance this software will just be installed automatically. However, if for some reason this software does not install automatically, then you must install it manually.

The version of the GroupWise DBCOPY and GroupWise Agent packages is important. The GroupWise 7.0.3 shipping version of DBCOPY and the Agents are the only versions that should be used until newer versions are released. Even if the GroupWise post offices that will be backed up with Reload are GroupWise 6.5 post offices, install the GroupWise 7 level DBCOPY and Agent packages on the Linux server. It's perfectly fine to be backing up a GroupWise 6.5 level post office with the GroupWise 7 level software.

If you need to manually install the GroupWise Agents or DBCOPY software, first locate the source .rpm files. Reload comes with the 7.0.3 and 8.0 Versions of DBCOPY and Agent .rpms, if you do not have them. They are located in,

```
/opt/beginfinite/reload/setup/rpms
```

To install an *.rpm use the command: rpm -ivh <name of the *.rpm file>

Example:

```
rpm -ivh novell-groupwise-agents-7.0.3-20080309.i386.rpm
rpm -ivh novell-groupwise-dbcopy-7.0.3-20080309.i386.rpm
```

The command to un-install, (erase), an RPM is: rpm -e <package>. So if you need to un-install some older GroupWise code in order to install newer code you would first use the follow commands:

THIS IS AN EXAMPLE ONLY

```
rpm -e novell-groupwise-agents
rpm -e novell-groupwise-dbcopy
rpm -e novell-groupwise-gwia
```

These are simply examples being provided. You may need to un-install more or fewer than the packages listed.

The Reload Server also must have the following three packages installed. On a default SuSE installation, these packages are automatically installed, however if the Reload Linux server was installed a minimum installation was performed, these packages may not be installed:

- Dialog – A text based menu system, used for the Reload Administration interface
- Perl – An interpretive language, used by the Reload Migration Agent, and Domain Backup Agent
- Python – An interpretive language, used by the Reload Daemon to carry on a simulated GroupWise client session with Restore Mode POAs

The installation status of these components is indicated on the Reload Web Interface in the Overview tab | Software Installation Overview. You may check the components' installation status there.



The screenshot displays the Reload Web Interface. At the top, there is a navigation bar with tabs: Monitor, Overview (selected), Configure, Event Log, and Agent Log. Below the navigation bar, the main content area is titled "System Overview". Underneath, there is a section titled "Software Installation Overview" which contains a list of software components and their installation status:

- ! Reload Relies On the Following Software Components to Be Installed:
- GroupWise DBCOPY: **Installed - Version 7.0.3**
- GroupWise Agents: **Installed - Version 7.0.3**
- Dialog Menu: **Installed**
- Perl: **Installed**
- Python: **Installed**

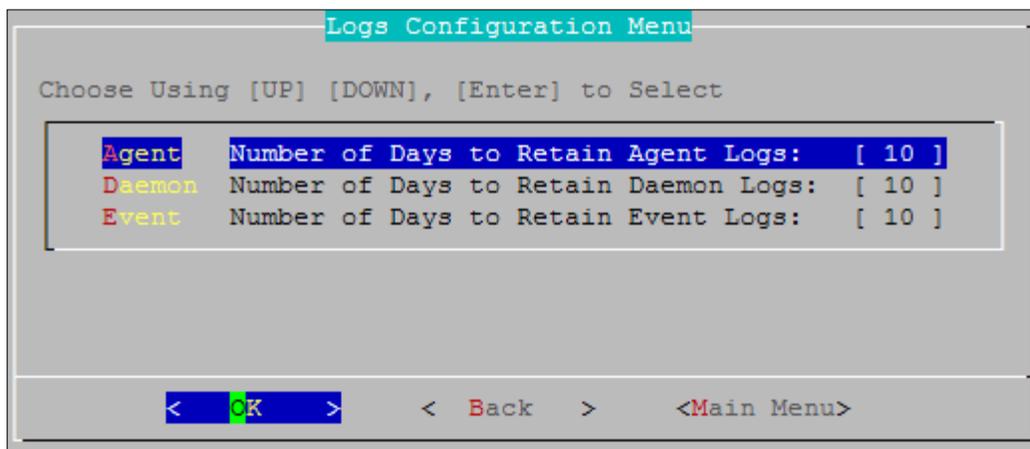
Logs

The **Event Log** is a **simple**, informative log. The **Agent Log** is a **verbose** log that tells everything that is going on. The Event Log is meant to be very structured, and intuitive. Generally you should just concern yourself with the Event Log. The Agent Log is not necessarily intuitive, but it is very informative. Sometimes you might see “errors” in the Agent Log, which are not actually errors, but just logging of conditions that the Reload Agents take into account when they run. Each profile has its individual Event and Agent log. When the Reload Agent acts upon a profile, almost all of its actions are written to both the system level Event and Agent logs, as well as the profile level logs.

Reload logs are kept in the /op/beginfinite/reload/logs directory, but all logs are accessible in the Web Interface under the general system or their respective profiles.

Configuring Log Expiration

The Reload System rolls the Daemon Log, Event Log and Agent Log at midnight each night. Rolled logs are saved for 10 days (by default). If you would like logs to be saved for a longer or shorter period of time, then choose from the Main Menu **System** (Administer System) | **Logs** (Log Expiration).



Configuring Reload Server Time Synchronization

Time affects Reload in the following manner:

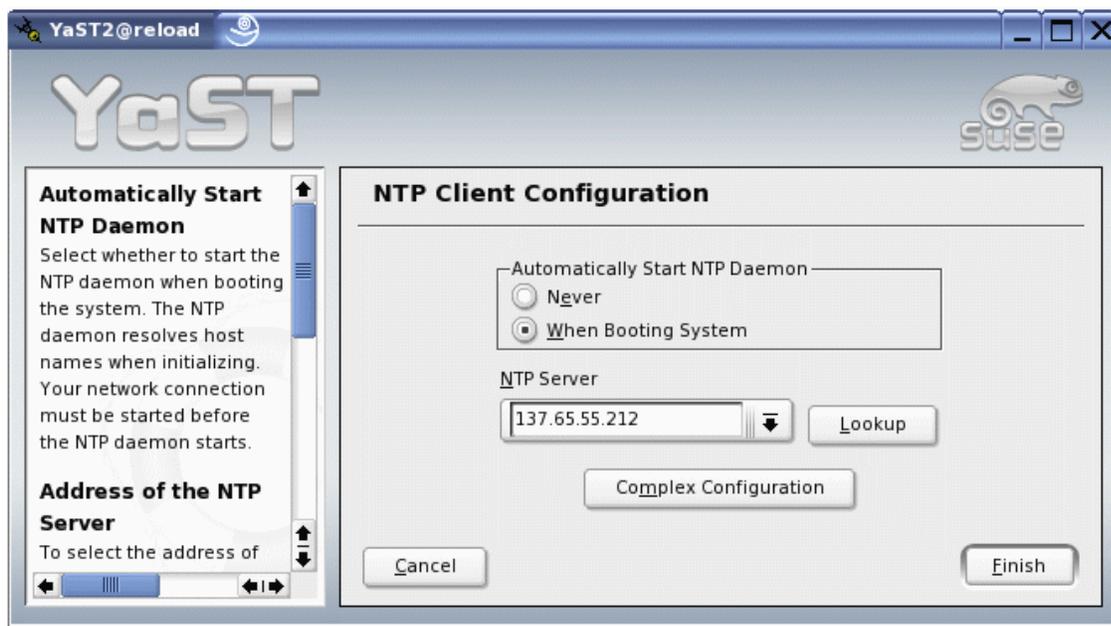
- Licensing
- Backup names
- Timestamps on user's mailboxes
- Scheduling of backup jobs

Ensure that the Linux server's time is synchronized correctly with the network. The correct time is **critical** to the success of Reload. The NTP Client is really simple to configure in YAST2 in an XWindows session or YAST in an SSH session. The quick terminal based command to get to the NTP client module in YAST2 is the following:

```
yast2 ntp-client &
```

Or, in a terminal session without an XWindows desktop, for example an SSH session:

```
yast ntp-client &
```



Enabling SmartPurge in ConsoleOne

VERY IMPORTANT: By enabling SmartPurge functionality within GroupWise, users will not be able to purge messages until their mailbox is backed up with Reload. This ensures that all sent or received messages cannot be deleted until they are backed up. Furthermore, by enabling SmartPurge functionality, data backed up to the Reload server cannot be purged.

Following are the steps you would perform in ConsoleOne, with GroupWise Administration SNAPins to ConsoleOne. To enable SmartPurge functionality on a GroupWise post office that is being backed up by Reload, do the following:

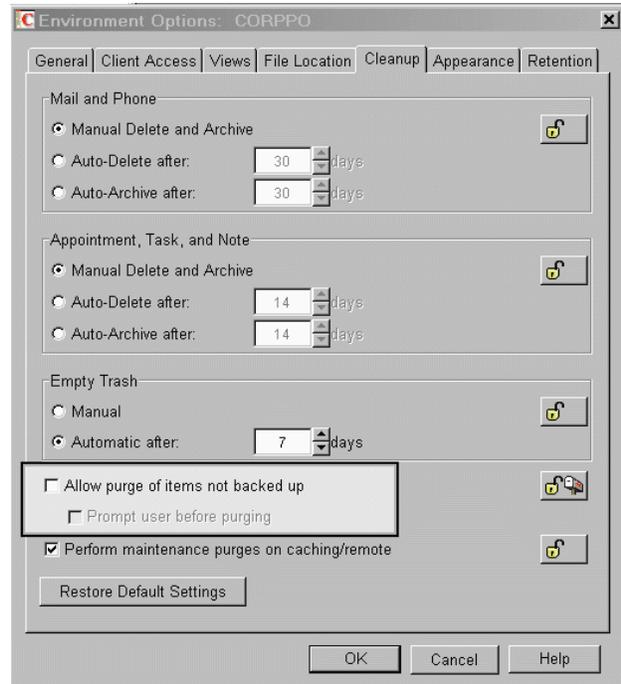
In ConsoleOne, **highlight the GroupWise post office** that will be backed up with Reload.

- Select **Tools | GroupWise Utilities | Client Options**
- Select **Environment | Cleanup**
- Ensure that the checkbox that reads "**Allow purge of items not backed up**" is **unchecked**.

Perform these steps on all GroupWise post offices that will be backed up with Reload.

By enabling GroupWise SmartPurge the following will be enabled:

- Users will not be able to purge messages from their trash unless they are backed up with Reload. This ensures that all sent or received messages cannot be purged, until they are backed up.
- Even if a user archives an item, before the item is backed up, a copy of the item is actually kept in the trash, until Reload has performed the backup of that item.
- When users access a backup from the Reload server, they will not be able to purge items in the backup. Even if the users archive items, the items are not actually removed; they are just moved to the Trash folder. That's good, because you do not want users to be able to purge items from the backup, or else it really is not much of a backup.
- All items are backed up. A copy of the mail item is actually kept in the user's trash until such time that the item is backed up by Reload. This assures that the GroupWise archive does not become a black hole for information as far as backups go. Because of the GroupWise SmartPurge technology that Reload integrates with, nothing that comes into the GroupWise message store can be fully removed from the message store until it is backed up with Reload.



NOTE: Perhaps you may want to exclude one or more users from the SmartPurge feature. For example, one customer wanted the SmartPurge feature in place, except for one executive that wanted the privilege to purge trash items if needed, so that certain trash items might not be backed up by Reload. In ConsoleOne, the SmartPurge feature was disabled for just this one user by editing their client options and disabling SmartPurge.

Administration

Reload 3 utilizes two different administration interfaces; Reload console administration and the Reload Web Administration. Reload Console Administration is the control core of the application and should be run in a terminal session, or from the desktop of the Reload Server. Reload Console administration can be used for all setup and maintenance tasks, but is mainly used to configure profiles, disaster recovery, and the access and restore POA's. It is important to know the use of both administration interfaces. Reload Console administration must be used to create the base of the system, where Reload web Administration is best used for day to day tasks.

To launch the Reload Console Administration, either select the desktop icon on the Server, or from a terminal session, enter the command:

```
reload
```

Reload Web Administration is designed to provide control of day to day functions and system monitoring tools in a pleasing and easily accessible interface. By default, Reload Web Administration does not require authentication as users cannot change the base profiles or configuration of the system through Web Administration, but it can be configured to require authentication. Reload Web Administration is served by the Reload Daemon, which must be running for the interface to be available.

To contact Reload Web Administration, open a browser on any machine with a network connection to the Reload Server and enter the following URL:

```
http://<Reload server IP or DNS>:5555
```

Unless SSL is enabled, then the address is:

```
https://<server ip or dns>:5555.
```

You can change the default port and other features of the HTTP monitoring page in Reload Administration.

The Web Administration is covered in detail later in the guide. See the [Web Administration](#) section for details.

Reload CONSOLE Administration

The Reload Console Administration is the place to start using Reload. There should be a Reload Administration launch icon on the server XWindows desktop, if the server is running "GNOME" or "KDE". (This should also show in a VNC session.)



This icon is only compatible with GNOME or KDE Desktops. If the icon does not work on your server, simply run the target command 'reload' in a Terminal session.

Reload Administration is completely compatible with an SSH client session, though you will want an SSH session that supports color. Administrators using a Windows workstation should consider getting the free SSH utility called "[Putty](#)". Putty will give you a terminal session to your Reload server, from your Windows workstation.

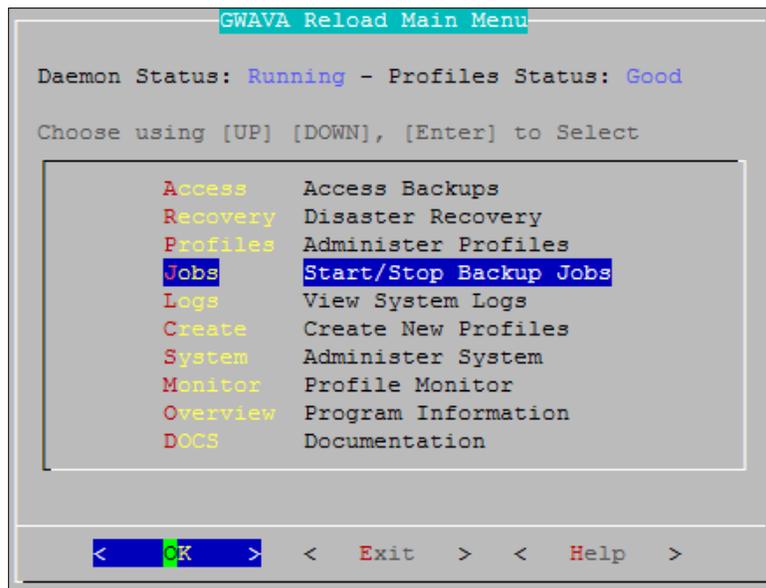
The Reload Administration was designed for a Terminal session window sized **80 Columns by 35 rows**. To determine the size of a terminal session window, issue the command:

```
stty -a
```

This command will report the size of the terminal session window. If the terminal session window is not the correct size, you can adjust it as needed.

Open a Terminal session, ([PuTTY](#), XTerm, Gnome Terminal, or the standard Terminal interface), then enter the command:

```
reload
```



Within Reload Console Administration, you can create backup "profiles" that correspond to your GroupWise Post Offices and GroupWise Domains. The maximum number of profiles that a Reload Server will support is 20 Post Offices and 20 Domains.

Each Reload server is configured via Reload Administration. In an environment in which there are multiple Reload servers, each Reload server acts independently of other Reload servers. The Reload Administration must be run on each individual Reload server.

Reload comes pre-configured with factory system defaults. You can alter these defaults as needed, or as instructed by GWAVA Support staff. The system defaults are located under the System menu. The Reload Administration has a quick-key worth noting. Wherever you are in Reload Administration, to get to the Main Menu screen, hit the **Escape Key** once or twice.

Issues with VNC Client Sessions

VNC is known to sometimes have problems where keystrokes entered, are enacted multiple times. VNC is particularly vulnerable in situations in which the network link to the Reload server is slow or the Reload server's CPU is being taxed. The Reload Administration menu will act like someone else is controlling or hitting keystrokes. Really, VNC is interpreting a single keystroke as multiple keystrokes. Reload was entirely developed using a VNC session to a VMWARE hosted SLES9 server, and worked flawlessly, but that was on a fast connection with no network latency. Here are some tips with regards to using VNC:

- Consider using mouse clicks in Reload Administration. For example, click a menu option, and then click the "OK" button. VNC does not repeat mouse clicks errantly, so the behavior should be predictable.

- Sometimes VNC client sessions just get too funny for words. Then it's time to bring down the VNC Server. The command for doing this is:

```
vncserver -kill <VNC Port Number>
```

Example: **vncserver -kill :01**

or:

```
killall Xvnc
```

Now the only trick is how to load the VNC Server again. The way to do this is to type in the command `vncserver :<vnc port>`. You need to get a terminal session with the server either through an SSH session, or at the server console. The command to start the VNC server might be:

```
vncserver :01
```

From a VNC Client, such as a Windows VNC client, the way to get to the server if you loaded the VNC Server with the ":01" command would be:

```
<ip address>:01
```

For example:

```
10.1.1.100:01
```

- If VNC is just too problematic, you may want to consider connecting to the Reload server with an SSH client such as "Putty" as mentioned earlier in this documentation.

Reload Administration from Mobile Devices

Reload Administration has a device friendly menu system called "**Reload Mobile**" which was created for the following scenario:

The ability to access backups through Reload is quick and efficient. Now the CIO is constantly calling you to get access to old e-mails. (No problem, you want to make the CIO happy, they sign your paycheck.) One day the CIO calls you while you are in training, or you are two hours from the office. No problem, you've punched a hole through the firewall for SSH clients to get to the Reload server. So you whip out

your **wireless device** (such as a **Blackberry**) and fire up an SSH client that you've installed to your wireless device. You authenticate to the Reload server and type in the command:

```
reload
```

The Reload administration auto-detects the screen size of your device, and presents the "Reload Mobile" menu. You easily navigate the Reload Mobile menu, using only numbers, and the enter key. And voila, in 5 minutes flat, you call the CIO back, and make them happy.

If Reload Administration does not properly detect that you are using a device with a small screen, you can **force Reload Mobile menu to load by typing in the command:**

```
reloadm
```

or

```
reload -m
```

To scroll within Reload Mobile, on most devices the plus (+) and minus (-) keys will scroll through menu lists.

Reload Daemon

COMMANDS:

```
reloadd restart
reloadd stop
reloadd start
reloadd status
```

Reload has a "Daemon". **This process must be running in order for Reload to function.** The Daemon is designed to automatically load when the Linux server loads. The Reload Daemon can be controlled completely from within the Reload Administration. Choose System (Administer System) | Control (Control Daemon). The Daemon can also be controlled with the "reloadd" script. To run the script, run the "reloadd" command in a terminal session.

The Reload Daemon has an auto-recovery script which runs every minute. So if the daemon is not running, the auto-recovery script attempts to start the daemon. If you want to make sure the Reload Daemon is not running, you must disable the auto-recovery script.

In Reload Administration select:

System (Administer System)

Control (Control Daemon Process). Then select the choice for Reload Daemon Auto Recovery, and select disable.



The Reload Daemon can be monitored by reading the Daemon Log file. The Daemon Log File can be viewed through the Reload Administration. To see the Daemon Log File, from within Reload Administration, select **Logs** (View Logs). The Active Daemon Log file is a rolling view of the Reload Daemon's log file. To see a static Daemon Log file, select **More** (More Log Viewing Options) | **Daemon** (Static Daemon Log).

Troubleshooting the Reload Daemon

If for some reason the Reload Daemon won't load, you can troubleshoot it using the following process: Change to the directory **/opt/beginfinite/reload/lib/code**

```
cd /opt/beginfinite/reload/lib/code
```

Type the following command to run the Daemon in the most basic mode:

```
./gre -r ../.. / &
```

This runs the Reload Daemon with its minimum command line requirements. In this mode the Reload Daemon is not providing a Web Page, or reading any other configuration parameters that are specified in Reload Administration. So if the Reload Daemon runs in this most basic mode, then the problem is one of the settings in Reload Administration. If the command to load the daemon fails, the daemon should give some kind of an error message, and the messages are generally informative, but not verbose. The way to bring down the Reload Daemon with the Reload Daemon script is:

```
reloadd stop
```

or

```
/etc/init.d/reloadd stop
```

The way to bring down the Reload Daemon manually is with the following command:

```
kill -3 <Reload Daemon PID>
```

TIP: You can find the PID for the Reload Daemon with the following command:

```
ps aux | grep "./gre -r"
```

Reload Agents

The Reload agents are spawned by the Reload Daemon as needed. The agents are the real workhorse of the Reload System. The Reload agents have two files to which they log: the Agent Log and the Event Log. Both of these can be accessed from Reload Administration, and from the Reload Web Administration page.

Configuring Reload System Settings

- From the Reload Console Administration, Reload administrators are able to:
- Administer all of the Reload system settings
- Create and configure "profiles" which correlate to backup profiles for GroupWise domains and post offices
- Easily access backed up data either for data recovery purposes, or even to make the Reload server a live GroupWise domain or post office in the case of a disaster recovery scenario
- Enabled Disaster Recovery failover for a Reload profile
- Manually request that the Reload server perform a backup job
- Monitor Reload logs

Whenever a setting change is made to the Reload Daemon configuration from within the Reload Administration, the Reload Daemon will be restarted so that it rereads the configuration settings that you made. **You do not need to restart the daemon in order for the changes you made to take effect.**

See the respective sections in the documentation on how to configure specific parts of Reload. Custom configuration of all major settings is explained. Almost all other Reload System settings should just be kept the same. Many of the settings are self-explanatory. Those settings not so intuitive, such as the "WAIT Counter" and the "KILL Counter" should be kept at factory defaults, unless support recommends that you make changes to them.

Understanding Reload Post Office Profile Backups

When a Reload post office profile is created, and initialized, it comes pre-configured to function. When a Reload profile is completed, the initial backup job is started within two minutes. But the Reload system may skip this step due to an upgrade or existing system settings. A running job is noted in the logs as well as under the 'Jobs' menu. The very first backup job can take a while depending on the size of the post office. However all other backup jobs should be significantly faster than the first backup job that Reload created for a particular profile. Most customers will find it educational to kick off a Standard Backup job for their newly defined Reload profile. To do this, do the following:

From the Reload Administration Main Menu, select **Jobs** (Start/Stop Jobs)

- Select **Start** (Start a Job)
- Choose the Reload profile you created
- Select **Standard Backup**

A "Standard Backup" is the backup job that would typically happen once a day, at night for example. Generally this kind of a backup job is called an "Incremental" backup job. However, what is different about Reload's Standard Backup job is that with Reload's synchronization model, **a Standard Backup job effectively becomes a fully accessible backup job that does not need to be manually combined with a "Full Backup" job in order to be of use.** The Standard Backup job daily retrieves the additions to the offiles, (blobs), and fresh copies of the ofuser and ofmsg directories. This allows the Standard Backup to catch all changes in the post office, but each Standard Backup job only takes approximately 12% of the post office's total size in order to replicate.

Job Preference

In Reload 3.1, preference is given to Standard Backup Jobs over any other types of jobs in the queue to run. This feature is enabled by default, and can be disabled under Job Handling Preferences.

The need to have a recent Standard Backup Job is extremely important during a disaster situation. Job prioritization feature ensures that Standard Backups are given the priority that they require.

There are times in which problems in the network or some other factor caused a Reload backup job to run indefinitely. Reload has several routines to discover a job that has failed, and needs to be restarted. Job recovery ensures that if a job is failing it will either be restarted or allowed to completely fail so that other jobs can be processed.

Accessing a Reload Backup through the Access Menu

By choosing the option "**Access** (Access Backups)" and following the menu prompts, Reload Administration can load a GroupWise Post Office Agent (POA) running against a Reload backed up GroupWise post office message store so that mail can be examined by any native GroupWise client. There are two different connectivity modes and POA types in Reload. They are:

- Access Mode
- Restore Mode

Here's an explanation of both of these modes.

Access Mode – All Post Office Platforms

With Access Mode, a GroupWise POA loads against the post office backup on the Reload box that represents a particular day that you want to access e-mail from. With the Access Mode POA loaded, a user will do the following:

- Exit their GroupWise client session connected to their live mailbox.
- Direct their GroupWise client to the IP address and port that the Access Mode POA is listening at on the Reload box.
- When a user logs into the Access Mode POA on the Reload box, it's as if the user is going back in time. They will see their GroupWise mailbox in the state it was when the backup was performed, for the day that you as the administrator selected.
- If a user wishes to actually retrieve and restore an email item to their live mailbox they would take the following steps:
 - Highlight the item
 - Select Actions|Move to Archive
 - Exit the GroupWise client session with the Access Mode POA on the Reload server
 - Return to GroupWise connecting to the live mailbox
 - Select File|Open Archive
 - Highlight the archived item, and select Actions|Move to Archive
 - Exit the archive mailbox by selecting File|Open Archive
 - The item will now be restored to the user's live GroupWise mailbox Using Access mode, the GroupWise client does not need any special plug-ins or file access in order to access the backed up message store. The user simply needs to point their GroupWise client at

the correct TCP/IP address and port to talk to the POA on the Reload server that was loaded from Reload Administration.

- If the archive path is not specified when the backup is made, then the path will need to be configured in the client while connected to both the reload and the production servers.

Access Mode has the following benefits and limitations:

- GroupWise client, version 6.5 and up, may be used in order to access backed up mail.
- The GroupWise password from the time the backup was performed may be needed. Generally this is not a problem, but sometimes it can be if a user changed their password, and cannot remember their old password. If the GroupWise post office is configured to use LDAP, then users do not need to remember an old password, their current password will work.
- Users use the Archive feature unless archiving is turned off.

Restore Mode – NetWare or Windows Post Offices (Not Linux Post Offices)

With Restore Mode, a GroupWise POA on the Reload server loads against the Live GroupWise post office that the Reload profile represents. As the administrator, you will still choose the backup that represents the particular day that you want to access e-mail from. With the Restore Mode POA loaded, a user will do the following:

- Exit their GroupWise client session connected to their live mailbox.
- Direct their GroupWise client to the IP address and port that the Restore Mode POA is listening at on the Reload box.
- When a user logs into the Restore Mode POA on the Reload box, they will actually see their current live mailbox.
- For a user to retrieve and restore an email item to their live mailbox:
 - Select File | Open Backup
 - Highlight the item that they wish to restore.
 - It is possible that the email item is in the trash bin within the backup. The user must first, undelete the item within the backup.
 - Select Actions | Restore
 - Exit the GroupWise client session with the Restore Mode POA on the Reload server
 - Return to GroupWise connecting to the live mailbox
 - The retrieved email item will now be in the user's live mailbox

Restored items will be returned to the location they were when the backup was taken. So, even though an item in the trash during the backup was undeleted and moved to the mailbox folder, and then restored, the item is actually restored to the live trash. The user will need to undelete the item from their master trash mailbox, and then the email item will be available in their mailbox for them to use again.

To use Restore mode, the GroupWise client does not need any special plug-ins or file access in order to reach the backed up message store. The user simply needs to point their GroupWise client to the correct TCP/IP address and port to talk to the POA on the Reload server that was loaded from Reload Administration.

Restore Mode has the following benefits and limitations:

- Restore Mode requires the GroupWise 7.0.1 client or better.
- User's only need to know their current password in order to use Restore Mode
- Users do not need to use the Archive feature, which is particularly helpful in organizations in which Archiving has been disabled.
- Restore Mode loads a GroupWise POA on the Reload server, running against the live post office. Using the Restore Mode POA is only feasible in environments in which the Reload server is in close network proximity to the live post office that Reload is servicing. If the network stability is in question in any way, it would be better to use the Access Mode POA.

- The Restore Mode POA in no way routes e-mail on the live post office.
- The Restore Mode POA also does not process administrative requests; it only accepts client/server connections.

Standard (Incremental) Backups

Generally you would pull a **Standard Backup (Incremental Backup)** every day. However, with the Reload Job Creation Utility, which is discussed in more detail in Chapter 7, you can pull backup jobs more often than once a day. Here are some important points to remember about Standard Backups:

- A **Standard Backup** equals approximately 12% of the size of the post office that the Reload profile is backing up.
- Only **Three Standard Backup** sets are retained per day. If you were to cause Reload to run more than three Standard backups in a day's time, Reload would actually get rid of all but three of the backups for a particular day. This is done so as to make sure to keep disk space usage down. Many customers will only need one Standard Backup per day.
- If **SmartPurge** is enabled, then after Reload backs up the GroupWise post office for a particular Reload profile, it flags the timestamps of the mailboxes to indicate that the backed up message items can be purged at will.

Portable (Full) Backups

A **Portable (Full Backup)** in Reload is different from most full backup jobs with other backup software in the following manner:

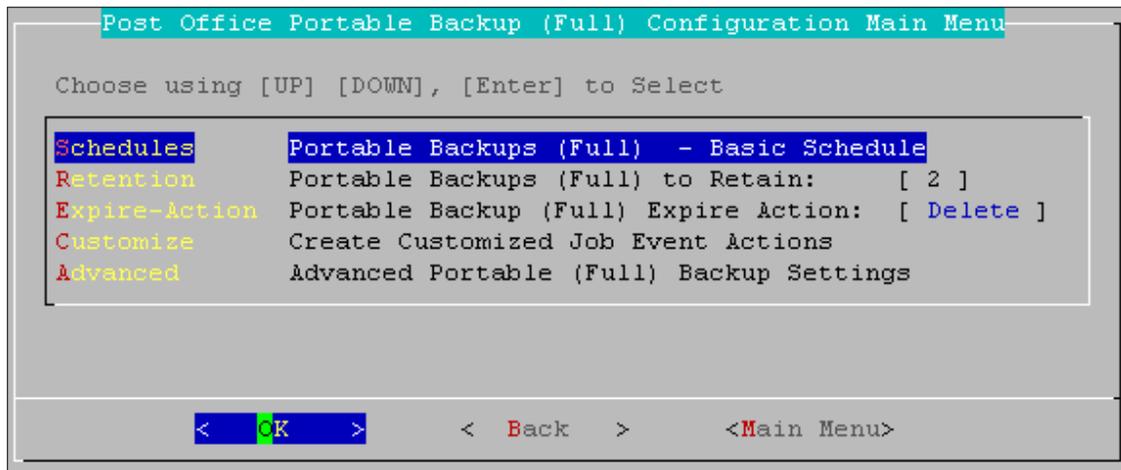
- A **Portable Backup** (Full backup) is done **once a week**, but the Portable Backup wraps up the week's Standard Backups (Incremental Backups), and is considered the ending of the week's backup cycle.
- **Portable Backups are not taxing** on the server that is running the live GroupWise post office. Because of this, it is very feasible to configure Portable Backups to happen in the middle of the day.
- **Portable Backups** require very little bandwidth. There is nothing actually being pulled from the live server, except for directory listing information when the Reload Agent's sub-process called "GRE_FULL_BLOBS" runs.
- **Standard Backups (Incremental Backups) are much more bandwidth intensive than a Portable Backup.** So if a GroupWise post office is 100 Gigabytes in size, then 12 Gigabytes will be pulled across the network to accomplish a typical Standard Backup process.
- **Portable Backups run significantly faster than most backup solutions that pull a full backup.** The reason for this is that Reload keeps a "master" copy of the post office's "OFFFILES" directory contents. After a Portable Backup is created, Reload synchronizes its' master copy of the OFFFILES directory contents with the live post office. Because of GroupWise's superior design, approximately 90% of its size on disk is kept in the OFFFILES directory. The contents of the OFFFILES directories only change on average by about 14% a week. Reload simply needs to synchronize its' master copy of the post office's OFFFILES directory to account for approximately a 14% change in content in order to be in perfect sync with the post office. This process appends very quickly when compared to the process that most Backup software needs to perform a full backup.

Expire-Portable Full Backups

It is very important that you design the Expire-Portable Backups process to run in a scheduled manner. **If the Expire-Portable Full Backups process does not run, the Reload server will eventually run out of disk space.** The Expire-Portable Full Backups process should generally be designed to happen right after a Portable Full Backup is created. Doing this will keep disk space usage at a minimum. One customer has 6 profiles on a Reload server. We'll call them Profile1, Profile2, etc. Here is how their Portable Backups and Expire-Portable Full Backups jobs are scheduled:

Profile Name	Portable Backup Time	Expire-Portable Backup Time
Profile #1	Sunday 01:00:00	Sunday 01:05:00
Profile #2	Sunday 02:00:00	Sunday 02:05:00
Profile #3	Sunday 03:00:00	Sunday 03:05:00
Profile #4	Sunday 04:00:00	Sunday 04:05:00
Profile #5	Sunday 05:00:00	Sunday 05:05:00
Profile #6	Sunday 06:00:00	Sunday 06:05:00

It is not a problem if the Portable Backup job takes longer than the 5 minutes before the Expire-Portable Backup job queues up. **Reload processes queued jobs according to the order that jobs are queued.** If two Reload profiles are scheduled to do an action at exactly the same time, then the profile that is in a higher alphabetical order will have its' job queued first. The Expire-Portable Backups process determines if a Portable Backup needs to be deleted as shown. The menu setting is found under **Profiles | Select desired profile | Portable.**



The Expire-Portable Backups process looks in the <Reload Profile Path>/backups directory, and looks for any <number>-week* directories. The directory with the lowest number on the farthest left-hand side of the directory name is the first directory that will be expired. The Expire Process can actually "Archive" an expired Portable Backup.

Tape Archive Backups

Tape Archives can be created from a Reload Portable Backup. The Tape Archive process should be designed to happen sometime after a Portable Backup is created. The Tape Archive process acts independent of other processes. So the Tape Archive process does not create a *.tar file of a Portable

Backup just before it is expired for example. Generally, you will design the Tape Archive process to happen as often as Portable Backups happen.

Determining Disk Space Needed for Backups

A Portable Backup is called “Portable” because the Portable backup set can be moved to another location, or committed to tape as a single Tape Archive (*.tar) file, and is entirely self-contained so that it can be moved off of the Reload server as needed.

Each portable backup uses on disk, approximately 250% of the size of the GroupWise post office that the profile represents. So if a post office is 100 gigabytes in size, the size of 7 day’s worth of backups, all wrapped up in a Portable Backup would cost 250 Gigabytes on disk.

Reload was designed with the following **observations in mind**:

- **25% of the time**, when data needs to be retrieved from backup, **the most recent backup is used.**
- **2-3 weeks worth of backups** retained on the Reload server **is going to fulfill 98% of customer’s needs** for easily accessible backups on the Reload server
- The other **2% of the time in which data is needed from a different time period, (such as 6 months ago), and then data will need to be retrieved from Tape.** Let’s say, that you want to calculate the disk space needed in order to have **2 weeks** of backups always available on the Reload server.

For a detailed example and calculation of disk space usage, see the following link:

<http://support.gwava.com/kb/?View=entry&EntryID=514>

When a Portable Backup is created, **expired Portable Backups are not deleted right away.** In a typical customer scenario, the expiring Portable Backup will actually be deleted later in the day after a new Portable Backup is created. This being the case, you need to add the cost of the third Portable Backup on the day that the newest Portable Backup is created. In total, the **peak disk space needed for two weeks of backups on a 100 GB Post Office would be 750 GB.**

Reload can take Portable Backups, and wrap them up into a single Tape Archive (*.tar) file. The *.tar file can then be committed to tape. Whenever a *.tar file is created, sufficient disk space equivalent to the size of the Portable Backup should be available for the creation of the *.tar file. A more in-depth discussion on creating *.tar files, will be discussed in greater detail later on in this chapter; outlining a fuller explanation of the advantages and methods of using Reload to create *.tar files.

When you configure a profile, you indicate how many Portable Backups to retain. When Reload removes a Portable Backup from the Reload server, it either deletes the Portable Backup, or it can be configured to “Archive” the Portable Backup. Later on in this chapter an explanation of how to configure Archives will be outlined. In order for Reload to expire Portable Backups, two things must be configured.

1. The number of Portable Backups to retain must be specified.
2. A scheduled “Expire” job must be created to run the backup expiration process.

Integrating Third-Party Backup Solutions with Reload

Some customers may want to do the following with Reload:

- Allow Reload to pull nightly backups from GroupWise post offices
- Backup up the GroupWise post offices each night from the Reload server using a third-party backup solution, this is feasible with Reload. The latest version of the GroupWise post office that the Reload profile represents is kept in a directory called:

```
<Reload profile path>/connect/current
```

If you were to view this directory, you would see that this directory looks just like a standard GroupWise post office. The.../connect/current directory is actually linked to the latest Standard Backup (Incremental) for the Reload profile. So when configuring the third-party backup solution, you would simply point the backup software to the.../connect/current directory. You will be required to get a backup agent for the third-party software that will run on Linux. However, the solution does not necessarily need to be integrated with GroupWise in any manner, because the files on the Reload server will not be locked, and data is not being added to the GroupWise message store on the Reload server. Furthermore, the Reload Agent has already flagged the databases on the live post office as having been backed up. And the data on the Reload Server has been flagged in such a manner that nothing in the GroupWise message store on the Reload server can be deleted.

The backup files in the Reload Server can be locked if the Access or Restore mode POA is loaded. Take loaded POA backups into consideration during a third-party backup.

Backup Schedule Times

Reload still uses the common model that most backup solutions use. That is, incremental backups (Standard Backups in Reload) are generally configured to happen each day, and full backups (Portable Backups in Reload), are generally configured to happen once a week. Specific schedules are configured inside each individual profile.

Creating a Reload Post Office or Domain Profile

The Reload System performs backup actions on GroupWise domains and post offices that are defined as a “**profile**” in the Reload system. **The entire Reload System really exists to manage and act upon the profiles that you create.** A Reload Profile is used for the following:

- To backup GroupWise domains or post offices
- To access backed up data from a GroupWise post office for message recovery and discovery.
- To bring backed up data on-line to be connected to as a live GroupWise post office or domain in a disaster recovery scenario.

Creating a profile is a wizard driven process within Reload Administration. When a profile is created, basic default settings are enabled. To configure beyond the basic defaults you will want to read the later chapters for more in-depth documentation on how to configure profiles beyond the factory defaults.

Reload requires direct file access to backup the Post Office or Domain databases. To accomplish file access, profile creation requires a share to be created on target Linux and Windows GroupWise servers. (NetWare already shares the appropriate files.) Please follow the appropriate instructions for your target servers to create a share.

After your share has been created, continue with profile creation.

Share Creation

Linux

You need to configure the Linux server that hosts the GroupWise post office or domain, so that it supports an NFS mount point. This way the Reload Agent can mount the NFS mount point on the remote server that has the GroupWise post office on it. The mount point should support a Read/Write [RW] NFS mount; Reload needs the ability to write to and modify files. The Reload server does not ever delete post office or domain type files when connected to a server that houses a GroupWise post office or domain.

Setting up NFS, can be tricky depending on your system. These courtesy instructions utilize YaST 2, and will not match every server environment. Most SUSE systems should work with these instructions, or be very similar.

Perform the following steps on the Linux server that houses the GroupWise post office or domain:

1. If you are in a graphical Xwindows type session to your Linux server, the quick command to get to the YaST 2 NFS Server module **yast2 nfs_server &**. Per the prompts, **allow the NFS Server to be started**, and then create an NFS mount point by doing the following.

If a post office were at the following path `/data/grpwise/po1`, then you could create an NFS mount point right at: `/data/grpwise/po1` by doing the following:

2. Select **"Add Directory"**
3. In the Directory to export dialog, **browse to, or type in the path to the post office or domain**, which in our example would be: `/data/grpwise` and `/data/grpwise/po1`
4. When prompted in the next dialog for the Hosts wildcard and Options, do the following:
5. **Hosts Wildcard Field:** `<The IP Address of the Reload Server>` (For Example: `10.1.1.100`)
6. **Options Field:** `rw,no_root_squash,sync`
7. Select **Finish** to apply the changes.

If you cat the `/etc/exports` file: **cat /etc/exports** you will see the new NFS export that you created.

For Example:

```
/data/grpwise/po1 10.1.1.100(rw,no_root_squash,sync)
```

To confirm that the NFS server is running type:

```
ps -eaf | grep nfsd
```

This command should present something similar to this if the NFS Daemon is running:

```
root 2942 1 0 Nov17 ? 00:00:00 [nfsd]
root 2943 1 0 Nov17 ? 00:00:00 [nfsd]
root 2944 1 0 Nov17 ? 00:00:00 [nfsd]
root 2945 1 0 Nov17 ? 00:00:00 [nfsd]
```

Now that the NFS server is on the server where the GroupWise post office or domain is, it can serve up the path of the GroupWise post office or domain. Now you can create a profile for the post office or domain inside of Reload Administration.

Create a separate export for each Post Office and Domain.

Windows

The Reload Server connects to a Windows server using the "CIFS" client that is included on the Linux platform. CIFS may be difficult to work with, because sometimes the underlying protocols for CIFS are disabled through routers. So, it may be necessary to have the Reload Server on the same network segment as the Windows GroupWise server with the target Post Office or Domain. The Windows server must have a Windows Share available for the Reload Server to connect to. **The following are steps used on a Windows 2000 Server to create a Windows share.** The steps appropriate for your server may vary. In the following example, the GroupWise post office is on d:\grpwise\po1

In Windows Explorer highlight the folder for the post office path at: d:\grpwise\po1

1. Select: **File Properties**
2. Select the tab across the top of the dialog box: **Sharing**
3. Choose the option: **Share this folder**
4. **Give the "Share" a name, and take note of the name** you will need it when creating the Reload Profile for this post office.
5. Select the tab across the top of the dialog box: **Security**
6. Choose a **user**, or add a user that will have the following **rights: Modify, Read & Execute, Write, List Folder Contents and Read**
7. This completes the process of making a Windows share. For troubleshooting purposes, first try to map a drive from a Windows workstation to the Share that was just created. Then create a file in the post office or domain directory before trying to create the Reload Profile for this post office or domain.
8. Now that the Windows server where the GroupWise post office or domain is can serve up the path to the GroupWise post office or domain, you can create a profile for the post office or domain inside of Reload Administration.

Profile Creation

1. In Reload Administration select the option “**Create (Create Profiles)**”.
2. Select whether or not to create a post office or a domain profile.
3. Enter a **name** for the profile. **Be aware, that a profile cannot be renamed, once it has been created.** Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office or domain that the profile represents. Select the **Next** button.
4. Enter a **description** for the profile. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the **Next** button.
5. Enter the **path** where the Reload server will store data for this profile. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available; Reload is not configured to mount paths in order to access stored data. Also, the path should be to a location that has a lot of disk space available. Select the **Next** button.
6. Select the server type. This is the target server holding the GroupWise Post Office or Domain Reload is to backup. (Netware, Linux, Windows)
7. Select standard or cluster server type, as appropriate.
 - a. (Windows servers will not have this option.)
 - b. **For a NetWare Cluster system, you must also indicate the IP address of the NetWare Cluster Resource and the volume on the resource that houses the GroupWise post office or domain.**
8. Select the **Next** button.
9. Indicate the path to the GroupWise Post Office or Domain on the target server.
 - a. **NetWare UNC path for standard NetWare servers:** Make sure to use the following convention: `\\<server name>\<volume>\<full path to p.o. or domain>` For example: [\\wwwfs1\vol1\apps\grpwise](#)
Select the **Next** button. Fill in the **TCP/IP address** of the NetWare server. Select the **Next** button
 - b. **NetWare UNC Paths for Cluster Systems:** Make sure to use the following convention: `\\<cluster resource ip address or DNS>\<volume>\<full path to post office or domain>`
For example: [\\137.65.55.211\vol1\apps\grpwise](#)
 - c. **Linux servers (cluster and standard):** Fill in the **TCP/IP address or DNS name** of the Linux Server. Select the **Next** button. Indicate the **NFS Export Path** on the Linux server that houses the GroupWise post office or domain. Select the **Next** button. Make sure to use the following convention: `/<full path to post office or domain via the NFS Export Path>` For example: `/data/apps/grpwise` Select **Next**. Linux users now move to step 13.
 - d. **Windows Servers:** Fill in the TCP/IP Address of the Windows Server and select **Next**. Indicate the **Windows Share Name** on the Windows server that houses the GroupWise post office. Select the **Next** button. Make sure to use the following convention: `<Windows Share Name>` For example: `grpwise`
10. Select the **Next** button.
11. Reload needs authentication information for NetWare and Windows systems.
 - a. **NetWare:** Specify the user name of an **eDirectory user** with **[RWMF] rights at the post office or domain path**, and the directories off of the post office or domain path. It's

probably best to create a user just for this purpose. The name of the user should be specified using their "**typless**" eDirectory username. For example: **reload.apps.acme**

- b. **Windows:** Specify the user name of a Windows user with the following rights: **Modify, Read & Execute, Write, List Folder Contents and Read at the post office path**, and the directories off of the post office path.
12. Select the **Next** button. Now indicate the **password** for the user that you specified in step 11. (The password does not display on the screen or in any log file. The password is kept in one ASCII text *.conf file on the Linux server. The directory where this *.conf file is located is: /opt/beginfinite/reload/conf.)
13. Select the **Next** button. At this point, you can go back in the wizard and make any needed changes, but **when you select the "Next" button after the password prompt, there is no going back to the wizard.**
14. Select the **Next** button.
15. Now the profile creation wizard gives a summary of the newly created profile. The profile is actually created at this point, but it does need to be **tested and initialized**. Until a profile is tested and initialized, it cannot be used in any manner. The testing process confirms that the Reload server can actually access the GroupWise post office or domain with the information you filled out in the profile creation wizard. For post offices, the initialization process actually pulls down the contents of the post office's OFVIEWS directory and the NGWGUARD.DC from the post office directory.

At the **Test and Initialize** screen you can either test the profile now, or you can choose to test it later. Until the profile is tested, it will not be usable. Most customers will want to choose **Test** to immediately test and initialize the profile.

Testing and initializing a profile, does not backup the post office or domain in any way.

The Test and Initialize utility gives a verbose, step-by-step explanation of each action that it is performing. If the profile does not successfully pass the testing process it should be easy from viewing the log, to see why it failed. You can then modify the profile by going to the "Create (Create Profiles)" menu from the Main Menu again, and selecting "Modify a Profile". Once the profile is modified, it can be tested again. If you want to see the log file from previous testing attempts on a particular profile, select the option "View" from the Create Profile menu, and you can view the testing log for any profile.

Once a profile is tested and initialized successfully, the profile is available to be configured further. The default configuration of a profile is sufficient for making quickly accessible backups with Reload.

Creating a Remote Reload Profile for a Reload Post Office or Domain Profile on a Different Reload Server.

There are several reasons why you would want this kind of a profile. For example: A firm has a site in Chicago and a site in New York. The firm likes Reload's abilities to do backups, but they are also interested in using Reload as an offsite disaster recovery solution for each of their sites.

Here is how they should design their system and specific benefits to this model:

- Setup a Reload server in Chicago to backup the post office and/or domain in Chicago
- Setup a Reload server in New York to backup the post office and/or domain in New York
- In Chicago, make an additional Reload profile that represents New York, but that pulls its data from the Reload server in New York rather than the live GroupWise post office in New York
 - **IMPORTANT:** The Reload profile in Chicago that is backing up New York from the Reload server in New York should have the profile setting of "Flag Messages Purgable After Backup" as "Disabled".
- In New York, make an additional Reload profile that represents Chicago, but that pulls its data from the Reload server in Chicago rather than the live post office in Chicago
 - **IMPORTANT:** The Reload profile in New York that is backing up Chicago from the Reload server in Chicago should have the profile setting of "Flag Messages Purgable After Backup" as "Disabled". Using this method of backing up a GroupWise post office or domain from a Reload server versus the live GroupWise post office or domain is ideal for the following reasons:
- Backup times are significantly improved using this model
- Databases on the live GroupWise post offices are not being backed up over a WAN link. A network outage could introduce database damage. In the case of a Reload to Reload backup, a database on the Reload server could get corrupted, however at least a database on the live post office will not get corrupted.

You need to configure the Linux server that hosts the Reload Profile (we'll call this the First Reload Server), so that it supports an NFS mount point. This way the Reload Agent on the Second Reload Server can mount the NFS mount point on the First Reload Server. The NFS mount point should support a Read/Write [RW] NFS mount.

Setting up NFS, can be difficult. Follow the NFS share creation [instructions for Linux](#). **Make sure to share the data path for the Reload Server.** (This is the location that Reload was told to store the backed up data.)

Once the NFS server on the First Reload Server can serve up the path to the original Reload profile, you can create a profile for the post office or domain inside of Reload Administration on the Second Reload Server.

1. In Reload Administration on the Second Reload Server, select the option "**Create** (Create Profiles)".
2. Select "**Create**" again
3. Enter a **name** for the profile. **Be aware, that a profile cannot be renamed, once it has been created.** Choose the name wisely. Perhaps you will want to name the profile so that its name is the same as the GroupWise post office that the profile represents.
4. Select the **Next** button.
5. Enter a **description** for the profile. The description of the profile will be added to the Agent Log when backup jobs are run for the profile. Select the **Next** button.

6. Enter the **path** where the **Reload server will put backed up data** for this profile. This path can be a location on the Linux server, or an NFS mount to another Linux/Unix server, or to a SAN. The path should always be available, Reload is not configured to mount paths in order to access Reload backed up data. Also, the path should be to a location that has a lot of disk space available. Select the Next button. ***The profile path also cannot be changed.***
7. Select the server type **Reload**. Select the **Next** button.
8. Fill in the **TCP/IP address or DNS name** of the Reload Linux Server. Select the **Next** button.
9. Indicate the **NFS Export Path** on the First Reload Server that houses the Original Reload Profile. Select the **Next** button. Make sure to use the following convention: **/<full path to Original Reload Profile via the NFS Export Path>**
For example: **/data/reload/po1**
10. Select the **Next** button. **At this point, you can go back in the wizard and make any needed changes, but when you select the "Next" button after the path prompt, there is no going back to the wizard.**
11. Select the **Next** button.
12. Now the profile creation wizard gives a summary of the newly created profile.
13. The profile is actually created at this point, but it does need to be **tested and initialized**. ***Until a profile is tested and initialized, it cannot be used.*** The testing process confirms that the Reload server can actually access the GroupWise post office or domain with the information you filled out in the profile creation wizard.
14. At the **Test and Initialize** screen you can either test the profile now, or you can choose to test it later. ***Until the profile is tested, it will not be usable.*** Most customers will want to choose Test to immediately test and initialize the profile.

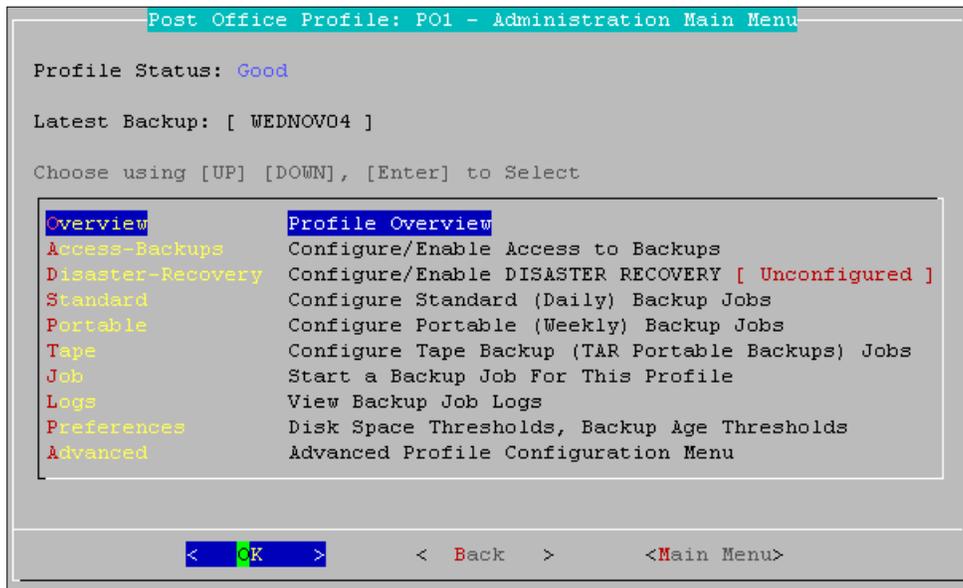
The Test and Initialize utility gives a verbose, step-by-step explanation of each action that it is performing. If the profile does not successfully pass the testing process it should be easy from viewing the log, to see why it failed. You can then modify the profile by going to the "Create (Create Profiles)" menu from the Main Menu again, and selecting "Modify a Profile". Once the profile is modified, it can be tested again. If you want to see the log file from previous testing attempts on a particular profile, select the option "View" from the Create Profile menu, and you can view the testing log for any profile.

Once a profile is tested and initialized successfully, the profile is available to be configured further. The default configuration of a profile is sufficient for making quickly accessible backups with Reload. However there are several other features in Reload that you may want to enable. See the chapters later in this documentation for detailed descriptions of the many feature settings available on a profile.

Basic Reload Post Office Profile Configuration

All of the basic settings of a profile are accessible by selecting the following from the Main Menu.

Profiles | select desired profile. By default, you should see the Profile Configuration Main Menu. If you have not yet configured the Disaster Recovery section, you will see a red warning that it is unconfigured.



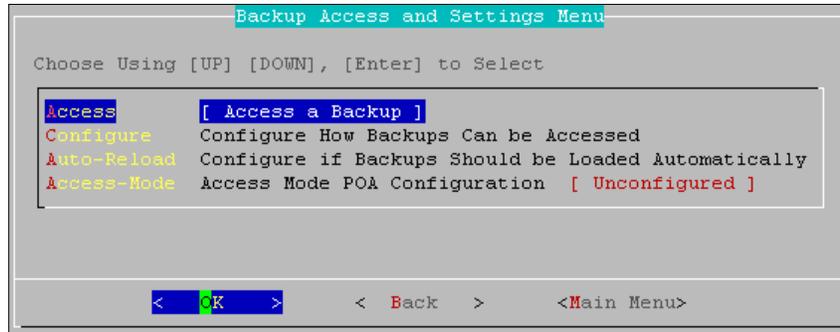
Overview

The Overview gives you detailed information on the general function of the Profile you selected. This option is just an informational display, but contains useful information about the Profile:

- Name
- Description
- Status
- Path to stored data
- Live POA platform
- Latest backup name
- Latest backup elapsed time
- Average backup time
- Disaster recovery status
- Hot backups status
- Quick Restore status
- Tape backup enhancement status
- GWAVA Retain Collection status
- GWAVA Vertigo restore point statu

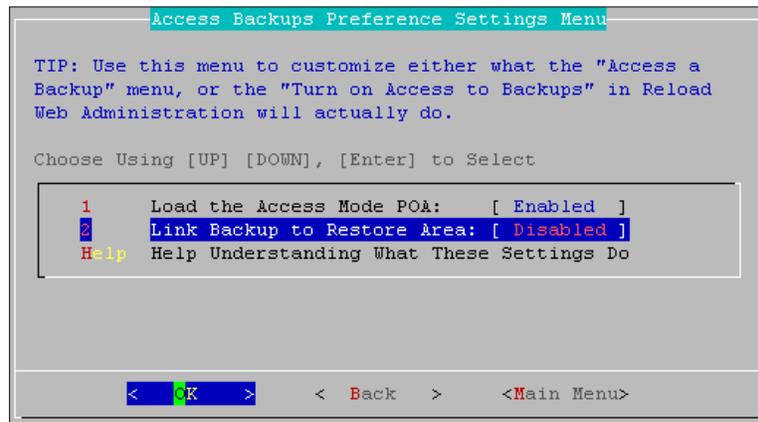
Access-Backups

The Access-Backups menu allows you to access and select a backup to load, configure how backups can be accessed, configure Auto-Reload settings, and configure the Access-Mode POA.



Configure - Access Backup Preferences

The Access Backup Preferences Menu primarily focuses on how backups on the Reload server can be accessed by the GroupWise client. Under the “Configure Access and Restore Mode POA Settings” menu, you can configure what should happen when you use the “**Access Backup**” menu in Reload Administration, or the “**Turn on Access to Most Current Backup**” choice from Reload Web Administration.



In order to understand how to configure these preferences, let’s first explain how Reload backups can be accessed. There are basically three different methods through which a Reload backup can be accessed. Here are notes about all three different methods:

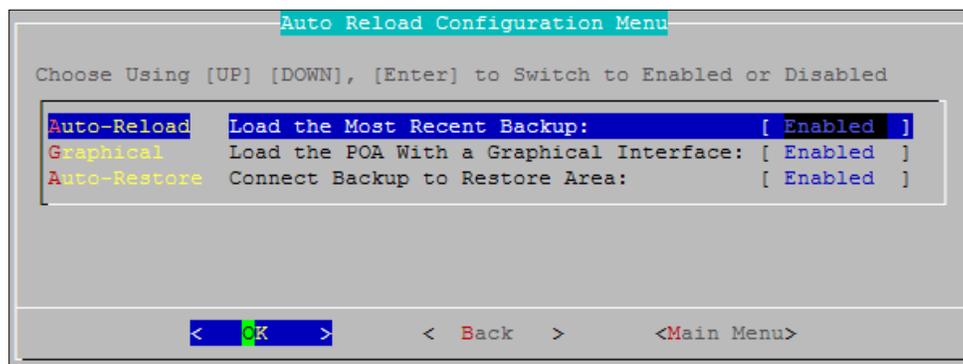
Access Mode - through the Access Mode POA

1. Any GroupWise 6.5 or GroupWise 7.0 client can utilize the “Access Mode POA” loaded against a Reload backup.
2. When the “Access POA” is loaded against a backup, in order for a user to get to the Access Mode POA, they must exit their live mailbox session. Then the user must log in with their GroupWise client to the “Access Mode POA” that has been loaded.

3. When a user logs into the “Access Mode POA”, they will see all of the items in the Reload backup that you have chosen to load.
4. The “Access Mode POA” requires that the user remember their password, at the time that the backup was created, unless you are using LDAP authentication, in which case, the current user’s password will allow the user access to their mailbox.
5. If a user wishes to retrieve message items from the Reload backup to their live mailbox, they must use the GroupWise archive feature in order to do so.
6. An “Access Mode POA” and a “Restore Mode POA” can be running simultaneously against a Reload backup. The “Restore Mode POA” and the “Access Mode POA” need to be configured in such a manner that there is not a port conflict.
7. If you are using GWAVA Reveal or Retain to integrate with Reload, the “Access Mode POA” must be loaded for use with these products.
8. See [Restore POA Configuration](#) for instructions on modifying the Access POA settings.

Auto-Reload Restore Area Access – Linux Post Offices Only

1. Because the Reload server is a Linux server, Linux post offices can be configured to access the Reload server with an NFS mount. With this configuration in place, users do not need to exit their GroupWise client to access a Reload backup. They can use the File|Open Backup feature within GroupWise.
2. Configuring a GroupWise Restore Area for a Linux post office is explained in the advanced profile configuration section.
3. Auto-Reload Preferences Menu



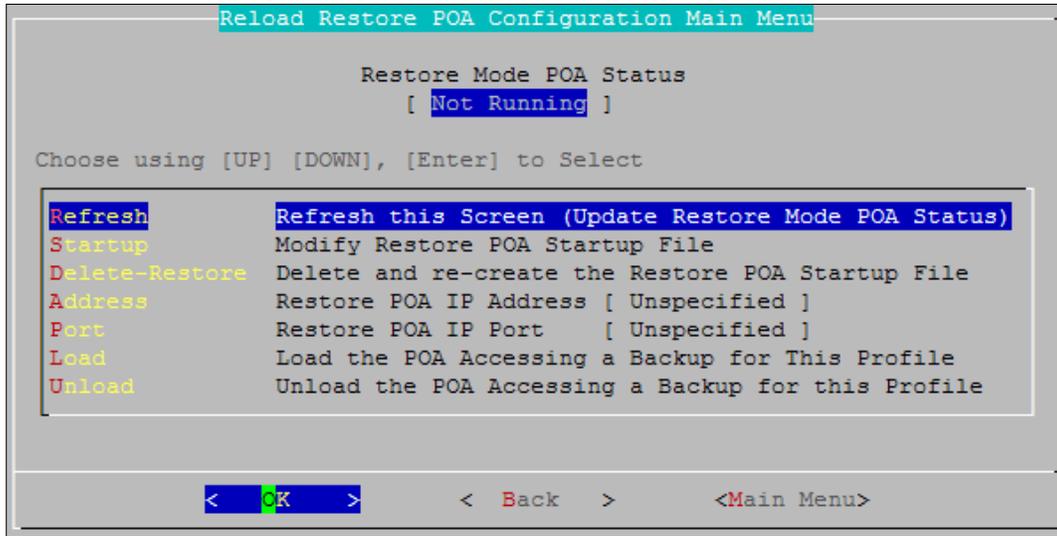
Auto-Reload is a feature that can do the following:

- Automatically loads the latest backup for a profile
- Loads the GroupWise Access and/or Restore Mode POAs either in the background, or with a graphical interface if needed.
- Connects the latest backup to the Restore Area (really only useful for Linux post offices)

In most customer environments, the most recent backup, is used approximately 25% of the time. Because of this, the Auto-Reload feature can be useful. By enabling Auto- Reload, the most recent backup is made available for GroupWise client connections. In effect users will have immediate self-service access to the most recent backup. This feature reduces the Reload administrator’s need to load the latest backup.

Restore POA Configuration

From the “**Restore**” menu you can modify the behavior of the Restore POA for a Reload Profile. The Restore POA is the POA that is loaded when a user needs to access the Reload server to retrieve backed up data via the File | Open Backup feature.



By default when loading a GroupWise POA accessing a Reload generated backup, the POA will listen on all IP addresses bound to the Reload Server, on the default port that the POA is configured to listen on. In some environments, this will work fine. However, in others, particularly those where the Reload server is housing several Reload Profiles, the behavior of the GroupWise POA needs to be configured differently.

Imagine the following example. ACME Corporation is using their Reload server to backup all three GroupWise post offices. The names of these post offices are:

- PO1 (po1.acme.com)
- PO2 (po2.acme.com)
- PO3 (po3.acme.com)

ACME wants to use the “Auto-Reload” feature as explained in Chapter 6. In their live GroupWise system, each of the GroupWise post offices is listening on port 1677. ACME would like to keep this same TCP port convention for user’s convenience when connecting to the Reload server. Here’s how then can accomplish this task:

- Bind the Reload Server to three different IP Addresses
- Configure the Restore settings for the Reload Profile so that the POA for that Reload Profile is using just one of the three IP Addresses
- For ease of use purposes, consider binding in the DNS server, the IP Addresses to logical names, for example:
 - PO1 on the Reload Server: **po1.backup.acme.com**
 - PO2 on the Reload Server: **po2.backup.acme.com**
 - PO3 on the Reload Server: **po3.backup.acme.com**

Managing Port Conflicts

If you do not configure the Reload server with multiple IP addresses, then you will need to modify the Restore POA's IP Port in most circumstances. Imagine that you are trying to load two POAs for different Reload Profiles. If both of the GroupWise post offices are configured to use port 1677 for example, there will be a port conflict when trying to load a second POA for a different Reload Profile. You could choose to change the Restore POA's ports so that only one of the POAs is using 1677, and another might be using 1678, etc.

Modifying a Reload Profile's Restore POA Startup File

In most customer environments, there is no need to modify the Access POA's startup file. However in some environments, especially those using LDAP, or SSL, there will be a need to modify the POA's startup file to add additional settings to the POA's startup file. You can do so by choosing the menu **Startup** (Modify Restore POA Startup File).

Using the menu option to modify the Access POA startup file, it only works if you are in an XWindows environment. So if you were SSH'd over to the Reload server, you will not be able to use this menu option. In an SSH session, the Reload administration utility will let you know what path the Access POA's startup file is located at so you can edit it with an editor such as vi. To change the default editor that Reload uses go to the following menu location in Reload Administration System | Editor, and choose the editor that will work in your environment. For a KDE desktop KWRITE, KATE and GEDIT will all work. For a GNOME desktop, only GEDIT will work. Modifying a Restore POA's Connectivity Settings

The Restore Mode POA loads against the live post office that the profile represents. As such, the Restore Mode POA needs to have all rights to the GroupWise post office in order to modify the databases at the post office. In order to accomplish this, the Restore Mode POA needs authentication credentials to be given full access to the live credentials.

Creating a GroupWise Restore Area for use with Reload – NetWare and Windows Post Offices

Using a Restore Area in conjunction with Reload is only valid if your users are using the GroupWise 7.0.1 client or later. In order to use the Restore POA functionality, you must create a GroupWise Restore Area in ConsoleOne. Once the Restore Area is created, and assigned to a post office, there are no other steps you need to take in ConsoleOne in order to use the Restore Area. Reload links up the backup that you wish to access, with the Restore Area path that you specify once in ConsoleOne.

Here are the steps to follow in ConsoleOne to create a GroupWise Restore Area:

1. Launch ConsoleOne
2. In ConsoleOne get connected to the Primary Domain. The reason for this is that GroupWise Restore Areas are considered "System Level Records" and as such, they are owned by the Primary Domain.
3. In the GroupWise view, highlight a domain in the GroupWise system, and select Tools | GroupWise System Operations | Restore Area Management
4. Select the "Create" button to create a new Restore Area. This Restore Area will be specific to a particular post office that Reload is backing up. Each post office that Reload is backing up will need its own Restore Area.

5. Give the Restore Area a name. For example, CORPPO-Reload
6. In the UNC path field, indicate the following path:

<entire path to the Reload profile on the Linux server>/connect/restore

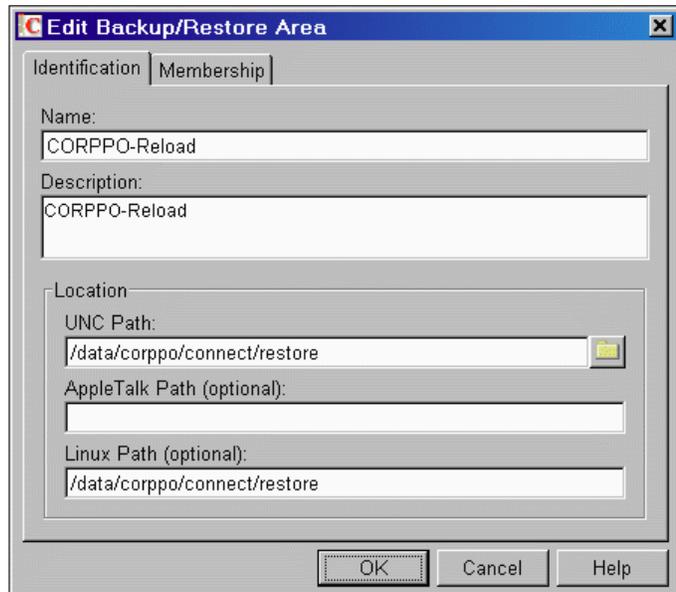
For example:

/data/corppo/connect/restore

If you wish to determine the path to the Reload profile, edit the profile in Reload Administration, and select the menu choice INFO – Profile Information.

It may not seem logical to put a Linux path in a UNC path, but because Reload is on Linux, this is the only way it will function.

7. In the Linux path field, fill in the exact same path that you did before, namely:



<entire path to the Reload profile on the Linux server>/connect/restore

For example:

/data/corppo/connect/restore

The Restore Area should look something like the settings shown here.

8. At the Membership tab, select the Add button, and add the GroupWise post office that this Restore Area represents.

The changes you made in ConsoleOne could take a few minutes to replicate. Once they do, the Restore Area functionality is immediately available via the “Restore Mode POA”. You do need to configure the Restore Mode POA as explained just a little earlier. And you must load the Restore Mode POA in order for users to be able to access the Restore Mode POA. All of the pertinent steps for using a Restore Mode POA have been discussed previously. Here is a brief outline of the steps that you need to take in order to use a Restore Area and the Restore Mode POA.

Steps to create and use a Restore Mode POA

1. Create a Restore Area in ConsoleOne.
2. Configure the Reload post office profiles’ Restore Mode POA Connectivity settings in Reload Administration.
3. Configure the Reload post office profiles’ Access Backup Preferences, so that the Restore Mode POA is loaded when you choose a backup.
4. Have the user connect to the Reload server, and restore e-mail.

Here is a quick review of how the Restore Mode POA is able to assist the GroupWise 7.0.1 client in accessing the Reload backup as a Restore Area:

1. The GroupWise client connects to the Restore Mode POA
2. As the GroupWise client connects to the Restore Mode POA, it reads the Restore Area record from the post office database
3. The GroupWise client determines if it has connectivity to the UNC or Linux path as indicated in the Restore Area record.
4. The GroupWise client determines that it does not have connectivity to the path where the Restore Area is.
5. The GroupWise client asks the GroupWise POA (Remember this is the GroupWise POA running in Restore Mode on the Reload server) if it has access to the Restore Area's UNC or Linux paths.
6. The GroupWise POA on the Reload server responds that it does have access to the path.
7. After the GroupWise client loads, when the user selects File|Open Backup, they are actually accessing the Reload backup on the Reload server via the Restore Mode POA's access to the Restore Area.
8. When a user restores an item, the Restore Mode POA, which is accessing the users' live GroupWise post office, along with access to the Reload backed up GroupWise post office, will read mailbox email items out of the Reload backup, and commits the live GroupWise post office, based upon GroupWise client requests to restore message items.

Creating a GroupWise Restore Area for use with Reload – Linux Post Offices

If a GroupWise post office is on the Linux platform, then using Reload is even simpler. In fact, users don't even need to exit their live GroupWise account to leverage Reload. The users only need to use the File|Open Backup feature in GroupWise to access a Reload backup. With Reload in play, the experience of using Reload from within the GroupWise 7.0.1 client feels completely natural. You need only to do some pre-configuration once to enable this feature for all users on a Linux-based post office. Here is a high-level outline of what you need to do:

- Configure the NFS Server software on the Reload server, and create an NFS export of the Reload profile directory
- Configure the NFS Client software on the Linux server housing the GroupWise post office, and create a mount point to the NFS export on the Reload server
- Define a GroupWise Restore Area in ConsoleOne that reflects the NFS mount point on the Linux server that houses the GroupWise post office

Configuring an NFS Server Export Location on the Reload Server

Configure the NFS Server software on the Reload server, and create an NFS export of the Reload profile directory. A Linux server allows file access to another Linux server through the NFS (Network File System) protocol. NFS is a reliable and fast file-system based protocol between Linux servers.

When a Linux host wants to share a location on one of its own partitions, it creates an "NFS export".

When the Linux host is running the NFS Server daemon, other Linux hosts running can request an NFS Client mount (much like a mapping) to the NFS Export.

The first item of business then is creating the NFS export, and running the NFS Server on the Reload server. Here are general instructions for doing so, based upon instructions on a SLES10 server, the menu prompts on your Reload server could be different.

- a. Go into the YaST Control Center. For example, if you are in a graphical session, to launch the graphical version of YAST from a terminal session, type in the command:
yast2

- b. Within the YaST Control Center, select **Network Services | NFS Server**
- c. Make sure to Start the NFS Server if prompted to do so
- d. In the Directories to Export screen, select the Add Directory button, and add the Reload profile path for the Reload profile that you are configuring to be accessible as an NFS export. For example:
/data/reload/corppo

If you want to determine the path to the Reload profile, edit the profile in Reload Administration, and select the menu choice INFO – Profile Information.

- e. When prompted in the next dialog for the Hosts wildcard and Options, do the following:
Hosts Wildcard Field: <The IP Address of the Reload Server> (For Example: 10.1.1.100)
Options Field: **rw,no_root_squash,sync**
- f. Select Finish for the changes to take effect.

If you cat the /etc/exports file:

```
cat /etc/exports
```

You will see the new NFS export that you created.

For Example:

```
/data/reload/corppo/ 10.1.1.100(rw,no_root_squash,sync)
```

To confirm that the NFS server is running type:

```
ps -eaf | grep nfsd
```

This command should present something similar to this if the NFS Daemon is running:

```
root 2942 1 0 Nov17 ? 00:00:00 [nfsd]
root 2943 1 0 Nov17 ? 00:00:00 [nfsd]
root 2944 1 0 Nov17 ? 00:00:00 [nfsd]
root 2945 1 0 Nov17 ? 00:00:00 [nfsd]
```

The command script to control the NFS Server is:

```
/etc/init.d/nfsserver
```

So to restart the NFS Server you would type in the command:

```
/etc/init.d/nfsserver restart
```

Configuring an NFS Client Mount Point on the GroupWise Post Office Server

Configure the NFS Client software on the Linux server housing the GroupWise post office, and create a mount point to the NFS export on the Reload server. The way a Linux server gets file access to another Linux server is through an NFS mount. All Linux servers keep their local partition mounts and their NFS mounts in the “fstab” file. The file is located in the /etc directory on the Linux server.

This section walks through using the NFS Client configuration utility in YAST, to define a permanent NFS mount point that the Linux host running the GroupWise post office, will always make to the Reload server. Here are general instructions for doing so, based upon instructions on a SLES10 server, the menu prompts on your Reload server may be different.

1. In a Terminal session or a File Manager on the Linux server, **Create** a new mount point local directory called **“backup”**. Generally mount points are made off of the /mnt directory. In a terminal session to make the mount point local directory type use the **“mkdir”** command.

For example:

```
mkdir /mnt/backup
```

2. **Go** into the YAST Control Center.

For example, if you are in a graphical session, to launch the graphical version of YAST from a terminal session;

Type in the command: **yast2**

Within the YAST Control Center, Select **Network Services | NFS Client**

3. **Select** the **Add** button, to add a new NFS mount point.

4. **Fill** in the fields, for example:

a. **NFS Server Hostname:** <IP Address or DNS Host name of the Reload server>.

For example: 137.65.55.214

b. **Remote File System:** <The NFS export created on the Reload server>.

For example: /data/reload/corppo/

c. **Mount Point (local)** <The local mount point that will become the link over to the Reload server>.

For example: /mnt/backup

d. **Select** the Finish button, to complete the NFS Client mount point.

5. **Select** Finish for the changes to take effect.

If you cat the /etc/exports file:

```
cat /etc/exports
```

You will see the new NFS-based mount point that you created. For Example:

```
137.65.55.214:/data/reload/corppo /mnt/backup nfs
```

The mount point **should already be established**, however if you ever wished to establish the mount point, since it's in the fstab file you would type in the command:

```
mount /mnt/backup
```

The command to dismount would be:

```
umount /mnt/backup
```

Creating the GroupWise Restore Area

Define a GroupWise Restore Area in ConsoleOne that reflects the NFS mount point on the Linux server that houses the GroupWise post office In order to use the Restore functionality, you must create a GroupWise Restore Area in ConsoleOne. Once the Restore Area is created, and assigned to a post office, there are no other steps you need to take in ConsoleOne in order to use the Restore Area. Reload links up the backup that you want to access, with the Restore Area path that you specify once in ConsoleOne. Here are the steps to follow in ConsoleOne to create a GroupWise Restore Area:

1. Launch ConsoleOne
2. In ConsoleOne connect to the Primary Domain. The reason for this is that GroupWise Restore Areas are considered “System Level Records” and as such, they are owned by the Primary Domain.

3. In the GroupWise view, highlight a domain in the GroupWise system, and select Tools|GroupWise System Operations|Restore Area Management
4. Select the "Create" button to create a new Restore Area. This Restore Area will be specific to a particular post office that Reload is backing up. Each post office that Reload is backing up will need its own Restore Area.
5. Give the Restore Area a name. For example, CORPPO-Reload
6. In the UNC path field, indicate the following path:
<path to the NFS client mount point on the Linux GroupWise server>/connect/restore

For example:

/mnt/backup/connect/restore

It may not seem logical to put a Linux path in a UNC path, but because Reload is on Linux, this is the only way it will function.

7. In the Linux path field, fill in the exact same path that you did before, namely:
<path to the NFS mount point on the Linux server>/connect/restore

For example:

/mnt/backup/connect/restore

The Restore Area should look something like this:

The screenshot shows a dialog box titled "Edit Backup/Restore Area" with a blue title bar and a close button (X) in the top right corner. The dialog is divided into two tabs: "Identification" (selected) and "Membership". Under the "Identification" tab, there are several input fields: "Name:" with the text "CORPPO-Reload", "Description:" with the text "CORPPO-Reload", "UNC Path:" with the text "/mnt/backup/connect/restore" and a small folder icon to the right, "AppleTalk Path (optional):" which is empty, and "Linux Path (optional):" with the text "/mnt/backup/connect/restore". At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

8. At the Membership tab, select the Add button, and add the GroupWise post office that this Restore Area represents. The changes you have made in ConsoleOne may take a few minutes to replicate. And once they do, the Restore Area functionality is immediately available via the File|Open Backup feature in the GroupWise 7.0.1 client.

In order to make sure that the latest backup is the one that is immediately available to your users, make sure to configure Reload to allow for this.

Do the following:

- A. Configure the Reload post office profile's Access Backup Preferences, under the Preferences menu, so that Reload links to the Restore Area when you choose a backup. The Restore Mode POA and Access Mode POA do not need to load because the clients are not connecting to POAs on the Reload server.
- B. Configure the Reload post office profile's Auto-Reload configuration under the Preferences menu, so that "Auto-Restore" is enabled. This will ensure that the most current backup is automatically linked to the restore area.

Disaster Recovery POA Configuration

Disaster-Recovery has been consolidated for this release of Reload, and now is entirely accessed through this menu structure, under each profile, the settings applying to the profile selected. The first menu allows for configuring or enabling the Disaster Recovery or Migration mode.



Disaster Recovery has three main modes:

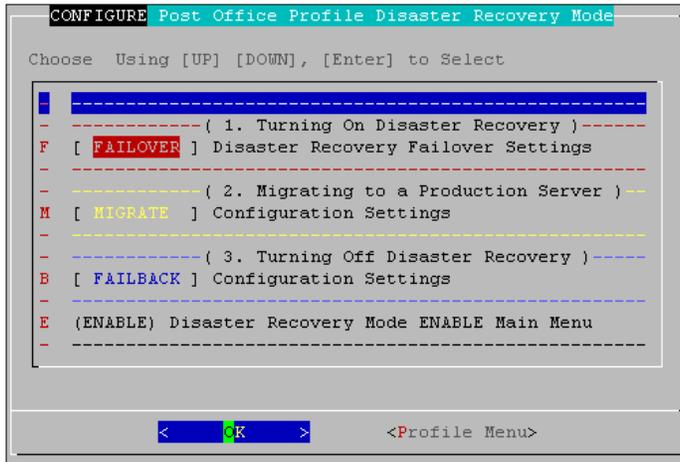
Failover: Reload uses a previous backup of the Post Office, activates a Post Office Agent and connects it to the backup selected. This loads a full functioning GroupWise Post Office.

Migrate: Reload copies the latest or running backup over to the GroupWise system, migrating the backed-up data to the live system, repairing or preventing any data loss.

Failback: Reload closes the active Disaster Recovery POA and returns to normal backup processes.

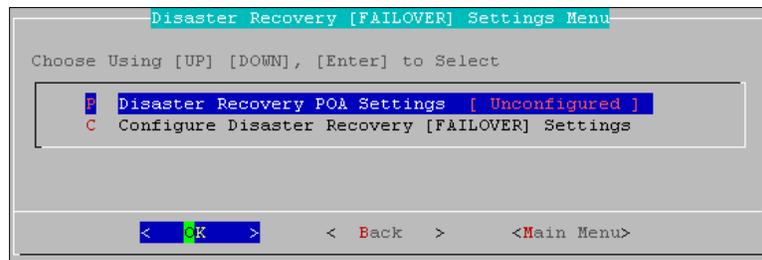
The three modes are sequential steps to fully recover from a complete disaster scenario. To Enable the different modes, select 'Enable' and then, in the subsequent menu, the mode you wish to enable. If Disaster Recovery is unconfigured, a red note will be displayed next to the configure menu option.

To configure the different modes, Select 'Configure' then choose the different mode you wish to configure.

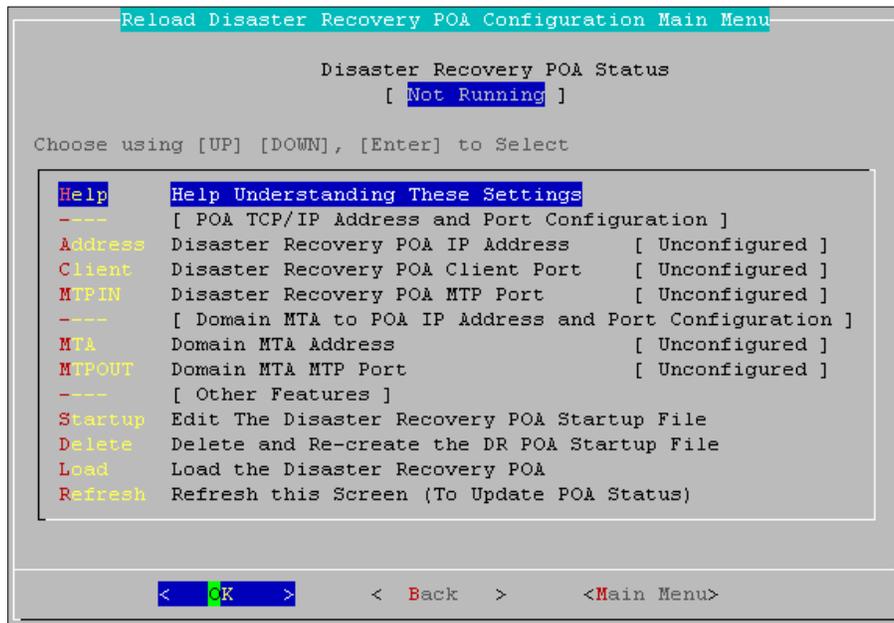


The Failover option allows you to configure the disaster POA in Failover mode. This is the POA that will load when Disaster Recovery is enabled. The unconfigured settings are shown below. The options to edit are shown, allowing extensive control over the behavior of the disaster POA. The 'Help' menu option describes each of the menu items and their use in a console window. Set the IP address and ports according to your GroupWise system needs.

You may select two different sections to configure for Failover mode; the disaster recovery POA settings, and the Failover settings.



Select 'Disaster Recovery POA Settings' to edit the POA connection settings.



By default when loading the disaster recovery POA against a Reload generated backup, the POA will listen on all IP addresses bound to the Reload Server, on the default port that the POA is configured to listen on. In some environments, this will work fine. However, in others, particularly those where the Reload server is housing several Reload Profiles, the behavior of the GroupWise POA needs to be configured differently.

Imagine the following example. ACME Corporation is using their Reload server to backup all three GroupWise post offices. The names of these post offices are:

- PO1 (**po1.acme.com**)
- PO2 (**po2.acme.com**)
- PO3 (**po3.acme.com**)

In their live GroupWise system, each of the GroupWise post offices is listening on port 1677. ACME would like to keep this same TCP port convention for user's convenience when connecting to the Reload server.

Here's how then can accomplish this task:

- Bind the Reload Server to three different IP Addresses
- Configure the **Disaster Recovery POA** settings for the Reload Profile so that the POA for that Reload Profile is using just one of the three IP Addresses
- For ease of use purposes, consider binding in the DNS server, the IP Addresses to logical names, for example:
 - PO1 on the Reload Server: **po1.backup.acme.com**
 - PO2 on the Reload Server: **po2.backup.acme.com**
 - PO3 on the Reload Server: **po3.backup.acme.com**

Managing Port Conflicts

If you do not configure the Reload server with multiple IP addresses, then you will need to modify the Disaster Recovery POA's IP Port in most circumstances. Imagine that you are trying to load two POAs for different Reload Profiles. If both of the GroupWise post offices are configured to use port 1677 for example, there will be a port conflict when trying to load a second POA for a different Reload Profile. You could choose to change the Disaster Recovery POA's ports so that only one of the POAs is using 1677, and another might be using 1678, etc.

Modifying a Reload Profile's Disaster Recovery POA Startup File

In most customer environments, there is no need to modify the Disaster Recovery POA's startup file. However in some environments, especially those using LDAP, or SSL, there will be a need to modify the POA's startup file to add additional settings. You can do so by choosing the menu **Startup** (Modify Disaster Recovery POA Startup File).

Using the menu option to modify the Access POA startup file, it only works if you are in an XWindows environment. So if you were SSH'd over to the Reload server, you will not be able to use this menu option. In an SSH session, the Reload Administration utility will let you know what path the Access POA's startup file is located at so you can edit it with an editor such as vi. To change the default editor that Reload uses go to the following menu location in Reload Administration System | Editor, and choose the

editor that will work in your environment. For a KDE desktop KWRITE, KATE and GEDIT will all work. **For a GNOME desktop, only GEDIT will work.**

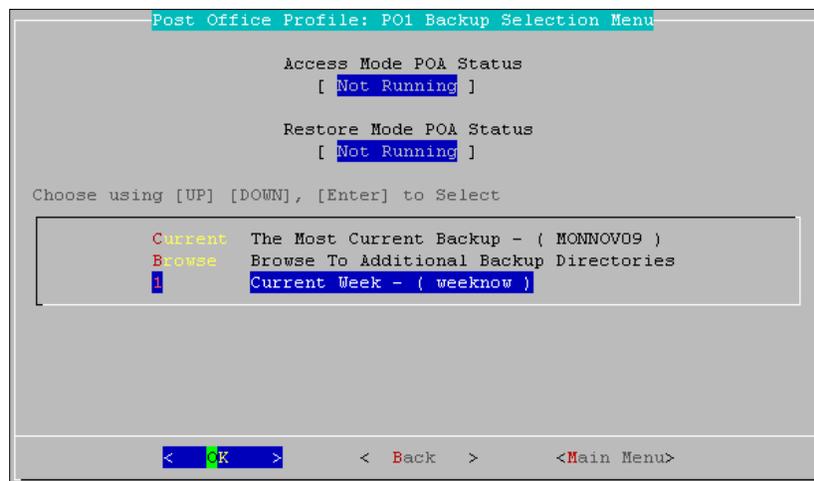
Load

In General, the Disaster POA is only loaded in conjunction with a 'disaster' which inhibits the Disaster Recovery POA from functioning in the mail system. However, every profile's Disaster Recovery Plan should be tested before an actual Disaster occurs. **Be sure to also create a [Disaster Recovery Plan](#) that dictates all actions needed to implement Disaster Recovery for your System.** This plan can be added to the Web Administration for easy access.

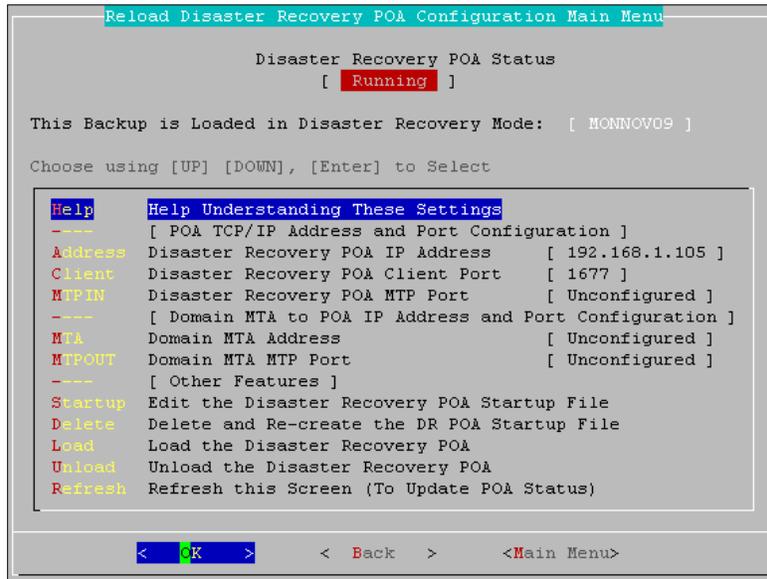
Your Disaster Recovery Plan should contain all the steps, in order, for your system. There may be several steps required for your system to connect the Disaster Recovery POA to the live GroupWise mail system. If setting changes are required to be made in ConsoleOne, those settings and changes should be listed, with the exact variables which are needed to be changed. There is a generic placeholder document which is currently linked in Reload Web Administration. The Placeholder disaster recovery plan contains helpful information in creating your own disaster recovery plan. Create your own and replace the placeholder. See the [Web Administration Preferences](#) section for details.

After you have configured and checked the settings for your Disaster Restore POA, you may continue on to test the Disaster POA for your system.

When you select and confirm to load the Disaster Recovery POA, you are prompted to choose which backup you wish to load the POA against. By default the Disaster Recovery POA will use the latest backup of the Post office unless you specify otherwise. Once you have selected the Backup to use, you may trigger a failover, from the Recovery menu or from the Web Administration.



Once the Disaster Recovery POA has been loaded, the Disaster menu will now display the backup that the Disaster POA is using, along with the option to unload the Disaster POA.



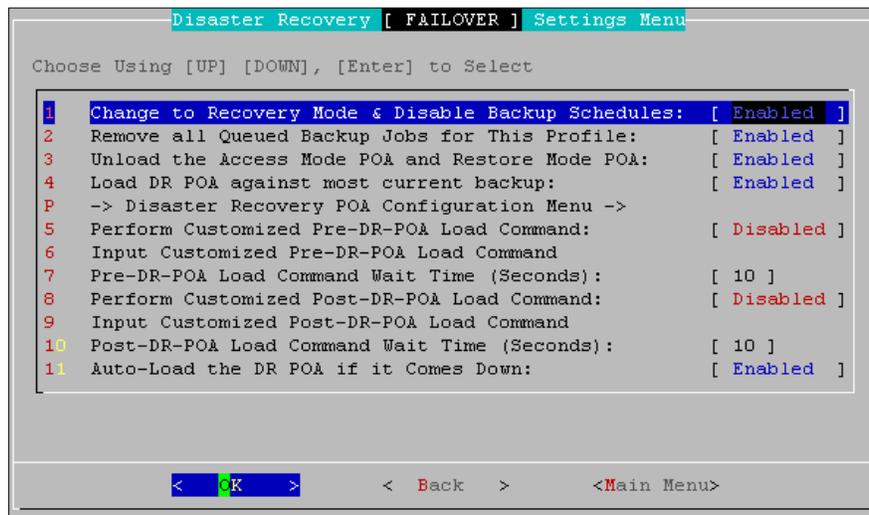
Verify that the Disaster POA is running and can be accessed by your Mail system. Run through your Disaster Recovery Plan and make sure that the system will work as expected.

Configure Disaster Recovery Failover Settings

Instead of modifying the Recovery POA settings, select to configure the Failover settings.



Failover is a process of steps that Reload takes when Disaster Recovery is enabled. These settings can be changed to affect the process that Reload uses for Disaster Recovery.



The steps Reload performs are listed sequentially. Default is shown.

First Reload disables backup schedules for this profile, and switches to recovery mode. Second, Reload removes all queued jobs, and then unloads the Access and Restore POA's, if they are loaded. By Default, Reload then loads the most current backup.

If desired, Reload can run a custom commands before and after loading the Disaster Recovery POA, with appropriate wait times between load and customized command execution. For example, you could call a script that loads a GroupWise Internet Agent or perhaps a script that telnets to a DNS server and switches a DNS record entry.

By Default, the Disaster Recovery POA is set to automatically reload if it goes down for any reason.

Disaster Recovery Migration Settings

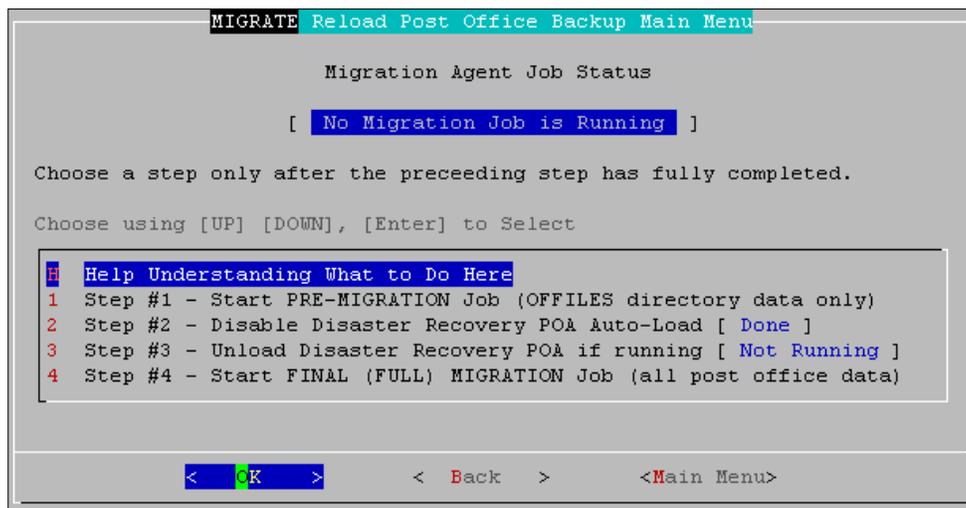
When you failover to a Reload server, the data on the Reload server will be updated with new data that you will want to have back on the Disaster Recovery GroupWise system. So once you have a live production server prepared to function as the live production post office or domain, you will need to get the data migrated from the Reload server, over to the live production server.

The Reload Migration Agent can help you to accomplish this. The Reload Migration Agent copies the live post office or domain that has been running on the Reload server, to the location that you specify.

To configure the actions of the Reload Migration Agent, use the MIGRATE option under Disaster Recovery, and simply follow the wizard for migrating. A post office migration can take a while, particularly for the contents of the OFFFILES directory to replicate over. It is for this reason that the pre-migration job type is in place. When migrating a GroupWise post office from the Reload server to a production server, make sure to run the pre-migration first. When the pre-migration job is running, your Reload server can still be hosting the post office. Then, when the pre-migration is complete, you will want to bring down the Live Mode POA, and run the Final, full-migration job.

To access the migration settings, select, **Profiles**, selected profile, **Disaster Recovery**, and select **Migrate**.

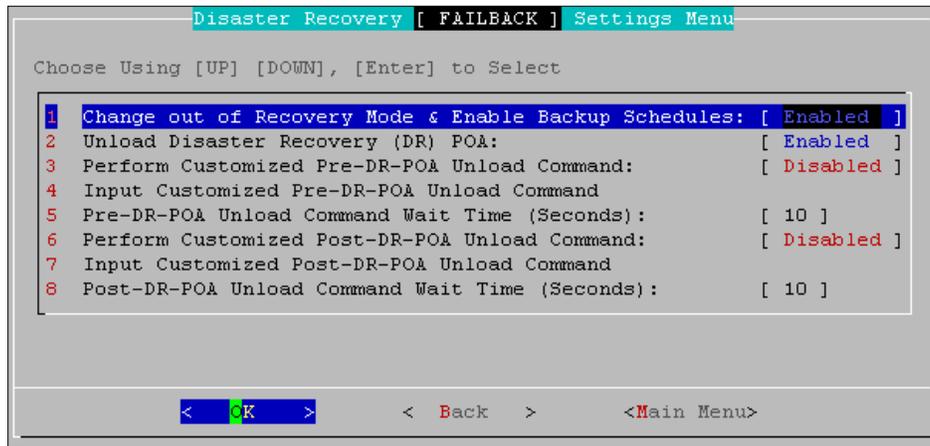
Be sure to select and Read the 'Help' option if you are not sure exactly what the migration process will accomplish.



Migration is a wizard-driven process which performs the steps listed, in the order listed. You may modify the variables in blue. When a migration job is started, either pre-migration or full migration, a wizard is started which asks how to connect to the target server, the target location, and then queues the job to run.

Configure Disaster Recovery Failback Settings

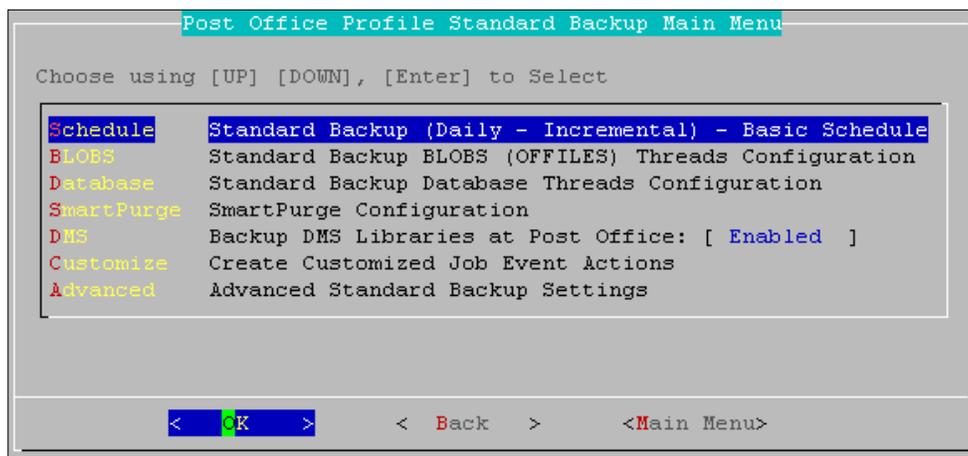
To access the Disaster Recovery Failback settings, from the main menu, select: **Profiles**, **<select profile>**, **Disaster-Recovery**, **Configure**, and **Failback** configuration settings.



Failback is the mode where Reload closes the Disaster Recovery mode and returns the Reload system to normal processing. The default settings for Failback re-enable the backup schedule and unload the Disaster Recovery POA. Customized pre and post Failback commands can be specified and executed with appropriate wait times between command execution and Reload system actions. This can be used, for example, to run scripts which return and modified DNS entries or to automatically restart the GroupWise system or agents.

Standard

Profiles | select desired profile | Standard



The Standard Backup job is the backup job that typically runs daily; it's the equivalent of an Incremental Backup. There are several aspects of a Standard Backup job that you should take into account in your overall design. Let's review them

Schedule

Most customers will want to configure their Standard Backup job to happen sometime once a day, during off-peak hours. The Schedule system within Reload works well with this paradigm. Your organization though, may want to pull multiple Standard Backup jobs throughout the day. Reload works just fine with this scenario; however you will want to use a different scheduling mechanism to accomplish this.

See the [Reload Job Creation utility](#) section to fit the paradigm of multiple daily backups.

BLOBS Threads

Reload can be configured to use up to ten of its own "GRE_BLOBS-Threads". Testing has shown that **using up to ten BLOBS threads can significantly improve performance of Standard Backup jobs**. Most customers will do well to increase their BLOBS Threads to the maximum of 10 threads. In WAN environments, having 10 threads could overwhelm the WAN, link, and actually make the backup times less efficient. You can test the feasibility of increasing the threads, by changing the GRE_BLOBS-Threads value, and then looking at the Event log to see the speed at which a Standard Backup was accomplished based upon changes that you made to the BLOBS threads.

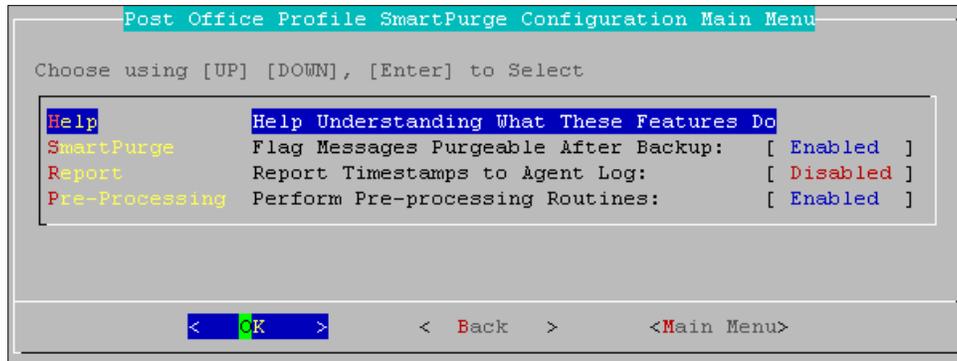
Database Threads

Reload 3 has multiple threading capability to improve backup speeds. Novell's development team has worked closely with GWAVA to create threading in DBCOPY also. The DBCOPY threading will only be available with the GroupWise 7.0.2 and later. Reload can be configured to use two of its own "GRE_DBS-Threads" however, testing has shown that doing so actually decreases performance in most customers' cases because the network card is overwhelmed. This feature is ahead of it's time for most environments. Most customers will do well to keep the GRE_DBS-Threads at the factory defaults of five threads.

Starting with the GroupWise 7.0.1 DBCOPY software, DBCOPY can listen on a TCP/IP port. The fact that DBCOPY listens on a TCP/IP port allows Reload to bring down an instance of DBCOPY more gracefully than it could otherwise. Having the DBCOPY listen on a TCP/IP port also allows GWAVA Technical Support some additional troubleshooting information in case there ever is a need to troubleshoot DBCOPY.

SmartPurge Configuration

By default a Reload profile is configured to "**Flag Messages Purgable after Backup**", as shown below. The setting is located at **Profiles | <select desired profile> | Standard | SmartPurge**. This means that after a post office is backed up with Reload, that Reload puts a timestamp on each user's database. The GroupWise SmartPurge feature built into the GroupWise client and POA ensures that messages that were received before the timestamp created by Reload, can be purged. However messages received after the timestamp, cannot be purged until Reload backs up the post office again.



In order for Smart Purge to actually work, you must **ensure that the SmartPurge feature is enabled through ConsoleOne**. The Reload server can be configured to allow for time zone differences between the Reload server and the server that houses the GroupWise post office. If for example, the Reload server was in Houston Texas, and the live post office was in Florida, the Reload backup profile can be configured to allow for the time difference, but still have the backup time stamp in Florida be correct according to local time.

Reload uniquely puts the SmartPurge feature of GroupWise to use in another way. After Reload has backed up a post office to the Reload profile's backup location, it flags all of the user's databases on the Reload server, to indicate that nothing has been backed up. What this does is ensures that **items cannot be purged from backup GroupWise message store on the Reload server**. Items can be deleted, from the Reload message store, but the items cannot actually be purged from the trash.

In scenarios in which one Reload server is backing up a "Remote Reload Profile" on another Reload server, the **Flag Messages Purgeable after Backup should be disabled**. The reason for this is that **you do not want messages on a Reload server to be purgeable**; you only want them to be purgeable on the server where the live GroupWise post office is.

In all possible cases, **Pre-Processing** should be enabled to perform database connectivity routines. See 'Help' for detailed information.

DMS - Backing up Document Management Libraries

Reload will backup Document Management libraries on the post office, as long as they do not use a remote "Document Storage Area". In order for this feature to work, the GroupWise 7.0.1 or later DBCOPY code must be installed. This setting is found under **Profiles | select desired profile | Standard**.

Customize

The customize feature allows for a custom action that the Reload server will perform in the event of the following three states of a Job.

- Job Start
- Job Error
- Job End

You could for example, have a script process send an e-mail if a Standard Backup job errors. Reload ships with a script called "mailer.sh". Because this is a script, and can be modified, the script is not a supported component of Reload. However you could consider using this script to generate an e-mail. The script is located in the directory:

```
/opt/beginfinite/reload/setup
```

If you were to reference the mailer script in as the Customized Job Error Command, the syntax you would use would most likely be:

```
/opt/beginfinite/reload/setup/mailer.sh -c /opt/beginfinite/reload/setup/mailer.conf
```

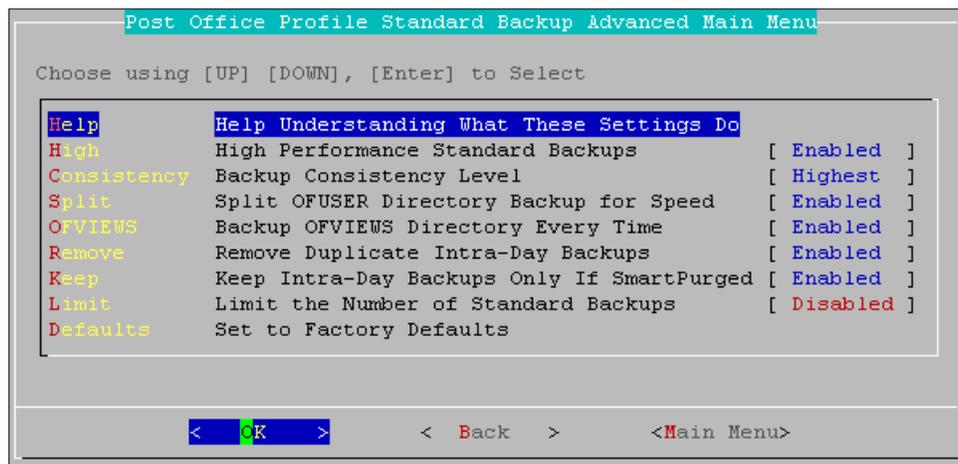
To learn more about the mailer script, run it once, to see the syntax and usage for this script. To run the script, do the following. In a terminal session, go to the directory where the script is located, and run it.

Example:

```
cd /opt/beginfinite/reload/setup
./mailer.sh
```

Advanced

The advanced menu has settings that may prove useful to specific situations, but should be mainly left as default.



Help

Provides a description on all the features listed below.

High-Performance Standard Backups

When the Reload Backup Agent performs a Standard Backup on a GroupWise post office, it allocates GRE-DBS threads, and GRE-BLOBS threads as explained earlier. For maximum backup speed, the GRE-DBS and GRE-BLOBS threads can run simultaneously. The High-Performance Standard Backups setting enables this functionality, and is enabled by default. Customers in a very low-bandwidth backup environment may consider disabling High-Performance Standard Backups.

Consistency

Having the consistency level turned to the highest is the default, because Reload then guarantees that no mail message in the Reload backup will be missing any portions, for instance, attachments. This makes backups take about 10% longer but is the best practice for good backups.

Split

When enabled, Reload separates the backup of the OFUSER/INDEX directories into two different backup actions. This allows Reload to initiate backup of the OFFILES directory contents sooner, providing for a faster backup of medium and small post offices. If a post office contains thousands of users, enabling this option may slow down the backup. If a Post Office has more than 3000 users, this feature should be disabled.

OFVIEWS

This option forces Reload to backup the OFVIEWS directory every time, ensuring the latest *.view files and full client compatibility.

Remove

This setting causes Reload to remove multiple redundant backups that have been processed throughout the day, only keeping the final backup. This setting is **ONLY** to be used in conjunction with the **“Keep Intra-Day Backups Only If SmartPurge Ran”** setting. Read the Remove section under ‘help’ for more details.

Keep

The ‘Keep’ setting is to be used in conjunction with the ‘Remove’ setting, to prohibit the Reload system from removing the backups that were created by a job which also performed a Smart Purge. This keeps the backups complete while still eliminating redundant backup data.

Limit

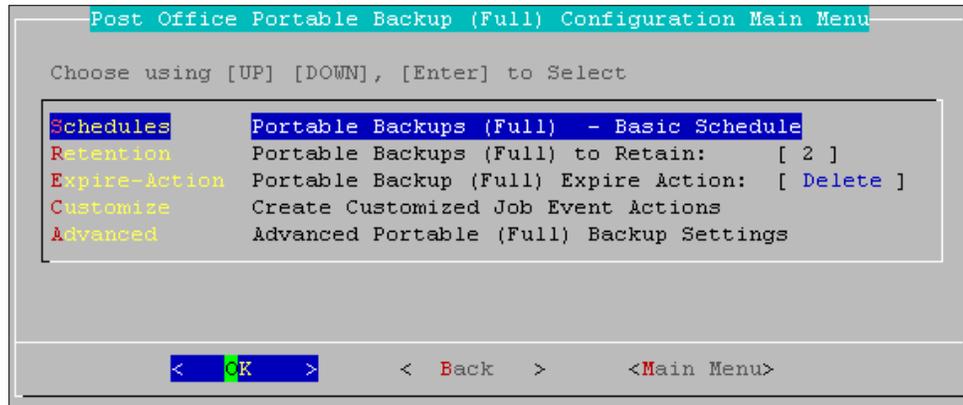
This setting limits the amount of standard backups kept for this Profile. If this setting is enabled, your system will trim the amount of standard backups to the limit defined. This setting saves disk space while enabling backups to continue. Read the ‘Help’ entry for more information.

Defaults

This option returns the advanced settings back to their original variables.

Configuring Portable Backups

Profiles | select desired profile | Portable



Schedule

Most customers will want to configure their Portable Backup Job (Full Backup) to happen sometime once a week. Portable Backup Jobs are unique in that they require very little network bandwidth, and as such can be scheduled to happen even during peak hours.

Retention

Each Portable Backup disk space cost is approximately 250% of the size of the GroupWise post office that the Reload profile is backing up. Most Reload customers have found that retaining 2 to 3 Portable Backups (generally 2 - 3 weeks worth of backups), fulfills 98% of their needs when needing immediate access to backed up data. When Reload runs the Expire process, it will expire all Portable Backups beyond the Portable Backups beyond the retention amount that you have specified. Generally, this means that each week, the oldest Portable Backup is deleted.

Expire Action - Delete or Archive

Reload can be configured to either delete or archive data that has expired. The Archive feature requires that you specify a location for the Reload Agent to move the data to after it has expired. The idea being, that perhaps a NAS device or some other mass storage solution is in-place where the backed up GroupWise data can be moved to. Once Reload has "Archived" a Portable Backup, the Reload server no longer manages the data. Most customers will not choose to use the "Archive" feature. Some may find it useful, if they have mass storage solutions in place and a need for backed up GroupWise data to be easily available.

Configuring Archive Settings

The Archive Settings menu is only accessible, if the **Expire-Action** is set to "**Archive**". Here's the concept behind the "Archive" ability within Reload. In the US, in the State of Florida, there are Sunshine Laws governing email archiving, retention, and archived access. A customer in Florida loves Reload's capabilities to back up email data and for it to be hot and live on their NAS device for a few years. So they configured the Reload server, to keep 2 weeks worth of Portable Backups available on the Reload server. Then, they configured the Reload server to perform the Expire-Action of **Archive**. If you would

like the Archive to be immediately useable by Reload make sure that the location where you put the Archived data fulfills the following requirements:

- The Archive location should support a Linux/Unix system file system that supports **Symbolic Links**
- The Archive location should be available as a Read/Write mountable location to the Reload server once an Archive is created, one way that you might access an Archive location from the Reload server would be to do the following:
 - On the Reload server, establish a mount point to the Archive location
 - In the Reload Administration menu, select **Access**
 - Choose the appropriate profile
 - Select **Browse**
 - Manually select all the way to the appropriate day directory that represents a GroupWise post office backup set. The directory you select should have a **wphost.db** file within it.

Specify Archive Path

This is the location that the Reload server should put the archived Reload Portable Backups. The Archive Path should be a path that is available to the Reload server. If you combine the "Pre-ARCHIVE" and "Post-ARCHIVE" commands (explained a little later) to create a mount to a different server, then Reload can "push" the Reload Portable Backups to the new server location. The Portable Backup Archive directory that gets created by Reload follows this naming convention:

<profile name>-<Portable Backup Directory Name>-archive

Example:

po1-1-week-05-2006-archive

Customize

The customize feature allows for a custom action that the Reload server will perform in the event of the following three states of a Job.

- Job Start
- Job Error
- Job End

You could for example, have a script process send an e-mail if a Portable Backup job errors. Reload ships with a script called "mailer.sh". Because this is a script, and can be modified, the script is not a supported component of Reload. However you could consider using this script to generate an e-mail.

The script is located in the directory: /opt/beginfinite/reload/setup

If you were to reference the mailer script in as the Customized Job Error Command, the syntax you would use would most likely be:

```
/opt/beginfinite/reload/setup/mailer.sh -c /opt/beginfinite/reload/setup/mailer.conf
```

To learn more about the mailer script, run it once, to see the syntax and usage for this script. To run the script, do the following. In a terminal session, go to the directory where the script is located, and run it.

Example:

```
cd /opt/beginfinite/reload/setup
./mailer.sh
```

Configuring Advanced Archive Settings

The Reload Agent can execute the commands called the “Pre-ARCHIVE” Command before it puts the Portable Backup to be archived at the Archive Path. The Reload Agent can also perform a “Post-ARCHIVE” command. When the Reload Agent executes the Pre-ARCHIVE command that you specify, the following happens:

- The Reload Agent sends the Pre-ARCHIVE command to the background to be executed by the Linux operating system.
- The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by the **Customized Pre-ARCHIVE Command Wait Time**.
- The Reload Agent moves the Portable Backup to be archived to the Archive Path.
- If a Post-ARCHIVE Command is specified then the Reload Agent does the following:
 - The Reload Agent sends the Post-ARCHIVE command to the background to be executed by the Linux operating system.
 - The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by **Customized Post-ARCHIVE Command Wait Time**.

Advanced

Help

Detailed information for all advanced settings are explained here.

Expire First

This allows the Reload system to delete expired Portable backups before creating a new portable backup. Reload must delete the oldest portable backup to comply with the portable backup limit.

High

Enabling ‘high performance backups’ allows two Reload agent processes to simultaneously clean up files which reside on the Reload backup which are no longer in use on the live server. This may improve performance for portable backup jobs, for systems that have enough resources.

Copy, Sync, DBCOPY

These thread options allow you to specify how many simultaneous threads can be run for each of these operations. Increasing threads for all these options above the recommended may cause a hard disk I/O bottleneck that adversely affects performance. Copy and Sync usually should have no more than 5 threads each and only 2 threads for DBCOPY, except in certain circumstances. For specific information on each process, read the ‘Help’ section.

Port-Allowed

Reload does not require DBCOPY to listen on a particular port, though it can be helpful in troubleshooting.

Port-Range

If a specific Port-Allowed is specified, this setting allows Reload to detect whether that port is in use and switch to a different port that is not in use. This port is the start port for the range.

Pre-Processing

Portable backups can take large amounts of time to complete on large systems, and pre-processing allows Reload to start a low-priority process to begin mirroring the 'master' OFFILES during standard backup jobs. This increased the standard backup time by 10%, but can greatly reduce the portable backup time for systems with enough resources.

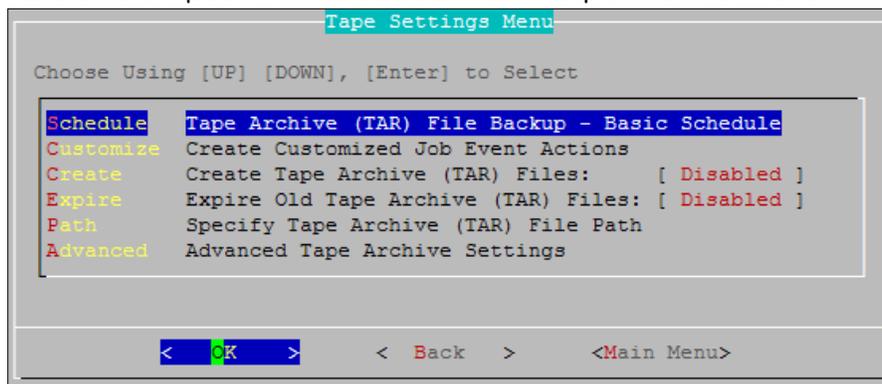
Defaults

Returns all advanced settings for this profile back to default.

Tape Backups

Reload does not eliminate the need for offline (cold) backup solutions, such as tape backup solutions. Most organizations will still need to retain a tape backup system. However, Reload can prolong the life and enhance tape backup solutions in the following manner:

- Eliminates wear and tear on your tape backup systems, because most backed up data will be retrieved from the Reload server, and not tapes
- Reload can create a Tape Archive (*.tar) file which contains the entire contents of a Portable Backup set within it. The Portable Backup will generally contain 7 days worth of backups. Writing to tape is significantly faster with backups created by Reload, because the Reload backup Agent does all the work of bundling the entire GroupWise message store into a single file. Writing a single file (yes it is a big file of course), to tape can be significantly faster than writing thousands of files to tape.
- Reload can be configured to run a "Pre-TAR" command and a "Post-TAR" command. With this architecture in place, some customers have designed Reload to "push" the *.tar file that Reload creates to their backup server. In this section we will explain how to do this.



Schedule

Most customers will want to configure their Tape Backup Job to happen sometime once a week, after the Portable Backup has been created, and then most likely after the Expire Portable Backup action has

also taken place. Tape Backup Jobs require no network bandwidth, and as such can be scheduled to happen even during peak hours.

Generally this is how Backup Jobs should be configured, for the best use of disk space on the Reload server:

1. Run the Portable Backup job
2. Run an Expire Portable Backup Job
3. Run the Tape Backup Job

Customize

The customize feature allows for a custom action that the Reload server will perform in the event of the following three states of a Tape Backup Job.

- Job Start
- Job Error
- Job End

You could for example, have a script process send an e-mail if a Tape Backup Job errors. Reload ships with a script called "mailer.sh". Because this is a script, and can be modified, the script is not a supported component of Reload. However you could consider using this script to generate an e-mail.

The script is located in the directory:

```
/opt/beginfinite/reload/setup
```

If you were to reference the mailer script in as the Customized Job Error Command, the syntax you would use would most likely be:

```
/opt/beginfinite/reload/setup/mailer.sh -c /opt/beginfinite/reload/setup/mailer.conf
```

To learn more about the mailer script, run it once, to see the syntax and usage for this script. To run the script, do the following. In a terminal session, go to the directory where the script is located, and run it.

Example:

```
cd /opt/beginfinite/reload/setup
```

```
./mailer.sh
```

Create Tape Archive (TAR) Files

By configuring Reload to create *.tar files, the Reload Agent creates a *.tar file out of the Portable Backups available for a particular Reload Profile. Creating the *.tar file does not eliminate the Portable Backup, the *.tar file is created in addition to the Portable Backup. **Because the .tar file is additional to the portable backup, the disk space required is an addition to the original needs.** After a Portable Backup has been backed up the name of the Portable Backup directory will be appended with a "-T". For example, a Portable Backup directory that has not had a *.tar file created for it might be called:

1-week-05-2006

After the Reload server has created a *.tar file from the Portable Backup the name of the directory would change to:

1-week-05-2006-T

NOTE: It's important to understand the **1-week-05-2006-T** is a directory and is not a *.tar file.

The *.tar file that gets created by the Reload Agent follows this naming convention:

<profile name>-<Portable Backup Directory Name>.tar

Example:

po1-1-week-05-2006.tar

Expire Old Tape Archive (TAR) Files

When Reload creates *.tar files at the path that you specify, you can have Reload delete the *.tar files that were created for the Reload profile previously. Here's what this does.

- Reload creates *.tar file when the Reload Agent runs the *.tar routine
- The tape backup solution can be pointed at the location where Reload creates the *.tar file so that it can be backed up
- The next time the Reload Agent creates a *.tar file (generally this will be a week later), the Reload Agent will delete any files that follow the naming convention of:

<profile name>-<Portable Backup Directory Name>.tar

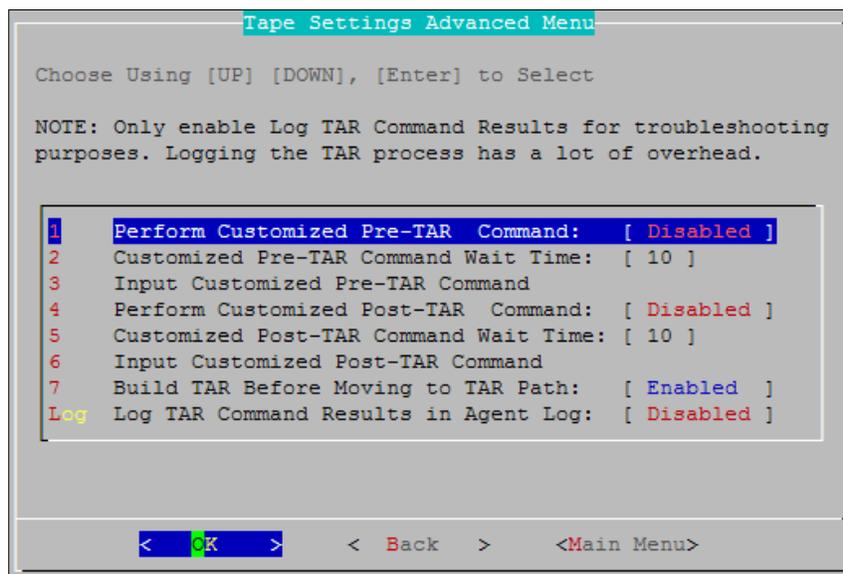
The Reload Agent deletes *.tar files prior to running the Pre-TAR command. So if the Pre-TAR command is used to mount an external server for example, the Reload Agent will not attempt to delete old *.tar files from the remote server. This was done by design, because there is no guarantee that once a *.tar file is created on a remote server, that the Reload server will have rights to delete the *.tar file from the remote server.

Specify Tape Archive (TAR) File Path

This is the location that the Reload server should put the *.tar file. The TAR File Path should be a path that is always available to the Reload server. However, if you combine the "Pre-TAR" and "Post-TAR" commands (explained a little later) to create a mount on the Reload Linux server to a different server, then Reload will effectively "push" the *.tar file to another server.

Configuring Advanced Tape Settings

The Reload Agent can execute the command called the "Pre-TAR" Command before it puts the *.tar file at the Tape Archive (TAR) File Path. The Reload Agent can also perform a "Post-TAR" command.



When the Reload Agent executes the Pre-TAR command that you specify, the following happens:

- The Reload Agent creates the *.tar file from the Portable Backup that is being copied into the *.tar file.
- The Reload Agent sends the Pre-TAR command to the background to be executed by the Linux operating system.
- The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by the **Customized Pre-TAR Command Wait Time**.
- The Reload Agent copies the *.tar file that it created previously, to the TAR File Path.
- If a Post-TAR Command is specified then the Reload Agent does the following:
 - The Reload Agent sends the Post-TAR the command to the background to be executed by the Linux operating system.
 - The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by **Customized Post-TAR Command Wait Time**.

Configuring the Reload Agent to “push” a *.tar file to another server

Because of the ability to specify a Pre-TAR and a Post-TAR command, you can effectively get the Reload Agent to “push” the *.tar file that it creates to a different server.

Configure Reload to push the *.tar file to a Windows server that is running Veritas.

1. Create a directory that will be mounted to the Windows server with a CIFS mount. For example: **/data/tape**
2. Create a BASH shell script to mount the /data/tape directory to a Windows share created on the Windows server running Veritas. For more guidance on making a Windows share, you can read the [windows share creation section](#).

Reload ships with a good, but un-supported, CIFS mount BASH shell script. You may consider using this script. The name of the file is cifsmnt.sh and it is located in the directory, /opt/beginfinte/reload/setup

3. Run the **cifsmnt.sh** script from within a terminal session, and read the instructions of this utility for more guidance on using this script.
4. In the Pre-TAR Command, specify the command that performs the CIFS mount.
5. Specify a time that the Reload Agent should pause to allow the Pre-TAR command to complete. Generally the default of 10 seconds is sufficient.
6. In the Post-TAR Command, specify the command that performs the unmount of the CIFS mount created with the Pre-TAR command.
7. Specify a time that the Reload Agent should pause to allow the Post-TAR command to complete. Generally the default of 10 seconds is sufficient.

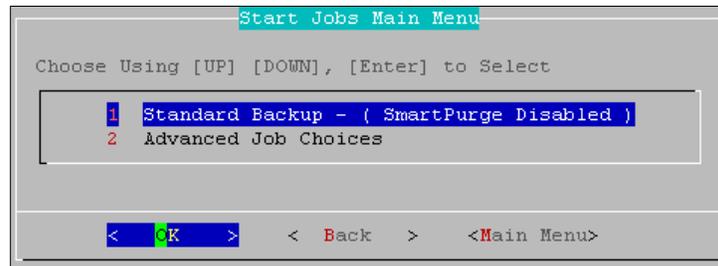
Build TAR Before Moving to TAR Path

By default when Reload creates a *.tar file, it first creates the *.tar file in a temporary location off of the profile directory for which the *.tar file is being created. In a case in which the *.tar file is being configured to go to a different physical disk drive than where the Reload profile is located, you could

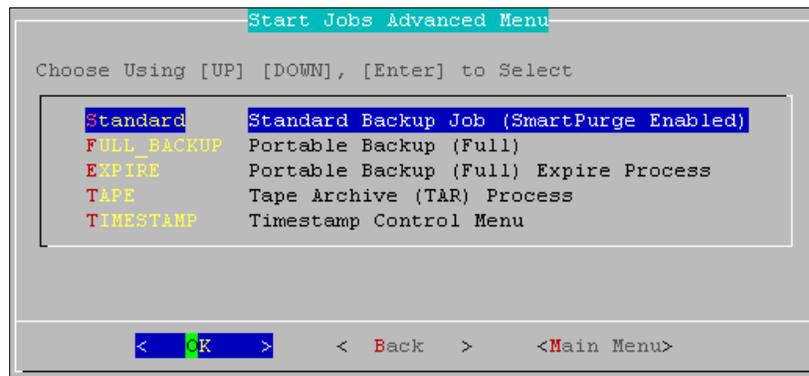
consider disabling the **“Build TAR Before Moving to TAR Path” feature**. This could allow the *.tar file creation to go quicker, since the disk where the Reload profile is located is only being read from, and not written to, simultaneously.

Job

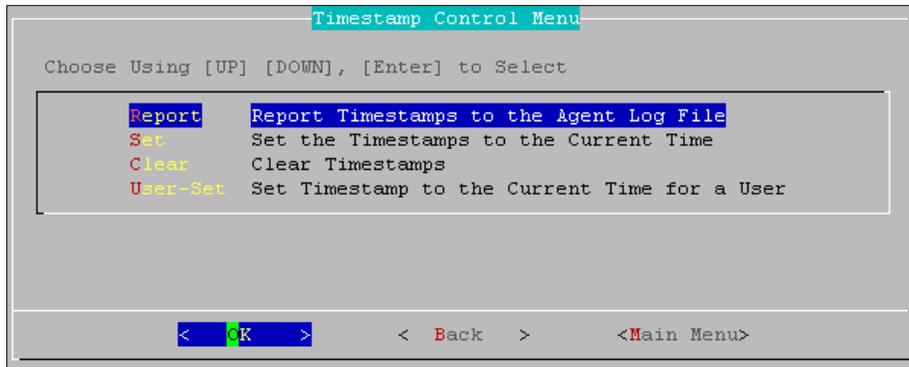
This menu provides the option to start, stop, or check the status of jobs on the active profile. The usual job to manually start is a Standard Backup Job. To run a different job or alter job settings, select Advanced Job Choices.



Advanced Job Choices allows different job types to be run, according to the settings in the system for each. The Job options located here only allow for creating a new job for the selected job type.

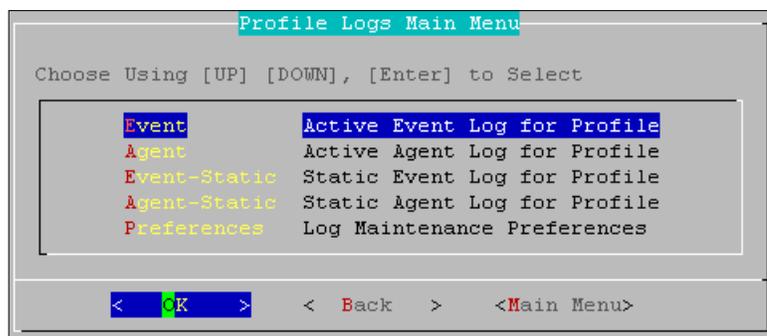


The Timestamp option allows a job to be set for the timestamp only in the system. This timestamp is the SmartPurge time stamp, and can be set, cleared, reported, or modified for a specific user. This affects both the SmartPurge options and the data that Reload will add to the Reload Backups.

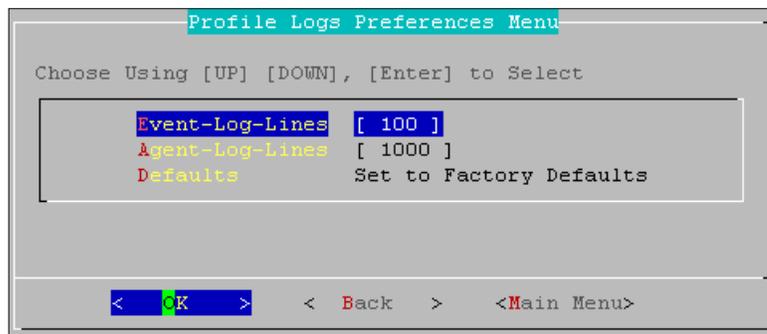


Logs

The Logs menu allows you to view either the rolling tail of this profile's agent or event logs, or the full logs, (static). This menu also allows you to set the log preferences for this profile.

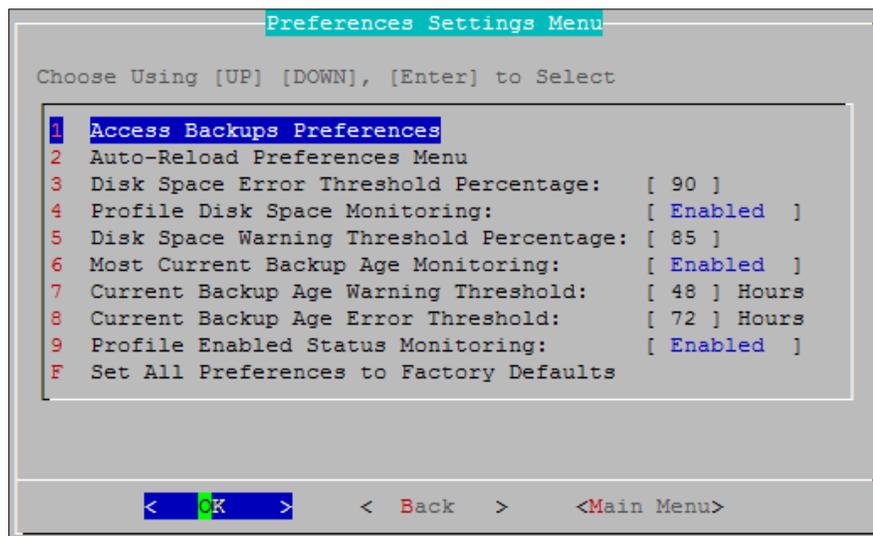


The log preferences set the configuration for how many lines will be stored in each log file, and whether to revert to defaults.



Profile Preferences

The Preference Settings Menu allows you to configure how backups are accessed, which thresholds are active for warning and error, and what they are set to.



Error and Warning thresholds

Setting the error and warning thresholds will allow Reload to alert you via email, before a problem blocks Reload's normal system functions can develop. This setting allows Reload to monitor the disk space and backup age for your system in order to warn you if they exceed your specified amount. The monitoring for each warning and error threshold must be enabled for the threshold to take effect. **The warning and error thresholds allow Reload to be a 'set and forget' system which will contact you if there is a problem.** Status reports, warning, and error threshold messages all use Postfix to send email messages. **Postfix must be running and configured for you to receive warning messages from the Reload system.** Postfix is included in the standard Linux platform by default, and as such is not supported by GWAVA support.

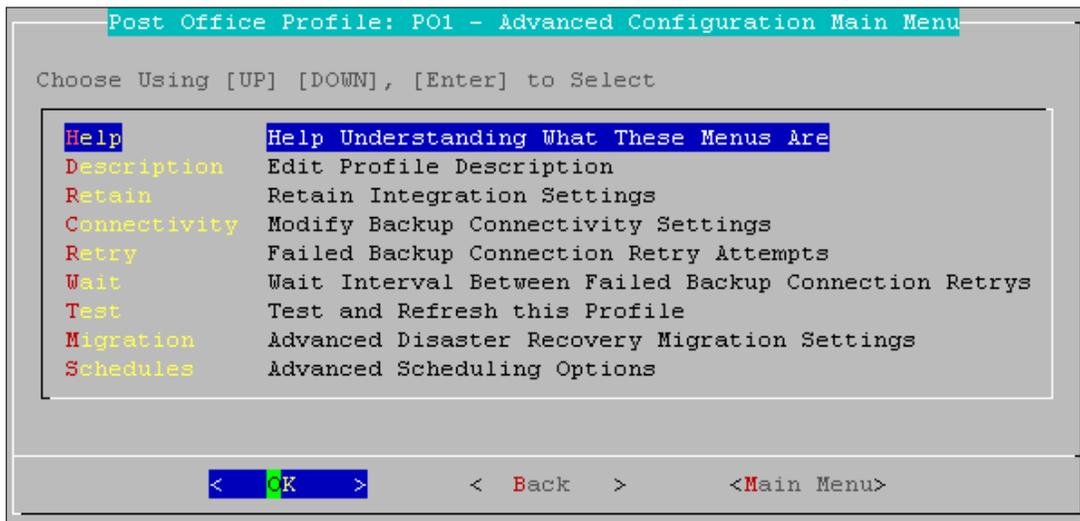
The Disk Space Warning and Error thresholds are a percentage, and are tied to the amount of space left on your hard disk. They will warn you when your system starts running out of disk space.

The Current Backup Age Warning and Error thresholds will warn you when the latest backup in your system exceeds the listed age for each threshold. The variable is in hours. This may indicate a failure for a Profile's backup schedule, and the status should be checked. A disk space error will lead to a backup age error. When there is no longer enough space to complete a full backup, Reload will stop creating backups until space becomes available.

Advanced Reload Post Office Profile Configuration

The Profile Advanced Configuration menu shown in Figure 7.1 is available by selecting the following from the Main Menu:

1. Profiles (Modify Profiles)
2. Choose the Reload Profile
3. Choose Advanced (Advanced Profile Configuration Menu)



Help

This contains specific information on all the settings in this menu.

Description

This section allows you to modify your 60 character description of the profile set during profile creation.

Retain Integration

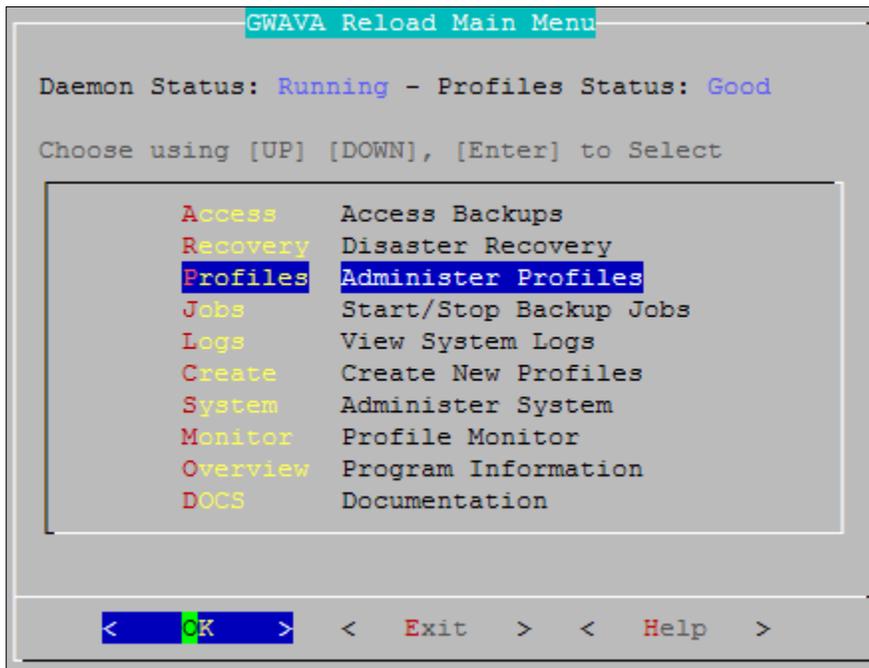
First, Reload must be set up so that the backups are available. There is a special feature in Reload for this. It calls up a post office agent that stays up all the time and it only goes down long enough to change to the most recent backup. So it will always be there with very small interruptions as 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.

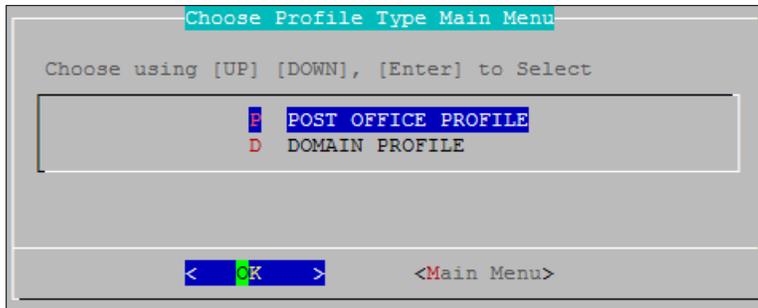
- 1) Start up Reload's Administration menu.



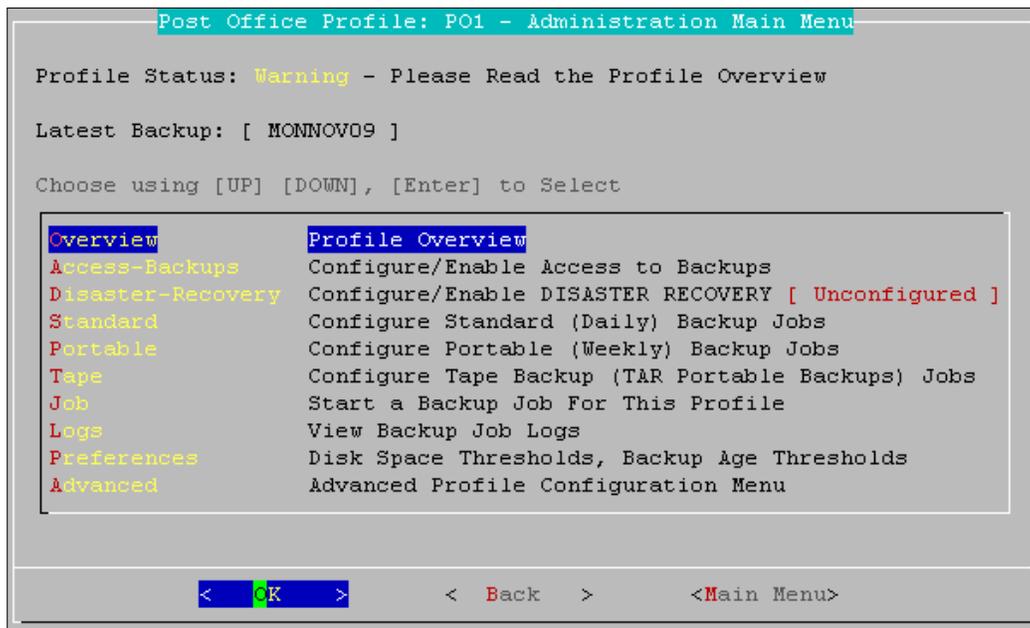
- 2) From the main menu, choose Profiles – Administer Profiles.



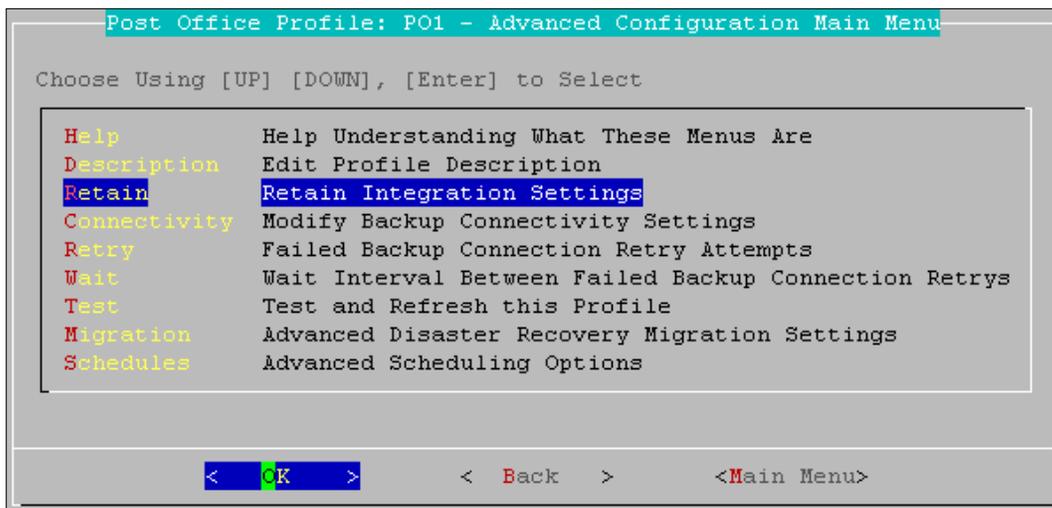
- 3) Select the Desired Profile. (The Retain POA must be setup for each profile).



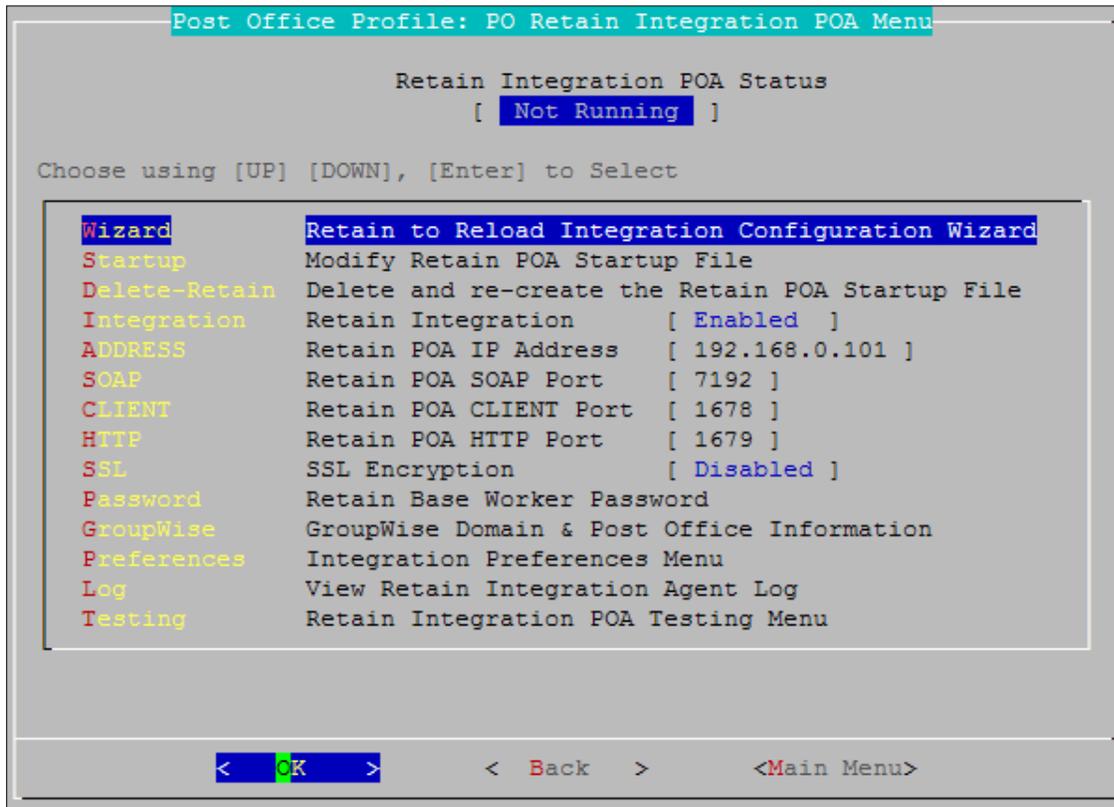
4) Choose Advances Profile Configuration Menu



5) 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 is a separate POA and the settings NEED to be different from the Disaster, Recovery, or Access POA. The easiest way to start is to run the wizard.



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 for GroupWise will use to access this POA.
- GroupWise: Specify the domain name and post office name for this POA.
- Log: View the Integration Agent Log.
- Testing: Offers support options to test load the Retain POA

- 1) Run the Wizard

GroupWise Post Office Name

In the field below indicate the name of the GroupWise Post Office that this Reload Profile represents.

po

< Save >

- 2) Enter the name of the post office and domain.

GroupWise Domain Name

In the field below indicate the name of the GroupWise Domain that owns the GroupWise Post Office:

po

dom

< Save >

- 3) Choose an authentication key that Retain will use to access this POA. **This password must also be set in the Retain Server for the Worker password. If the passwords do not match, Retain will be denied access to the Reload backups.**

Retain Base Worker Password

In the field below indicate the password (string of characters) that the Retain Worker can use to get access to the Retain to Reload integration for this profile.

NOTE: Use only letters and numbers for the password. The case of the letters does matter.

NOTE: Do not exceed 40 characters.

123

< OK > <Cancel>

- 4) Set the IP address and ports which the Retain POA will bind to. If this POA will be sharing the IP address with any other Reload POA, the Client, SOAP, and HTTP connection ports must be unique to avoid port conflicts.

Retain POA IP Address

In the field below indicate the IP Address on this Reload server that the Retain Integration POA should bind to.

NOTE: Use digits, not letters

192.168.0.101

< OK > <Cancel>

Retain POA CLIENT Port

In the field below indicate the CLIENT port on this Reload server that the Retain Integration POA should use.

NOTE: Use digits, not letters

1678

< OK > <Cancel>

Retain POA SOAP Port

In the field below indicate the SOAP port on this Reload server that the Retain Integration POA should use.

NOTE: Use digits, not letters

< OK > <Cancel>

Retain HTTP Port

In the field below indicate the HTTP port on this Reload server that the Retain Integration POA should use.

NOTE: Use digits, not letters

< OK > <Cancel>

Reload should be installed on a machine other than the live POA server, but the standard ports are usually best used for one of the other Reload POAs, (Disaster, Restore, and Access). Pick a port for each connection which you know is open.

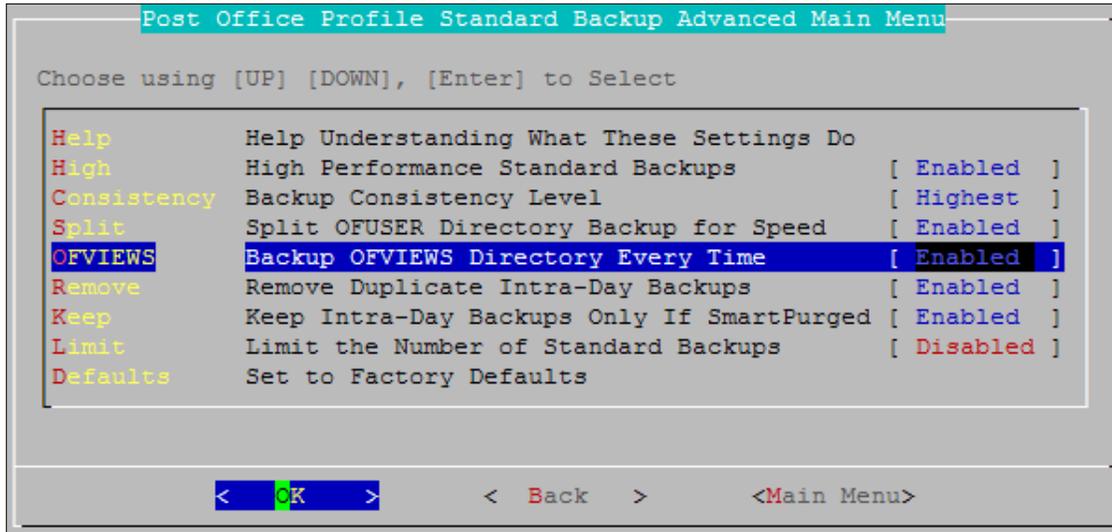
Retain will pull all necessary connection information from the Reload server. There is no need to enter these settings into the Retain Server.

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.

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 | (Select Profile) | Standard | Advanced | Consistency: Set to highest.



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.

Retain Settings for Reload Integration

A quick list of tasks for Retain settings:

- Configure the Retain job to use the Reload backups
- Set and use the Date Range. This automatically selects the latest Reload backup.
- Use the Item Store Flag
- Set the Retain Worker password to the Retain integration password you set in Reload
- Recopy the bootstrap file to the worker

Configure to use Reload

Retain has been designed to work with Reload, and all that is involved is to assign the running jobs to use the Reload integration. This setting is found in the Jobs configuration page in the Retain management console, (you must be logged-in as the administrator or posses administrator rights).

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.)

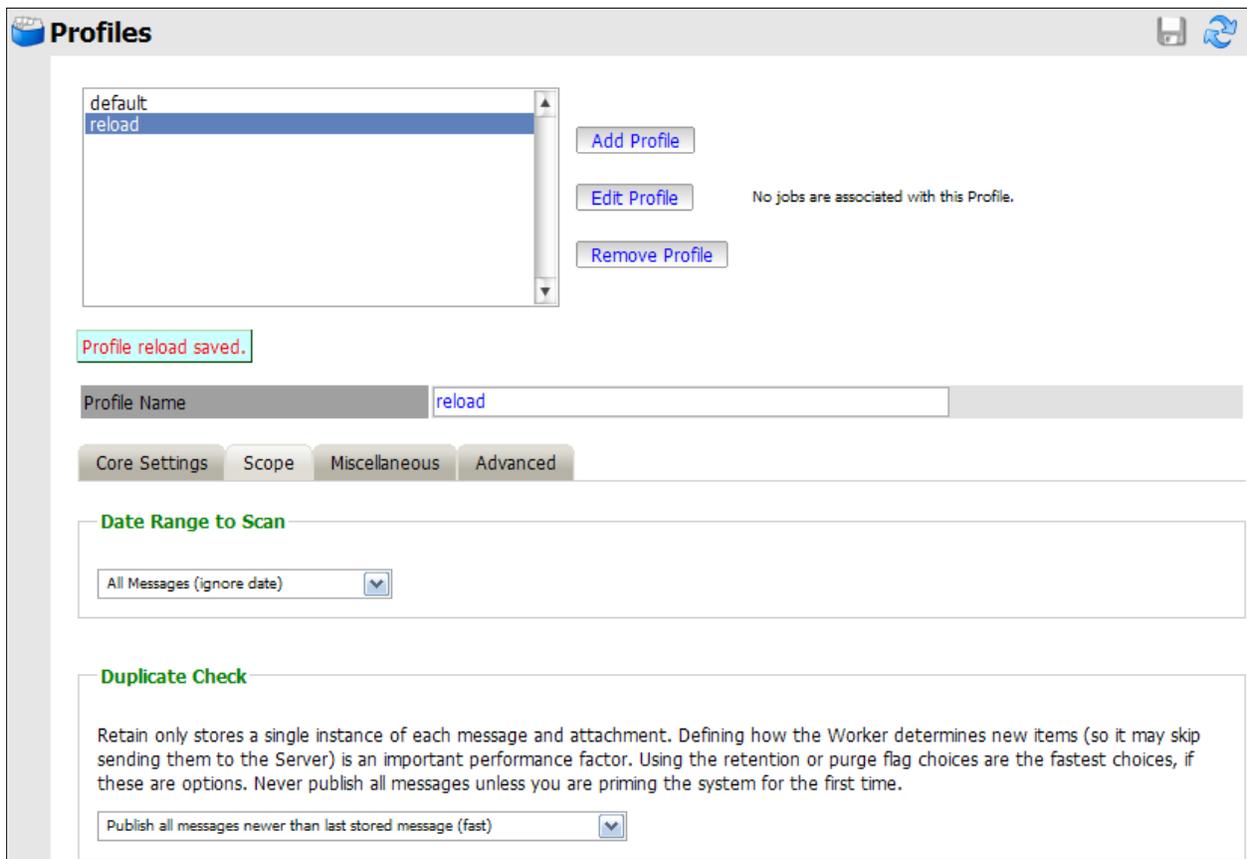
Set the rest of the Core Settings, Notification, and Status as you would normally for your Retain system, but note that in the Mailboxes section you MUST assign the mailbox that Reload is backing-up. Save the changes.

Schedule

It's important to schedule 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.

Profile Scope

To ensure that the latest Reload snapshot is used with Retain backups, the Retain profile should be set to use the 'Date Range to Scan' setting. Set this to scan for mail at the desired amount of days after job start.



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.

Set Storage Flags

If you are using either the Purge or Retention features in GroupWise, you probably want these to be advanced automatically as items are stored, so users may delete messages in their mailbox that have been stored by Retain. The Item Store flag is of similar function, stored in Retain itself, but cannot prevent users from deleting it. It is most useful in conjunction with GWAVA Reload or in use with multiple overlapping jobs.

Retention Flag Purge Flag Item Store Flag

Set Worker Password

The Retain Worker assigned to the job configured to connect to the Reload system **MUST** have the worker password changed to match the password specified in the Reload system. **The password supplied to the Reload system for Retain MUST match the Retain Worker password or the connection will be refused.**

Under the worker menu | Connection tab, reset the Worker password to match the password set in Reload.

Worker

Poling | Logging | Connection | Status | Bootstrap

Server Connection

The worker will need to know how to connect to the Server. It is highly recommended that you use a DNS host name for the Host Name. It's important to note that you are specifying the URL from the point of view of the **Worker contacting the Server**, which may or may not match the URL you'd use from your browser to reach the Worker or Server.

For administrators using the Reload interface, note the worker password assigned must be the same for each worker that contacts the Reload Server. As part of setting of the Reload Server, you must know this password.

Server Protocol	http
Server Host Name	192.168.0.101
Server Port	80
Server Path	/RetainServer
Worker Password

Note: Changing any of these parameters will require recopying the worker bootstrap file!

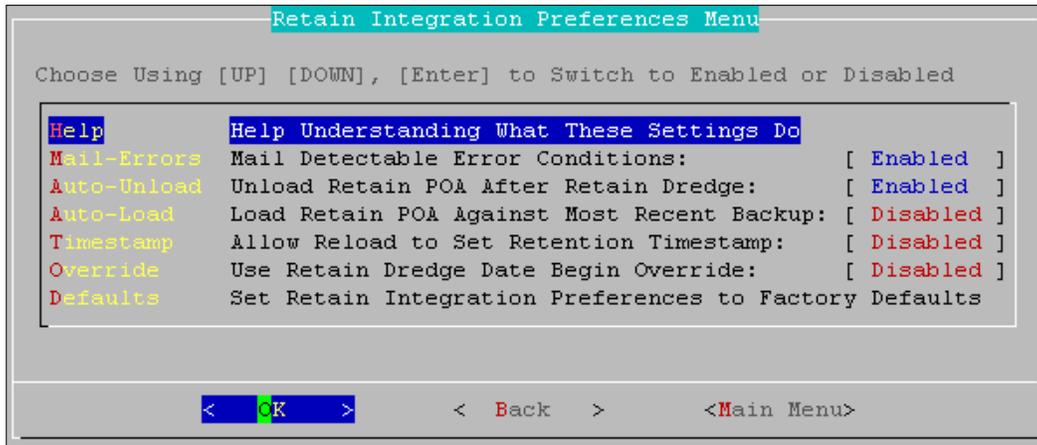
Recopy the Bootstrap File

Once the worker password has been changed, the bootstrap file (worker.cfg) must be recopied over to the worker. If this is a new worker which does not have a bootstrap file, you can upload the new bootstrap file through the web interface at http://<server_address>:48080/RetainWorker To recopy the bootstrap file to an existing worker you must replace the existing bootstrap file.

- Shutdown tomcat
- Copy the new bootstrap file over the existing file in /opt/beginfinite/retain/RetainWorker/WEB-INF/cfg/ or <your retain install directory>/RetainWorker/WEB-INF/cfg
- Restart tomcat

The following menu and features are maintained for support purposes only. These options are antiquated and should not be used against Retain Version 1.5 except at the request of GWAVA Support.

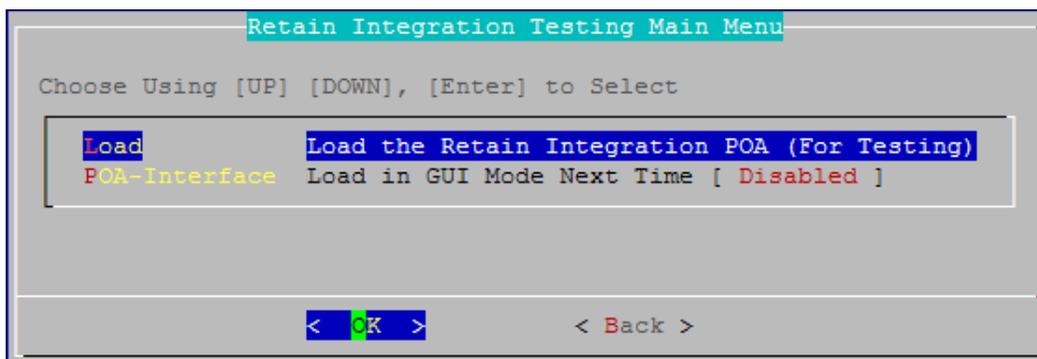
Retain Integration Preferences Menu



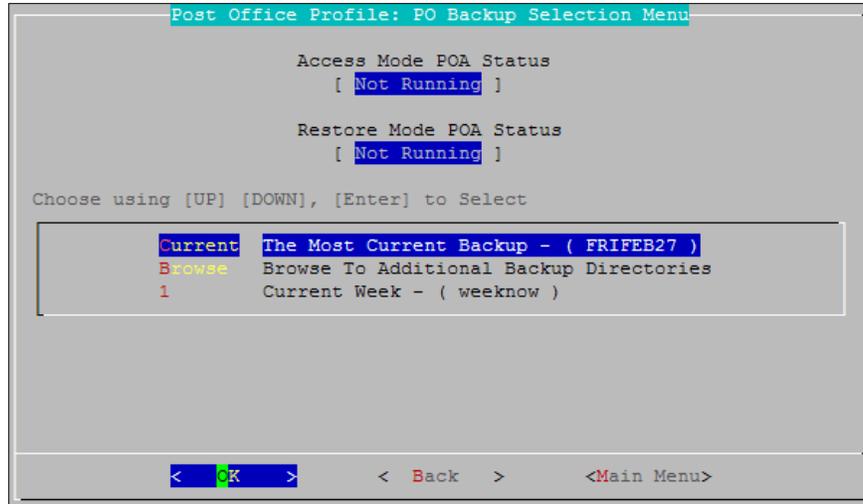
- Specify whether to load this POA against the most recent backup automatically.
- Specify whether to enable support for the GroupWise retention flag.

TESTING the Retain Integration Piece

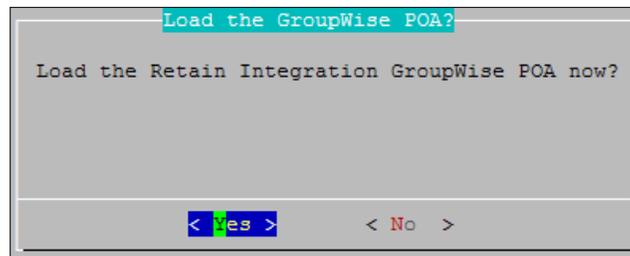
From the testing menu, you can load the POA to test it. You can also specify whether the POA should be loaded in graphical mode. Ordinarily, this is not necessary but for the purposes of testing, you may want to see it. This setting automatically reverts to DISABLED once you've done a load-up in graphical mode, so the setting is never stuck to ON



When you ask it to load the POA, it will ask you which backup to load. This is also a handy way of manually enabling an older backup for Retain to dredge. You will then be asked whether you want to load the POA.



Load the POA.



Once the Reload POA is loaded, you can run the Retain Job against Reload's POA.

Connectivity

The Connectivity settings option re-runs the connection settings wizard that is first filled out when the Profile is first created. This allows the administrator to change the settings if the environment of the Profile's target Post Office changes.

Working with a Reload Profile for a GroupWise Post Office That Has Moved to Another Server Platform

If a GroupWise post office has moved to a server that is on a different operating system or platform, the profile's connectivity settings must be edited. Change the connectivity settings to reflect the new platform and proceed through the prompts of the Connectivity Settings wizard. Make sure to test the profile, because when you change the Connectivity Settings of a profile, it is automatically disabled until such time as the testing process has verified the changes you have made.

Configuring the Reload Agent For Failed Connectivity

When the Reload Agent attempts to get a connection to the server that hosts the GroupWise Post Office, it can retry in its attempts if at first it fails. Use the **Retry** and **Wait** settings to configure the Reload Agent's behavior when connectivity cannot be established or re-established immediately.

Retry

When the Reload Agent runs a Standard (Incremental) Backup, it has several sub processes that run in order to obtain the data for a Standard Backup. If any one of the processes fails, a "Process Retry" counter increments. By default, if the Process Retry counter increments beyond 5, then the backup job is aborted. The value of this is if a Reload server is backing up other Reload Profile, it will not be consumed for a day trying to get the backup for a Profile that may be having problems. The factory default of 5 is a good Process Retry number, it can be lowered or increased, but it is not recommended that you lower the value below 2.

Wait

Reload can be set to 'wait' for a specified time after a failed attempt to connect to the live GroupWise system. This setting is used in conjunction with the 'Failed Backup Connectivity Retry Attempts' setting under the **Retry** menu. Both the **Retry** and **Wait** options are not necessary on a profile for a local machine.

Testing a Profile

Testing a Profile kicks off the Test and Initialize utility. If a Reload Profile is tested, and fails to pass the testing process, the only way to modify the profile and/or to correct the reason for the testing failure, is to go back to the "Create" menu from the Reload Administration Main Menu.

Advanced Scheduling

The Advanced Scheduling menu allows the ability to specify Reload backup job types to happen in a different manner than the daily/weekly approach of the Standard Schedule for a Reload profile. Most customers will want to stick to the Standard Schedule to mirror common backup procedures throughout the rest of their computing systems.

Using the Reload Run Job Creation Utility for Enhancing Reload Backups for Disaster Recovery Applications

Sit back for a minute, and really think this section through. Imagine that when your Reload server backs up your GroupWise post office, it takes approximately 18 minutes. What if you could get Reload to backup your GroupWise post office every hour, why not? For disaster recovery, wouldn't it be nice to have the most current backup be the one that Reload pulled just an hour ago? The Reload menu-based scheduling system has a traditional approach that is designed to only pull one Reload Standard (Incremental) Backup each day. Even if the scheduling system could allow for multiple backups, the Reload system is hard-coded to only keep up to three Standard Backups around per day. This way, if you were to manually kick off ten Standard Backups for a particular Reload Profile, Reload would automatically prune off the first seven Standard Backup jobs for that particular day. The "pruning" process of Reload is by design. However, if you were to pull 10 backups in a day, the problem is that users' mail that was purged from their trash, which was in one of the first 7 backups, is essentially not backed up. That's bad! How do we fix this?

The **Reload Run Job Creation Utility** allows you to work around Reload's standard design. Let's set up an example scenario. At ACME Corporation, they would like to backup up one of their GroupWise post offices every hour, from 6:00 (6:00 A.M.) to 18:00 (6:00 P.M.) However, they do not want any of the mail to be purgable, until a final backup is done by the Reload Scheduling system at 22:00 (10:00 P.M.) Here's how they would accomplish this task, as explained at a high-level.

- Use the **Reload Run Job Creation Utility** to create the six "Incremental" jobs using the Linux server's CRON system which is enabled by modifying the `/etc/crontab` file.

By default, unless you specify otherwise, the Reload Run Job Creation Utility tells the Reload Agent not to flag message items as purgable.

- Use the Reload Scheduling System to run the final Standard Backup job at 22:00 (10:00 P.M.). When this job runs, then the SmartPurge features that Reload integrates with will function, and messages will be flagged as purgable after the 22:00 (10:00 P.M.)

To see the syntax for the **Reload Run Job Creation Utility** type in the following command from in a terminal session:

```
reloadj
```

The output will be similar to this:

Reload Run Job Creation Utility - Version 1.2

This utility is for creating Reload run jobs

See the Reload documentation at www.gwava.com for more help.

The supported switches are as follows:

- h This help screen
 - p Specify the Reload profile to create run job for, use lowercase
 - i Create a Standard Backup (Incremental) run job
 - f Create a Portable Backup (Full Backup) run job
 - t Create a Tape Archive run job
 - e Create an Expire run job
 - s Do run a SmartPurge of messages when running an Incremental job
 - q Query to find out if a Reload job is currently running
- Incremental & SmartPurge Example: `reloadj -p po1 -i -s`
Incremental Example: `reloadj -p po1 -i`
Full Backup Example: `reloadj -p po1 -f`
Tape Archive Example: `reloadj -p po1 -t`
Expire Example: `reloadj -p po1 -e`

To schedule a Standard (Incremental) Backup job to happen for the Reload Profile “**po1**” the command would be:

```
reloadj -p po1 -i
```

To have the job executed by the Linux server’s CRON system every hour, add the following line to the `/etc/crontab` file:

```
1 6-18 * * * root reloadj -p po1 -i
```

This means the following:

<On the first Minute><Of Hours 6 – 18><Every Day><Every Day of the Month><Every Week of the Year> <root user privileges> `reloadj -p po1 -i`

For additional help on modifying a crontab file, consider searching for “linux crontab” at <http://www.google.com>.

Domain Database Profiles

Understanding What a Domain Database Profile Does

A Reload Domain Database profile backs up the essential components of a GroupWise domain, so that it can be used for disaster recovery purposes. A Reload Domain Database profile does not back up the subdirectories off of a GroupWise domain, or the configuration files for GroupWise gateways. The reason for this is that GroupWise is currently, running a GroupWise gateway on a different platform, and path is invalid.

A Reload Domain Database profile backup backs up the following files, and **only** the following files:

- wpdomain.db
- wpdomain.dc
- gwdom.dc
- gwpo.dc
- reveal.ini (For GWAVA Reveal)
- archsearch.txt (For GWAVA Reveal)
- reveal.xml (For GWAVA Reveal)
- gwsystem.xml (For GWAVA Reveal)

Accessing a GroupWise Domain Database Backup

Accessing a GroupWise Domain Database backup is easy. Here are the steps you would take:

For the most Current Backup

1. Go to the Reload Web Administration
2. Choose the Domain Database profile under the Domain Profiles section.
3. Select the "Access Backups" tab
4. Choose the option "Download Most Current Backup" as shown.



A Backup Other Than the Most Current Backup

1. Go to the Reload Web Administration Choose the Domain Database profile under the Domain Profiles section.
2. Select the “Access Backups” tab
3. Select “Select another Domain Backup for Download”. A drop-down menu will appear allowing you to choose the desired backup.
4. Select “Download Selected Backup”



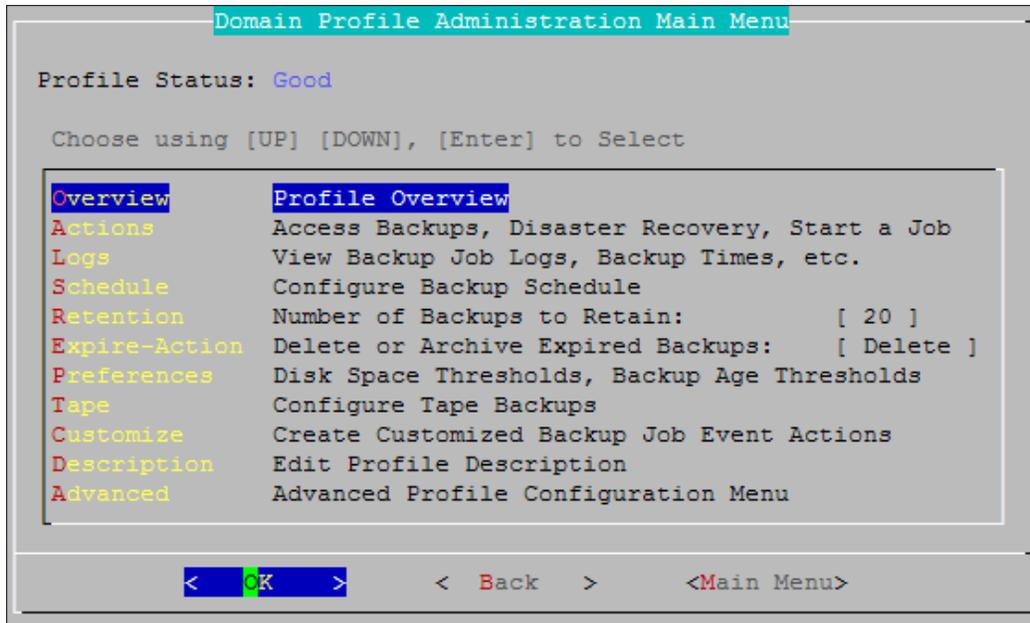
Basic Reload Domain Database Profile Configuration

This section discusses the basic configuration of a Reload Domain Database profile. All of the basic settings of a profile are accessible by selecting the following from the Main Menu.

Select Profiles (Modify Profiles)

Choose the domain profile to be modified

Having done this, you should see the **Profile Configuration Main Menu**, as shown in



Overview

The Overview gives you detailed information on the general function of the Profile you selected. This option is just an informational display, but contains useful information about the Profile:

- Name
- Description
- Status
- Path to stored data
- Live Domain platform
- Disaster recovery status
- Hot backups status
- Quick Restore status
- Tape backup enhancement status

Actions

The Actions menu allows you to access and select a backup to load, initiate disaster recovery, or start a backup job. Started jobs may take a minute or two before becoming active.

Logs

The Logs menu allows you to view either the rolling tail of this profile's agent or event logs, or the full logs, (static). This menu also allows you to set the log preferences for this profile.

Schedule

A Reload Domain Database profile Standard Backup job can generally happen any time of the day. It doesn't take long and generally does not require much bandwidth. If you would like to create more than one intra-day backup of a Reload domain profile, see the [Reload Job Creation utility section](#) for details on how to fit the paradigm of multiple daily backups.

Retention

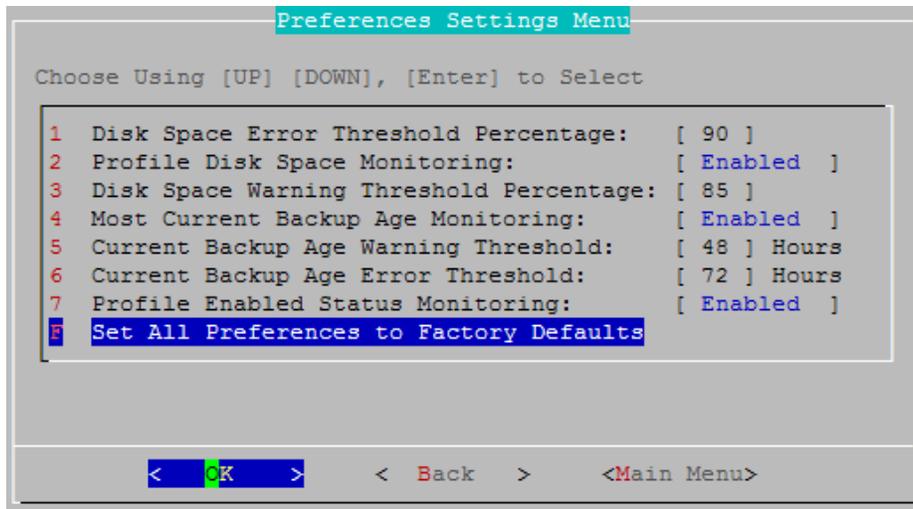
Each Domain Database backup uses approximately the size of the WPDOMAIN.DB from a GroupWise domain in disk space. Because of this, it is feasible to keep around several weeks' worth of backups of a Reload Domain Database backup.

Expire Action - Delete or Archive

Reload can be configured to either delete or archive data that has expired. The Archive feature requires that you specify a location for the Reload Agent to move the backup after it has expired. The idea being, that perhaps a NAS device or some other mass storage solution is in-place where the backed up GroupWise data can be moved to. Once Reload has archived a Domain Database backup, the Reload server no longer manages the backup. Most customers will not choose to use the Archive feature, but some may find it useful, if they have mass storage solutions in place and a need for backed up GroupWise data to be easily available.

Preferences

The Preference Settings Menu allows you to configure monitoring and the warning and error thresholds for this profile.



Error and Warning thresholds

Setting the error and warning thresholds will allow Reload to alert you via email, before a problem blocks Reload's normal system functions can develop. This setting allows Reload to monitor the disk space and backup age for your system in order to warn you if they exceed your specified amount. The monitoring for each warning and error threshold must be enabled for the threshold to take effect. **The warning and error thresholds allow Reload to be a 'set and forget' system which will contact you if there is a problem.** Status reports, warning, and error threshold messages all use Postfix to send email messages. **Postfix must be running and configured for you to receive warning messages from the Reload system.** Postfix is included in the standard Linux platform by default.

The Disk Space Warning and Error thresholds are a percentage, and are tied to the amount of space left on your hard disk. They will warn you when your system starts running out of disk space.

The Current Backup Age Warning and Error thresholds will warn you when the latest backup in your system exceeds the listed age for each threshold. The variable is in hours. This may indicate a failure for a Profile's backup schedule, and the status should be checked. A disk space error will lead to a backup age error. When there is no longer enough space to complete a full backup, Reload will stop creating backups until space becomes available.

Specify Archive Path

This option will only appear if the Expire-Action is set to "Archive". This is the location that the Reload server should put the archived Reload Domain Database backups. The Archive Path should be a path that is available to the Reload server. If you combine the "Pre-ARCHIVE" and "Post-ARCHIVE" commands (explained a little later) to create a mount to a different server, then Reload can "push" the Reload Portable Backups to the new server location. The Portable Backup Archive directory that gets created by Reload follows this naming convention:

<profile name>-<Backup Directory Name>-archive

Example:

dom1-15-monaug28-2006-archive

Configuring Tape Backups

Reload does not eliminate the need for offline (cold) backup solutions, such as tape backup solutions. Most organizations will still need to retain a tape backup system. However, Reload can prolong the life and enhance tape backup solutions in the following manner:

- Eliminates wear and tear on your tape backup systems, because most backed up data will be retrieved from the Reload server, and not tapes
- Reload can create a Tape Archive (*.tar) file which contains the entire contents of a Domain Database backup set within it.
- Reload can be configured to run a “Pre-TAR” command and a “Post-TAR” command. With this architecture in place, some customers have designed Reload to “push” the *.tar file that Reload creates to their backup server. In this section we will explain how to do this.

Schedule

When the Reload Domain Database backup runs, it runs the Tape Backup routine towards the end of the backup. There is no need to schedule a special time that the *.tar file will be created.

Create Tape Archive (TAR) Files

By configuring Reload to create *.tar files, the Reload Agent creates a *.tar file out of the Domain Database backups available for a particular Reload Profile. Creating the *.tar file does not eliminate the backup, the *.tar file is created in addition to the backup.

The *.tar file that gets created by the Reload Agent follows this naming convention:

<profile name>-<Domain Database Backup Directory Name>.tar

Example:

dom1-15-monaug28-2006.tar

Expire Old Tape Archive (TAR) Files

When Reload creates *.tar files at the path that you specify, you can have Reload delete the *.tar files that were created for the Reload profile previously. Here’s what this does.

- Reload creates the *.tar file when the Reload Agent runs the tar routine
- The tape backup solution can be pointed at the location where Reload creates the *.tar file so that it can be backed up
- The next time the Reload Agent creates a *.tar file (generally this will be the next day), the Reload Agent will delete any files that following the naming convention of:

<profile name>-<Domain Database Backup Directory Name>.tar

- The Number of Tape Archive Files to Retain setting does allow for Reload to allow a certain number of *.tar files to be retained, before it expires them. This design is in place particularly to help in scenarios where customers expect to be creating intra-day backups.

Specify Tape Archive (TAR) File Path

This is the location that the Reload server should put the *.tar file. The TAR File Path should be a path that is always available to the Reload server. However, if you combine the “Pre-TAR” and “Post-TAR” commands (explained a little later) to create a mount on the Reload Linux server to a different server, then Reload will effectively “push” the *.tar file to another server.

Configuring Advanced Tape Settings

The Reload Agent can execute the command called the “Pre-TAR” Command before it puts the *.tar file at the Tape Archive (TAR) File Path. The Reload Agent can also perform a “Post-TAR” command. When the Reload Agent executes the Pre-TAR command that you specify, the following happens:

- The Reload Agent creates the *.tar file from the Portable Backup that is being copied into the *.tar file.
- The Reload Agent sends the Pre-TAR command to the background to be executed by the Linux operating system.
- The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by the **Customized Pre-TAR Command Wait Time**.
- The Reload Agent copies the *.tar file that it created previously, to the TAR File Path.
- If a Post-TAR Command is specified then the Reload Agent does the following:
 - The Reload Agent sends the Post-TAR the command to the background to be executed by the Linux operating system.
 - The Reload Agent does not check to see the status of the command, but it does wait for the amount of seconds specified by **Customized Post-TAR Command Wait Time**.

Configuring the Reload Agent to “Push” a *.tar File to Another Server

Because of the ability to specify a Pre-TAR and a Post-TAR command, you can effectively get the Reload Agent to “push” the *.tar file that it creates to a different server. Some customers have done this. Here’s an explanation of how it is done. Goal: Get the Reload server to push the *.tar file to a Windows server that is running Veritas.

1. Create a directory that will be mounted to the Windows server with a CIFS mount.

For example: **/data/tape**

2. Create a BASH shell script to mount the /data/tape directory to a Windows share created on the Windows server running Veritas. For more guidance on making a Windows share, you can read the section titled “Creating a Reload Profile for a GroupWise Post Office or Domain on a Windows Server” in Chapter 4.

Reload ships with a great little (un-supported) CIFS mount BASH shell script. You may consider using this script. The name of the file is cifsmnt.sh and it is located in the directory: /opt/beginfinte/reload/setup

Run the **cifsmnt.sh** script from within a terminal session, and read the instructions of this utility for more guidance on using this script.

3. In the Pre-TAR Command, specify the command that performs the CIFS mount.

4. Specify a time that the Reload Agent should pause to allow the Pre-TAR command to complete. Generally the default of 10 seconds is sufficient.
5. In the Post-TAR Command, specify the command that performs the dismount of the CIFS mount created with the Pre-TAR command.
6. Specify a time that the Reload Agent should pause to allow the Post-TAR command to complete. Generally the default of 10 seconds is sufficient.

Customize

The customize feature allows for a custom action that the Reload server will perform in the event of the following three states of a Job.

- Job Start
- Job Error
- Job End

You could for example, have a script process send an e-mail if a Standard Backup job errors. Reload ships with a script called “**mailer.sh**”. Because this is a script, and can be modified, the script is not a supported component of Reload. However you could consider using this script to generate an e-mail. The script is located in the directory:

/opt/beginfinite/reload/setup

If you were to reference the mailer script in as the Customized Job Error Command, the syntax you would use would most likely be:

```
cd /opt/beginfinite/reload/setup
./mailer.sh -c mailer.conf
```

To learn more about the mailer script, run it once, to see the syntax and usage for this script. To run the script, do the following. In a terminal session, go to the directory where the script is located, and run it. Example:

```
cd /opt/beginfinite/reload/setup
./mailer.sh
```

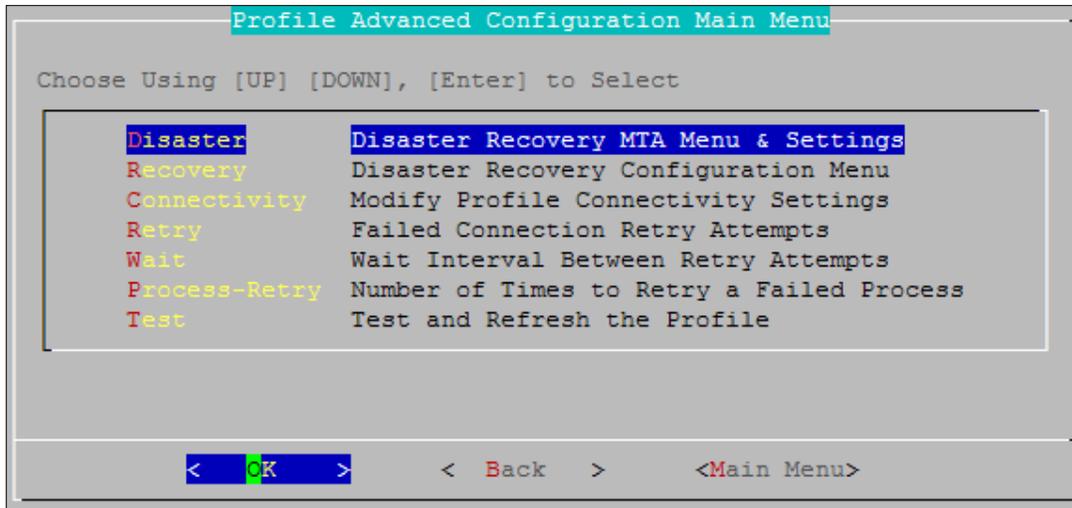
Customize - Job Event Actions

The Reload Agent can execute the commands called the “Job Start” Command before it puts the Domain Database backup to be archived at the Archive Path. The Reload Agent can also perform “Job Stop” and “Job Error” commands. All these commands can be specified here.

Advanced Reload Domain Database Profile Configuration

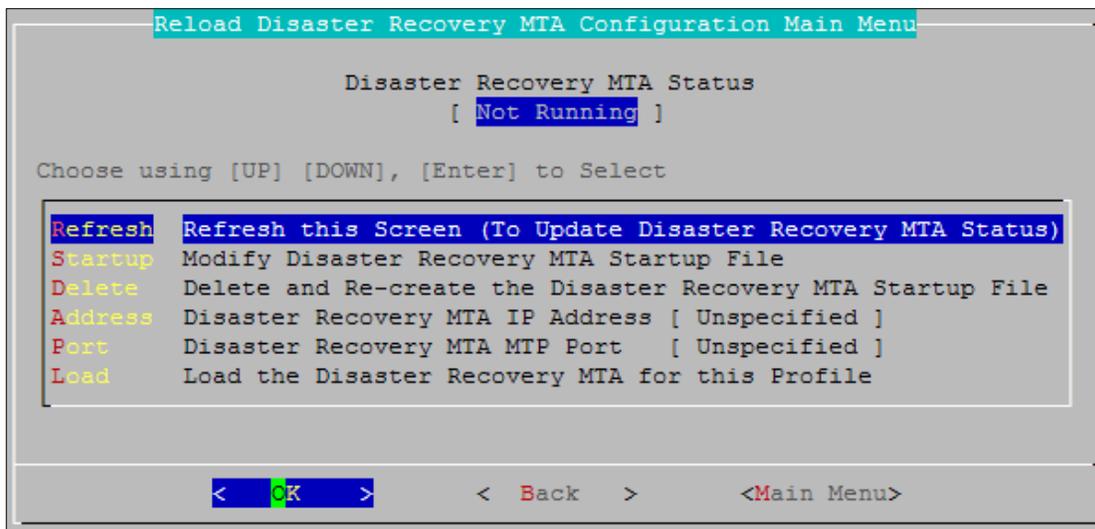
The Profile Advanced Configuration menu, shown below, is available by selecting the following from the Main Menu:

- **Profiles** (Modify Profiles)
- **Choose** the Reload Profile
- **Choose Advanced** (Advanced Profile Configuration Menu)



Disaster MTA Menu & Settings

From the “**Disaster**” menu, shown below, you can modify the behavior of the Disaster MTA for a Reload Profile. The Disaster MTA is the MTA that is loaded when disaster recovery is enabled for a Reload Domain Database profile.



By default when loading a Disaster MTA accessing a Reload generated backup, the MTA will listen on all IP addresses bound to the Reload Server, on the default port that the MTA is configured to listen on. In some environments, this will work fine.

However, in others, particularly those where the Reload server is housing several Reload Profiles, the behavior of the GroupWise MTA needs to be configured differently.

Imagine the following example. ACME Corporation is using their Reload server to backup all three GroupWise domains. The names of these domains are:

- DOM1 (**dom1.acme.com**)
- DOM2 (**dom2.acme.com**)
- DOM3 (**dom3.acme.com**)
-

ACME wants to enable disaster recovery for all three domains. In their live GroupWise system, each of the GroupWise MTA's are listening on port 1700. ACME would like to keep this same TCP port convention for convenience. Here's how then can accomplish this task:

- Bind the Reload Server to three different IP Addresses
- Configure the **Live** settings for the Reload Profile so that the MTA for that Reload Profile is using just one of the three IP Addresses
- For ease of use purposes, consider binding in the DNS server, the IP Addresses to logical names, for example:
 - DOM1 on the Reload Server: **dom1.backup.acme.com**
 - DOM2 on the Reload Server: **dom2.backup.acme.com**
 - DOM3 on the Reload Server: **dom3.backup.acme.com**

Modifying a Reload Profile's Disaster MTA Startup File

In most customer environments, there is no need to modify the disaster MTA's startup file. However in some environments, especially those using SSL, there will be a need to modify the MTA's startup file to add additional settings to the MTA's startup file. You can do so by choosing the menu **Startup** (Modify Disaster MTA Startup File).

Using the menu option to modify the Live MTA startup file, it only works if you are in an XWindows environment. So if you were SSH'd over to the Reload server, you will not be able to use this menu option. In an SSH session, the Reload Administration utility will let you know what path the Live MTA's startup file is located at so you can edit it with an editor such as vi. To change the default editor that Reload uses go to the following menu location in Reload Administration System | Editor, and choose the editor that will work in your environment. For a KDE desktop KWRITE, KATE and GEDIT will all work. For a GNOME desktop, only GEDIT will work. Loading the Live MTA for a Profile

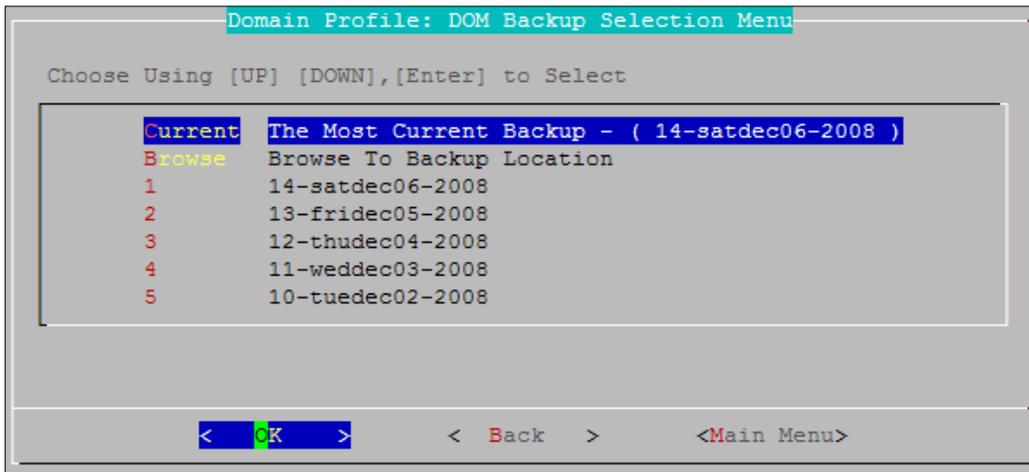
Load

In General, the Disaster MTA is only loaded in conjunction with a 'disaster' which inhibits the live GroupWise POA from functioning in the mail system. However, every profile's Disaster Recovery Plan should be tested before an actual Disaster occurs. **Be sure to also create a [Disaster Recovery Plan](#) that dictates all actions needed to implement Disaster Recovery for your System.** This plan can be added to the Web Administration for easy access.

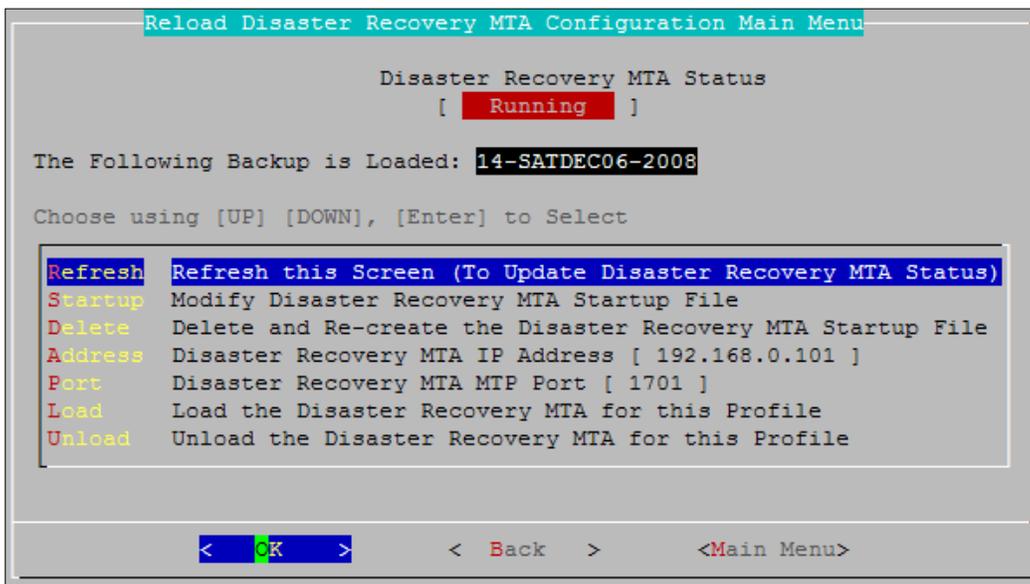
Your Disaster Recovery Plan should contain all the steps, in order, for your system. There may be several steps required for your system to connect the Disaster MTA to the live GroupWise mail system. If setting changes are required to be made in ConsoleOne, those settings and changes should be listed, with the exact variables which are needed to be changed. There is a generic placeholder document which is currently linked in the Reload Web Administration. The Placeholder disaster recovery plan contains helpful information in creating your own disaster recovery plan. Create your own and replace the placeholder. See the [Web Administration Preferences](#) section for details.

After you have configured and checked the settings for your Disaster MTA, you may continue on to test the Disaster MTA for your system.

When you select and confirm to load the Disaster MTA, you are prompted to choose which backup you wish to load the MTA against. By default the Disaster MTA will use the latest backup unless you specify otherwise. Once you have selected the Backup to use, you may trigger a failover, from the Recovery menu or from the Web Administration.



Once the Disaster MTA has been loaded, the Disaster menu will now display the backup that the Disaster MTA is using, along with the option to unload the Disaster MTA.



Verify that the Disaster MTA is running and can be accessed by your Mail system. Run through your Disaster Recovery Plan and make sure that the system will work as expected.

Recovery

This menu links to the Disaster Recovery menu for this Profile. See the [Disaster Recovery section](#) for information.

Connectivity

The Connectivity settings option re-runs the connection settings wizard that is first filled out when the Profile is first created. This allows the administrator to change the settings if the environment of the Profile's target Post Office changes. Once you modify a Profile's Connectivity Settings the Reload Profile needs to be tested and initialized again in order for the Profile to be active.

Working with a Reload Profile for a GroupWise Domain That Has Moved to Another Server Platform

If a GroupWise domain has moved to a server that is on a different operating system or platform, the profile's connectivity settings must be edited. Change the connectivity settings to reflect the new platform and proceed through the prompts of the Connectivity Settings wizard. Make sure to test the profile, because when you change the Connectivity Settings of a profile, it is automatically disabled until such time the testing process has verified the changes that you have made.

Configuring the Reload Agent for Failed Connectivity

When the Reload Agent attempts to get a connection to the server that hosts the GroupWise domain, it can retry in its attempts if at first it fails. Use the **Retry** and **Wait** settings to configure the Reload Agent's behavior when connectivity cannot be established or re-established immediately.

Retry

When the Reload Agent runs a Standard Backup, it has several sub-processes that run in order to obtain the data for a Standard Backup. If any one of the processes fails, a "Process Retry" counter increments. By default, if the Process Retry counter increments beyond 5, then the backup job is aborted. The value of this is that if a Reload server is backing up other Reload Profiles, it will not be consumed for a day trying to get the backup for a Profile that may be having problems. The factory default of 5 is a good Process Retry number, it can be lowered or increased, but it is not recommended that you lower the value below 2.

Testing a Profile

Testing a Profile kicks off the Test and Initialize utility. If a Reload Profile is tested, and fails to pass the testing process, the only way to modify the profile to correct the reason for the testing failure, is to go back to the "Create" menu from the Reload Administration Main Menu.

Disaster Recovery

Reload has three different Disaster Recovery Modes. They are:

- **FAILOVER** – When your live post office or domain server cannot be recovered, and you need to use Reload as a live server.

- **MIGRATE** – When you have re-built a live server and you want to move the post office or domain off of the Reload server, back to a live server.
- **FAILBACK** – You take this action when the live data is migrated back to the live server, and you are no longer using the Reload server as a live server.

Disaster Recovery

Disaster Recovery must be configured and tested before a disaster happens. The Disaster POA and MTA will default to the Reload Server’s IP address(es) with the default port and the latest backup for each profile unless configured otherwise. If this default behavior is not desired, each profile must be configured separately. See the profile “disaster” sections for details. ([Disaster MTA](#) , [Disaster POA.](#))

In the case of a disaster, there are three different methods for enabling disaster recovery for a GroupWise post office or domain:

Reload Web Administration Method

Log into the Reload Server’s Web Page

Choose the post office or domain profile that needs to be switched over to for disaster recovery purposes.

Choose the “Disaster Recovery” Tab.

Choose the option for **FAILOVER**.

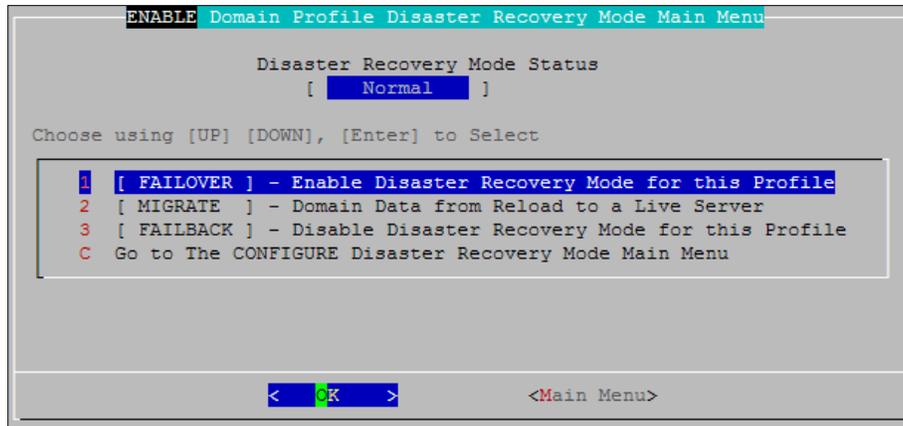


Reload Console Administration Method

1. **Get** a VNC, or SSH session, or go to the Reload server Console
2. **Run** Reload Administration, either from an icon, or type in the command:

reload

3. **Select** Recovery (Disaster Recovery)
4. **Choose** the post office or domain profile that needs to be switched over to for disaster recovery purposes.
5. **Choose** the option for **FAILOVER**.



Reload Mobile Administration Method

1. **Get** an SSH session to your Reload server from your wireless device
2. **Run** Reload administration by running the command:

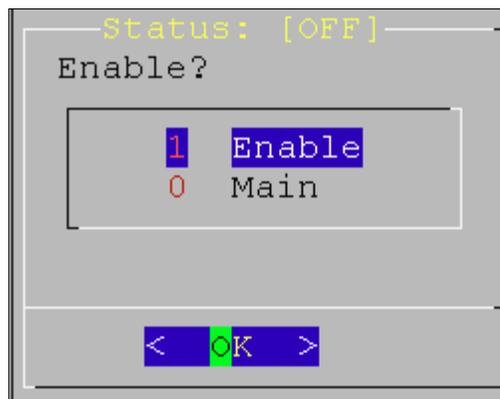
reload

or

reloadm

(This forces the Reload Mobile menu)

3. **Select** DR
4. **Choose** the post office or domain profile that needs to be switched over to for disaster recovery purposes.
5. **Choose** the option "1. Enable".

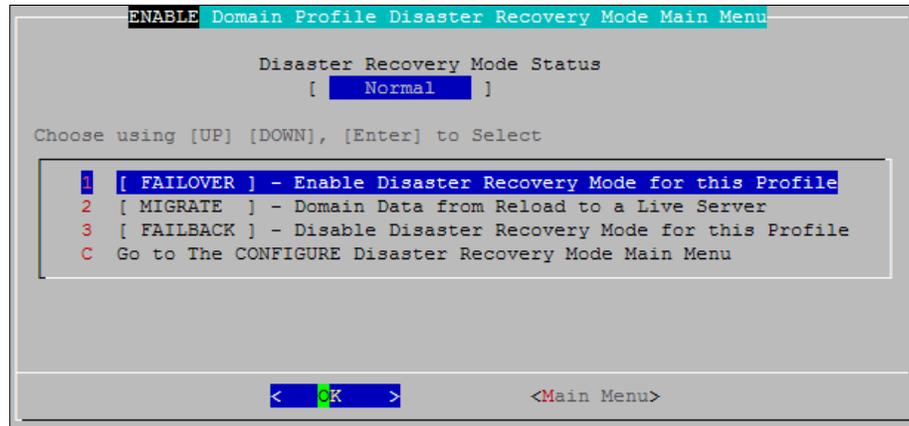


Configuring Disaster Recovery Actions

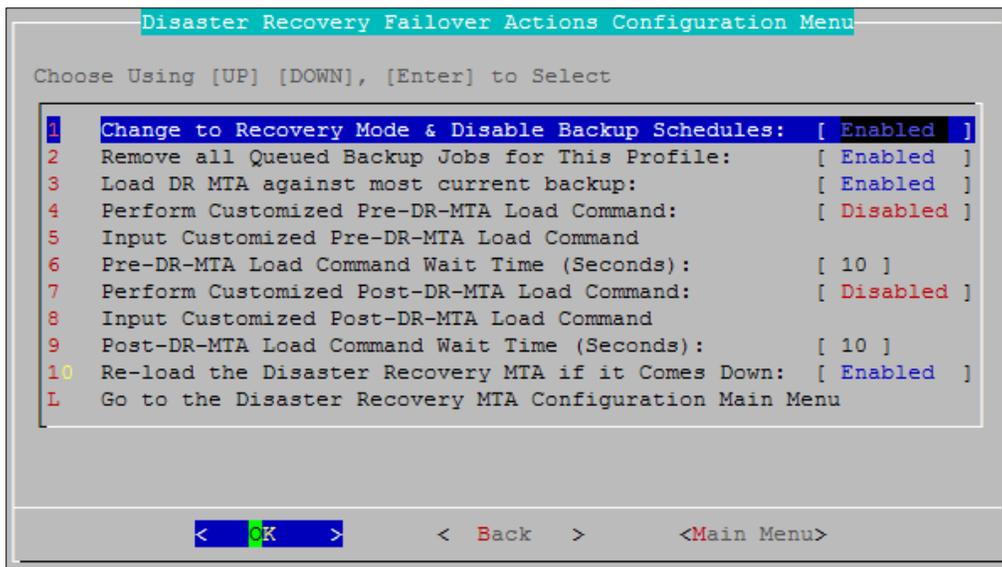
Reloads disaster recovery **FAILOVER** and **FAILBACK** capabilities are meant to be enabled with the push of a button. When the button is pushed, a handful of things can happen, and will happen by default. By default a **Reload** profile has default actions that are taken when **FAILOVER** or **FAILBACK** are chosen. However, Reload also creates a framework for allowing the **FAILBACK** and **FAILOVER** actions to perform automated actions also. Generally in the case of a disaster recovery scenario you would do the following:

- **Choose FAILOVER**

- **Rebuild** a live server that will house the GroupWise post office or domain that is currently running on the Reload server
- **Choose MIGRATE**; to move the data from the Reload server back to a live server. **Test** the migrated data at the new location to ensure that it is working just fine
- **Choose FAILBACK**



To Configure the steps taken during failover, Select the “Go to the CONFIGURE Disaster Recovery Mode Main Menu” option and select “Configure [Failover] – Enable Disaster Recovery Mode Settings”

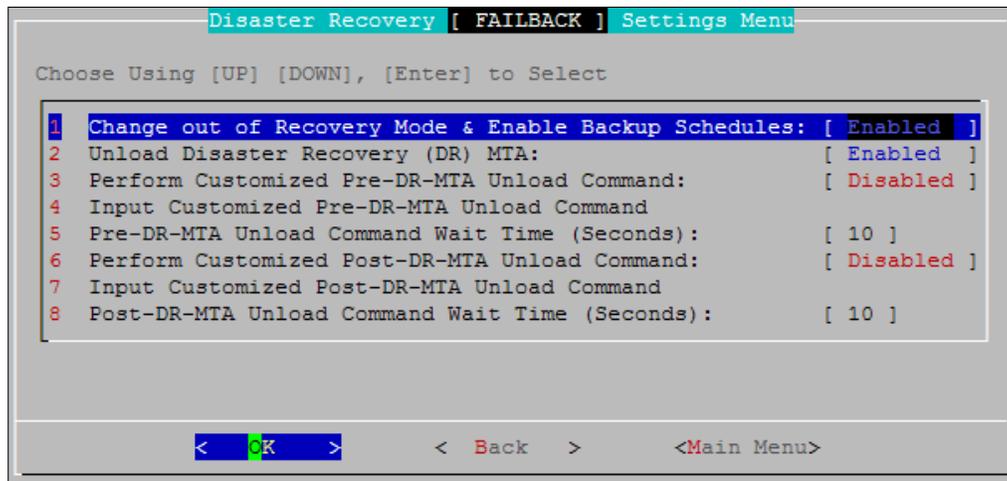


Here you can define the actions that are taken with FAILOVER option enabled. By Default, the following actions are taken:

- The **Profile** is **switched** to **FAILOVER** mode
- **All** backup schedules for the **profile** are **disabled**, until **FAILBACK** is **enabled**
- **All** queued **jobs for backups** for the **profile** are **removed**
- The **Disaster Mode agent (POA or MTA)** for the profile is **loaded**
- **Optional** – A customized pre-load agent and post-load agent command can be executed

The idea behind the customized pre-load and post-load commands is that you can make a script that performs an action. For example, you could call a script that loads a GroupWise Internet Agent or perhaps a script that telnets to a DNS server and switches a DNS A record entry.

You may also modify the **FAILBACK** options.



Here are the Default actions that are taken with **FAILBACK** are enabled:

- The **Profile** is **switched** back to **normal** mode
- All **backup schedules** for the profile are **re-enabled**
- The **Disaster Recovery Mode agent** (POA or MTA) for the profile is **un-loaded**
- **Optional** – A customized pre-unload agent and post-unload agent command can be executed

The idea behind the customized pre-load and post-load commands is that you could make a script that performs an action. For example, you could call a script that unloads a GroupWise Internet Agent or perhaps a script that telnets to a DNS server and switches a DNS A record entry.

It is vitally important to test your setup and Disaster Recovery configuration before a Disaster occurs.

After configuring your system for Disaster Recovery, test the configuration and verify that all steps work as expected for your system.

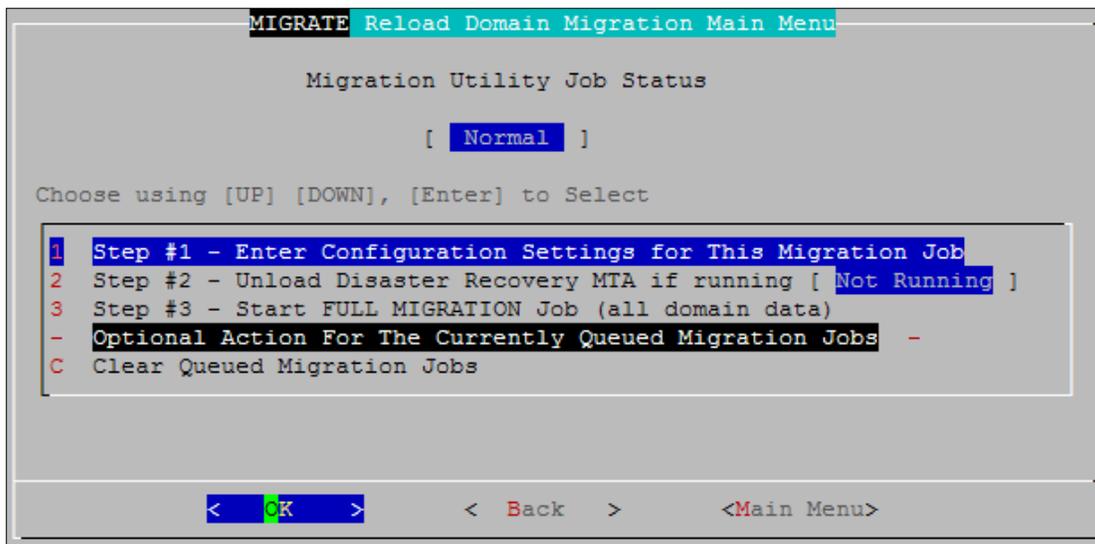
After you have successfully tested your system, verify and upload your [Disaster Recovery Plan](#) to the [Web Administration](#).

Migrating Data Back to a Live Server

When you failover to a Reload server, the data on the Reload server will be updated with new data that you will want to have back on the Disaster Recovery GroupWise system. So once you have a live production server prepared to function as the live production post office or domain, you will need to get the data migrated from the Reload server, over to the live production server.

The Reload Migration Agent can help you to accomplish this. The Reload Migration Agent copies the live post office or domain that has been running on the Reload server, to the location that you specify.

To configure the actions of the Reload Migration Agent, use the MIGRATE option under Disaster Recovery, and simply follow the wizard for migrating. A post office migration can take a while, particularly for the contents of the OFFFILES directory to replicate over. It is for this reason that the PRE-MIGRATION job type is in place. When migrating a GroupWise post office from the Reload server to a production server, make sure to run the PRE-MIGRATION first. When the PRE-MIGRATION job is running, your Reload server can still be hosting the post office. Then, when the PREMIGRATION is complete, you will want to bring down the Live Mode POA, and run the FULL-MIGRATION job.



Disaster Recovery and Internet Mail

Perhaps you want to make your Reload server a GWIA in the case of a disaster. This is feasible; however it is important that you design your system to allow for this to happen very smoothly. Please read the Novell Press Novell GroupWise 7 Administrator Solutions Guide. Then read Chapter 32 of this guide titled: "Creating a Highly Available GroupWise Internet Agent Solution". You should then consider creating a GroupWise secondary domain that will always be hosted on the Reload server. This secondary domain will host an auxiliary GroupWise Internet Agent that will most likely not be running. You can then configure the Reload Domain Database profile that is backing up the GroupWise domain that also hosts your GWIA regularly, to load the auxiliary GWIA. This can be done with the Customized Load Command functionality of the FAILOVER feature of a profile.

The reason you must use an auxiliary GWIA is because GroupWise gateways cannot be run from a location other than the location they are hard-configured to run at. So the next best thing is to use an auxiliary GWIA, in conjunction with the instructions in Chapter 32 "Creating a Highly Available GroupWise Internet Agent Solution" in the Novell Press Novell GroupWise 7 Administrator Solutions Guide.

Upgrading Reload Software

Reload is being actively developed. Reload is being continuously improved, and tightly integrated with changes made to GroupWise. It is important to keep your Reload software upgraded. There are four different ways to upgrade Reload. This chapter explains all four ways to upgrade Reload. The Reload Upgrade Tool cannot be run more than every 10 minutes. So if you attempt to upgrade Reload, you must wait another 30 minutes in order to make another upgrade attempt. If you do attempt to upgrade within the 30 minute window the Reload Upgrade tool notifies you via its log how many more minutes you must wait until you can attempt an upgrade.

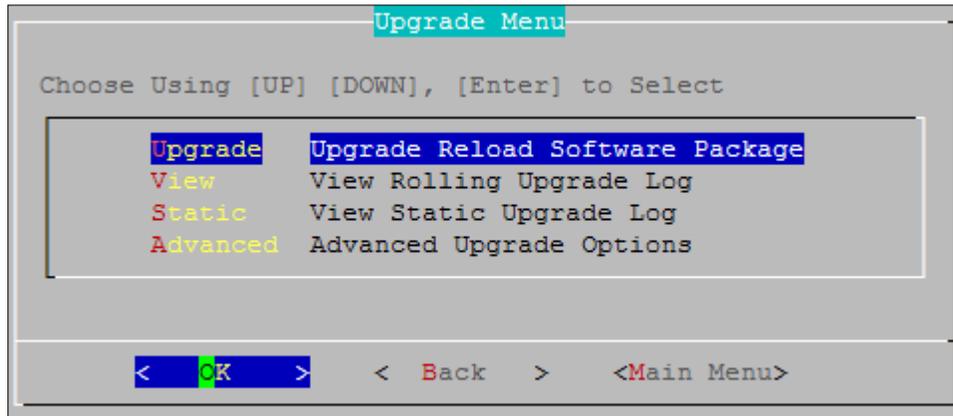
The Reload Upgrade Tool requires that the Reload Server have HTTP access to the Internet. If the Reload Server does not have HTTP access to the Internet it will write to its log file that is unable to access the Internet. The Reload Upgrade Tool keeps a log called: **upgrade.log**. This log file is located in the following path

`/opt/beginfinite/reload/logs`

The **upgrade.log** records the events associated with the upgrade of the Reload Software Package. The **upgrade.log** file is viewable from within Reload Administration within the Upgrade Menu. The **upgrade.log** file is self-pruned by the Reload Upgrade Tool, and will not grow too large.

Upgrading Reload Through Reload Administration

To access the Upgrade Menu within Reload Administration, select: **System | Tools | Upgrade**



1. When you select **Upgrade** the Reload Upgrade Tool checks to see if a newer version of Reload is available. If a newer version is available, the Reload Upgrade Tool will install the newest shipping version of Reload.
2. From the Advanced Upgrade Options menu you can upgrade Reload to the latest Field Test Code. You can also choose to roll back off of the latest Field Test Code and revert to the latest Shipping Code for Reload.

Upgrading Reload from a Command Line Session

The Reload Upgrade Tool can be run within a Terminal Session outside of Reload Administration.

To do so just open up a terminal session, or an SSH session to the Reload server and type in the following command:

```
reloadu
```

The Reload Upgrade Tool has some additional switches that it supports. For example to instruct the Reload Upgrade Tool to download the latest Field Test Code (if there is any) then type in the command:

```
reloadu -f
```

Or if you want to override the Reload Upgrade Tool's version control logic, you can use the command:

```
reloadu -o
```

If you have upgraded to the latest Field Test Code, and you want to roll back to the latest Shipping Code, then you can type in the command:

```
reloadu -r
```

To install the latest GroupWise Software Integration components (DBCOPY and the GroupWise Agent Software, then you can type in the command:

```
reloadu -g
```

Upgrading Reload from the Reload Web Administration

See the [Web Administration Upgrading](#) Section.

Upgrading Reload Automatically

You may want to have the Reload Upgrade Tool run automatically, via a “cron” job on the Reload server. To do so, you should add an entry to the **crontab** file on the Reload server. Here are example steps for having the Reload Upgrade Tool run on the Reload server every week on Wednesday at 1:00 A.M. Edit the **/etc/crontab** file in text editor. For example the Kwrite, gedit or vi editors. We’ll use Kwrite in this example:

```
kwrite /etc/crontab &
```

Add the following text on its own line in the **crontab** file:

```
00 1 * * 3 root /usr/sbin/reloadu
```

Save the **crontab** file.

For additional help on modifying a crontab file, consider searching for “linux crontab” at <http://www.google.com>.

Uninstalling and Re-installing Reload With the Reload Upgrade Tool

By uninstalling the Reload Software Package, and re-installing it you can get a newly install Reload code set in case you suspect that the Reload software is corrupt.

Uninstalling Reload does not delete any configuration data, profiles, or profile backups.

If you wanted to uninstall the Reload Software Package, and then re-install it, here are the steps for doing so:

1. **Open** up a terminal session on the Reload server, or an SSH session to the Reload server
2. **Run** the Reload Uninstall utility in the following manner: **/opt/beginfinite/reload/uninstall**
3. **Follow** the prompt to uninstall Reload.
4. **Type** in the command: **reloadu**
5. This will download and install the Reload Software Package from the Internet

Reload Web Administration

Reload Web Administration is mainly a monitoring application designed for everyday use. Reload's Console Administration provides full functionality and access to the creation and modification of profiles, data locations, and backup schedules. These should remain consistent for your system. Reload Web Administration does not allow profile creation or editing.

Web Administration does provide a graphical display that combines all pertinent information at a glance to provide ease of use for monitoring and daily administrative tasks without the danger of inadvertent changes to the critical backup infrastructure.

Every icon and clickable item in the Web Administration has a tool-tip explanation which will give you information on the function of the item or what the icon represents.

Reload Web Administration can be accessed through any browser with the following address:

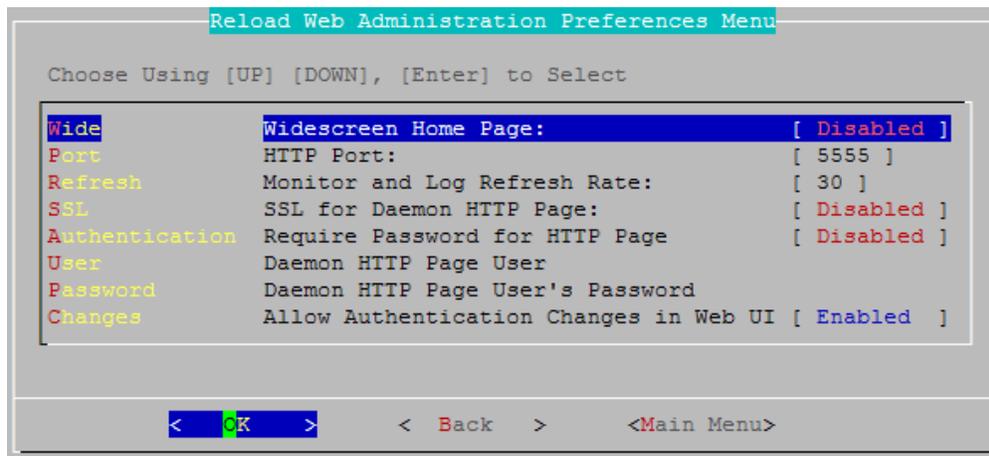
http://<Reload_server_ip_or_DNS>:5555

Unless you have enabled SSL, which would change the address to:

https://<Reload_server_ip_or_DNS>:5555

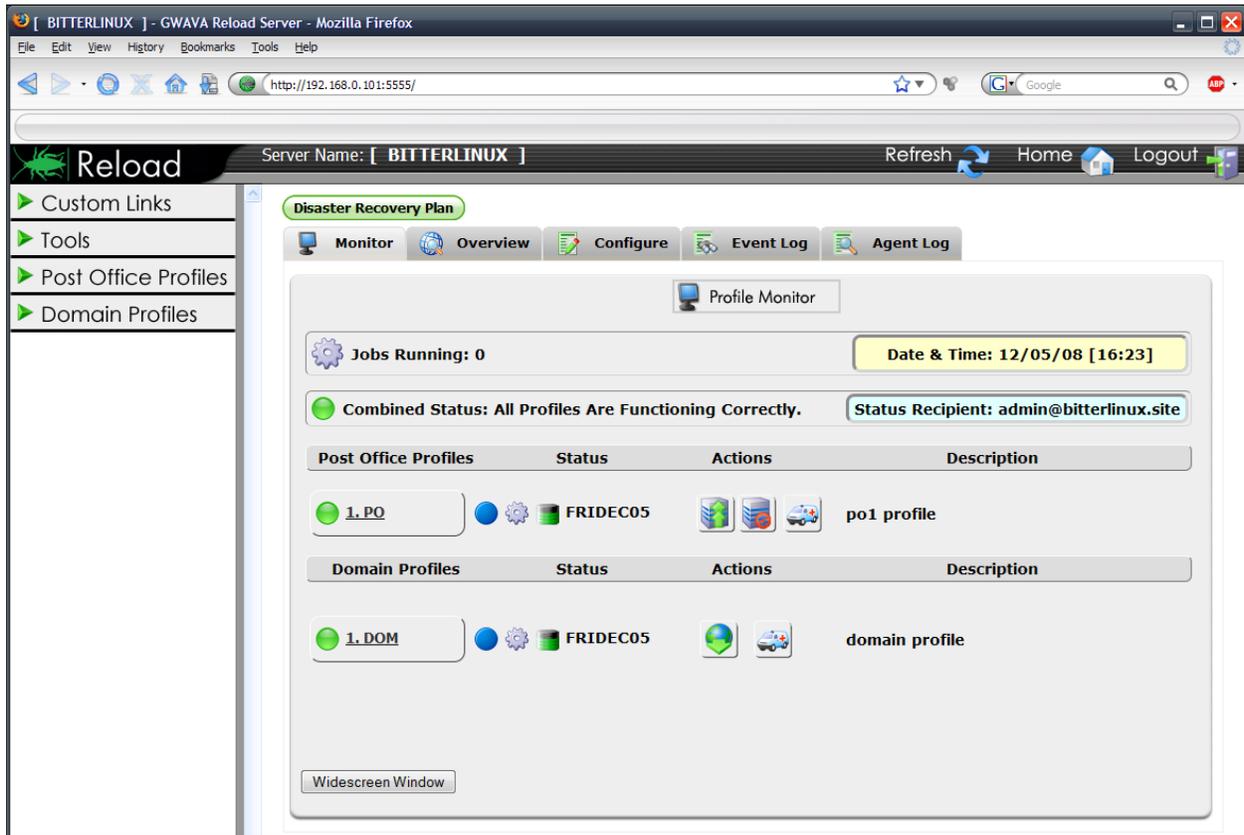
Much of the functions of the Web Administration can also be modified through Reload Console Administration. In Reload Console Administration, select **System | Web**.

This menu allows you to modify the general preferences, port, refresh rate (in seconds), SSL, authentication and whether to lockdown changes in the Web Administration or not.



When you first connect, unless you have modified it, you will see the default homepage, the monitor page for your Reload system.

Monitor



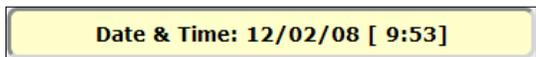
The above window shows a small Reload system with a post office and a domain profile active. If you have not yet created a domain or post office profiles, then this screen will have no profiles listed. To create a profile, you must use Reload Administration.

The initial screen displays the status of your Reload Post Office and Domain profiles, if there are any running jobs, and provide links to each particular profile or system for you to view the details.

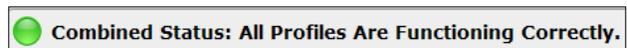
Disaster recovery Plan – this download link to the disaster recovery plan document. This should be created by the system administrator for future reference. On default, the document is a placeholder document which details what a disaster plan should contain. To edit the download link, see the configure tab, [web administration section](#).

Jobs Running – This shows how many jobs are running currently.

Date & Time – The current time for the Reload server.



Combined Status – The combined status shows the overall health of your system. The Green light shows no problems. Yellow, Red, or blue lights indicate a system that requires attention or has an error. Click on the combined status indicator to send the current



status report to the status recipient.

Status Recipient- the destination email address for all status reports is listed here.



Post Office profile (1. PO in the picture): All post

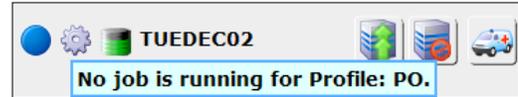
office profiles are listed here, along with their status and possible actions. Selecting the Profile name opens the page for that Profile.



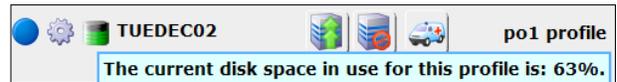
Status – like with the combined status, this indicator shows the overall status of this specific profile. A simple hover with the mouse will tell you details about the status.



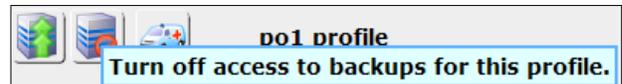
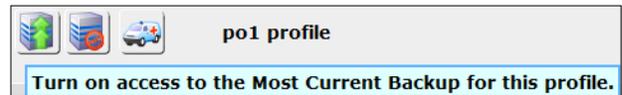
Running Job – if a job is running in your system, one of your profiles will be involved. The gears next to the profile status will indicate if a job is running. Animated green gears indicate a running job. Gray static gears indicate no job running.



Disk Usage – One of the most important bits of information on the profile is the current disk usage. This is most often overlooked, and is vitally important for your Reload system. The current disk usage is the total amount of used and free space for the hard drive resources in the Reload Server. If the free space is used-up, Reload will be unable to create rolling backups. Hover over the icon with your mouse to be shown the percentage of disk usage.



Most Current Backup Access – These buttons turn on and off access to the most current backup. This allows the users to access the information that is stored in the backup.

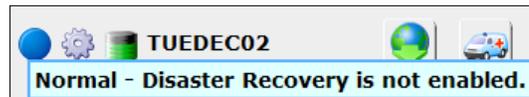


Enable Disaster Recovery Failover – With one click you can initiate disaster recovery Failover. If currently enabled, this switch allows you to reverse the process.



Domain Profile (1. DOM in the picture):

The only difference in the interface between Post Office profiles and Domain profiles is the access to the backup. Since mail is not stored in the Domain, the entire domain is allowed to be downloaded. This is the



actual domain database file, zipped, for download from this link.

The **Widescreen Window** button adds or removes the navigation panel on the left of the browser. This changes between the traditional Reload **navigation window** and the new widescreen interface for the web browser.

The picture below shows a running job on the Post Office profile.

Disaster Recovery Plan

Monitor Overview Configure Event Log Agent Log

Profile Monitor

Jobs Running: 1 Date & Time: 11/25/08 [12:17]

Combined Status: All Profiles Are Functioning Correctly. Status Recipient: joe@example.com

Post Office Profiles	Status	Actions	Description
1. PO	MONNOV24		po1 profile

Domain Profiles	Status	Actions	Description
1. DOM	MONNOV24		domain profile

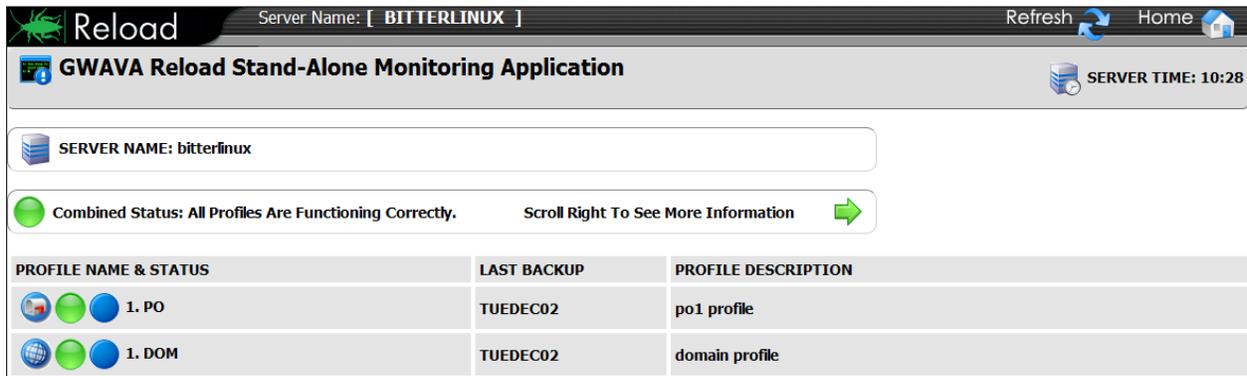
Widescreen Window

Profile Monitor

The Profile Monitor is a new feature only displaying information on the profiles without any active buttons or need to login to Web Administration. This allows the user to secure the login and have a timeout for the interface, while having a permanent monitoring window available to show the status of the system. This window will not close or timeout, and will actively poll for data twice a minute to show the status of your Reload system.

When you select the Profile Monitor button, a new window or tab will be spawned that contains the Profile Monitor.

The Profile Monitor window has information organized into long rows. How many profiles you have determines how many rows are displayed. Each profile occupies one row. Because the Rows are long, you must scroll to the side to see all the information available.



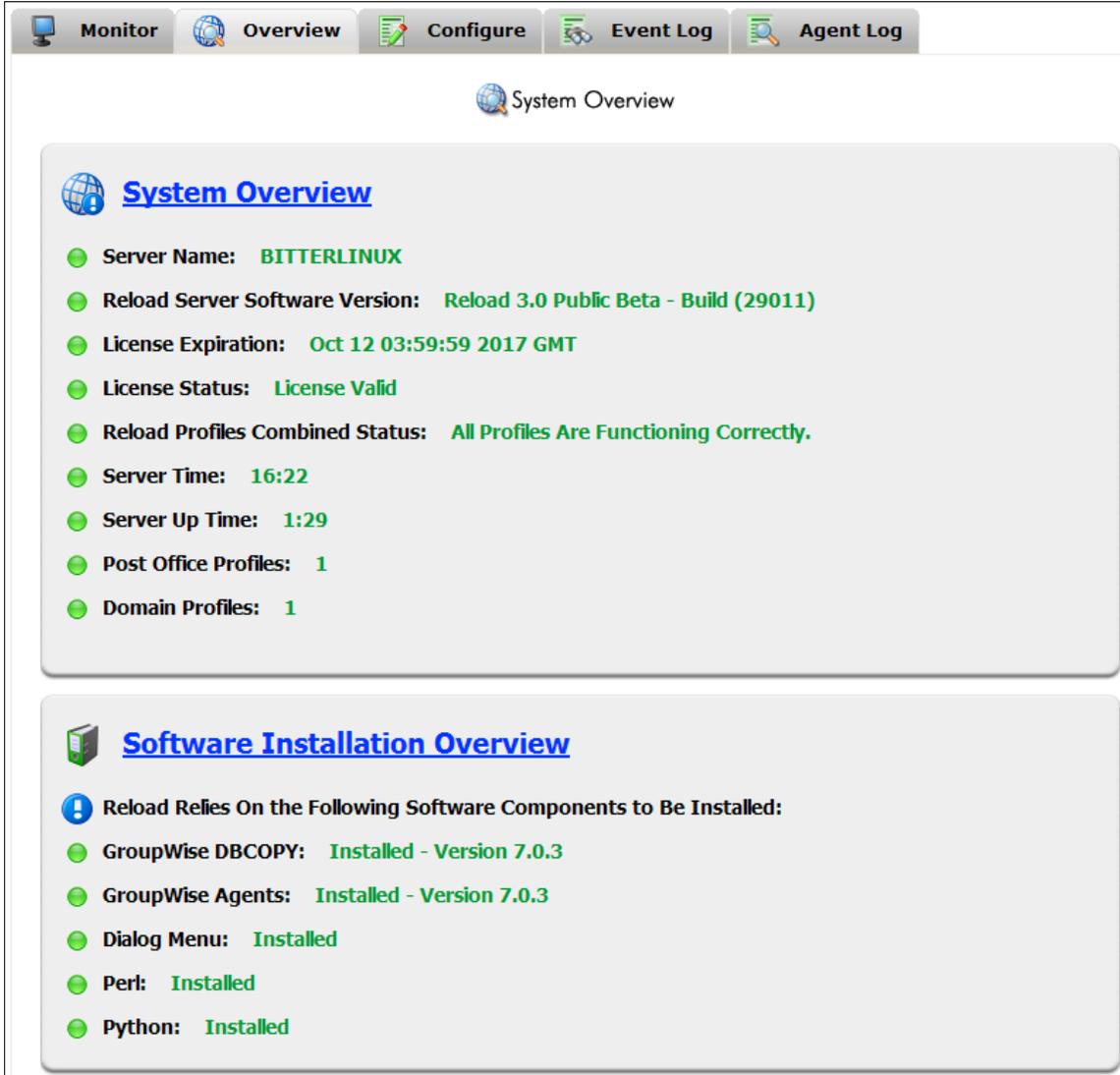
PROFILE NAME & STATUS	LAST BACKUP	PROFILE DESCRIPTION
 1. PO	TUEDEC02	po1 profile
 1. DOM	TUEDEC02	domain profile

The Profile Monitor contains all the profile information that the Web Administration home screen contains, and is an excellent way to monitor your Reload system throughout the day without having to worry about a session timing out or authenticating.

Overview

The overview tab provides information on the settings and installed software for your Reload server.

If the System Overview or the Software Installation Overview sections are not expanded, clicking on the name will expand or collapse the section for viewing. The Overview tab is very useful for viewing when checking for the versions of software are installed and active in the system.



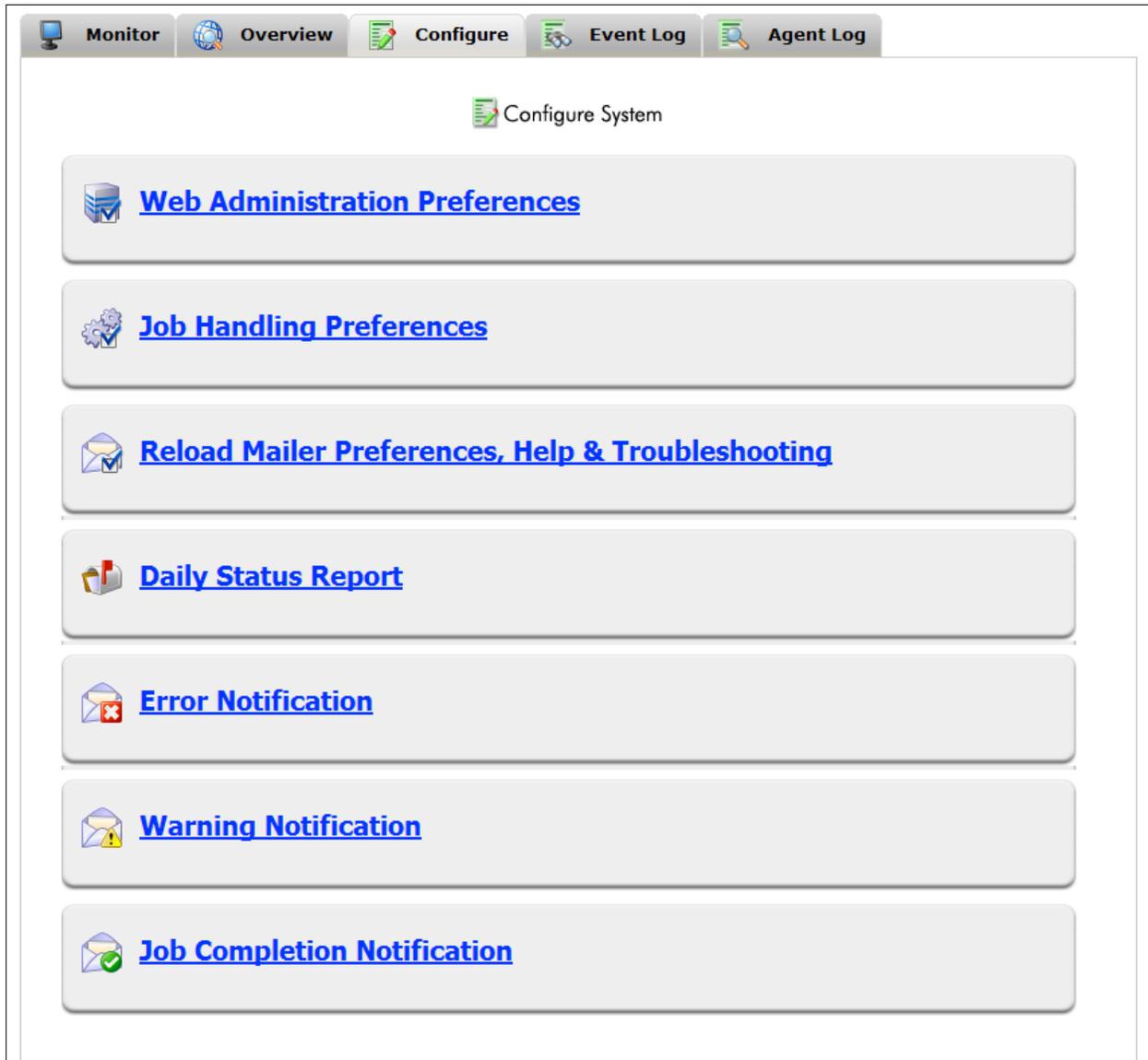
The screenshot displays the 'Overview' tab of a Reload server interface. At the top, there is a navigation bar with five tabs: 'Monitor', 'Overview' (selected), 'Configure', 'Event Log', and 'Agent Log'. Below the navigation bar, the main content area is titled 'System Overview'. It contains two main sections:

- System Overview**: A section with a globe icon containing the following information:
 - Server Name: BITTERLINUX
 - Reload Server Software Version: Reload 3.0 Public Beta - Build (29011)
 - License Expiration: Oct 12 03:59:59 2017 GMT
 - License Status: License Valid
 - Reload Profiles Combined Status: All Profiles Are Functioning Correctly.
 - Server Time: 16:22
 - Server Up Time: 1:29
 - Post Office Profiles: 1
 - Domain Profiles: 1
- Software Installation Overview**: A section with a software box icon containing the following information:
 - Reload Relies On the Following Software Components to Be Installed:
 - GroupWise DBCOPY: Installed - Version 7.0.3
 - GroupWise Agents: Installed - Version 7.0.3
 - Dialog Menu: Installed
 - Perl: Installed
 - Python: Installed

This section is an information display only, with no menus or actions available.

Configure

The Configure tab allows you to edit non-essential Reload settings and the look and feel of Web Administration. Each section can collapse or expand, and carries its own specific options. They are explained below.



The screenshot displays the 'Configure System' interface. At the top, there is a navigation bar with five tabs: 'Monitor', 'Overview', 'Configure', 'Event Log', and 'Agent Log'. The 'Configure' tab is currently selected. Below the navigation bar, the main content area is titled 'Configure System'. It contains seven configuration options, each represented by a button with an icon and a text label:

-  [Web Administration Preferences](#)
-  [Job Handling Preferences](#)
-  [Reload Mailer Preferences, Help & Troubleshooting](#)
-  [Daily Status Report](#)
-  [Error Notification](#)
-  [Warning Notification](#)
-  [Job Completion Notification](#)

Reload Web Administration Preferences

Web Administration allows you to modify how Web Administration acts and is displayed. Most settings are self explanatory, though some do deserve note.

If you enable web administration authentication, the browser will require you to login to monitor the system. You may use the system monitor page without logging in to allow monitoring with no timeout while still requiring authentication.

The Disaster Recovery Plan document URL is the document that is linked to the green Disaster Recovery Plan button always at the top of Web Administration. This is simply a document for download which details what to do in the event of a 'disaster' such as a data loss, disk failure, or system unavailability. The placeholder is located at `/opt/beginfinite/reload/web/custom/drplan/drplan.pdf`. Place your customized plan in the same directory on the Reload server, and change the name, or replace the current `drplan.pdf`. You may use any file format you desire.

Web Administration Preferences

- ! Reload Web Administration Can Load The Home Page You Prefer
- Default to the Reload Web Administration Widescreen Window **Disabled**
- Reload Web Administration HTTP Port: **5555**
- HTTPS/SSL Web Administration: **Disabled**
- Reload Web Administration Authentication: **Disabled**
- Reload Web Administration User Name: *********
- Reload Web Administration Authentication Password: *********
- Disaster Recovery Plan Document URL: **http://192.168.0.101:5555/custom/drplan/drplan.pdf**

Job Handling Preferences

Job Handling allows you to specify if the Reload server is allowed to run more than one job simultaneously. This can improve performance only when the Reload Server and the host network have unused resource potential during a currently running Reload job. Running more than one job simultaneously may adversely affect performance on all but high-end systems and networks. Jobs will only run concurrently if the scheduled start times overlap any other running job. You may specify how many simultaneous jobs will be allowed and enable or disable the feature.

 **Job Handling Preferences**
 **Help Understanding What These Settings Do**
 **Allow Concurrent Standard Backup Jobs:** **Enabled**
 **Number of Concurrent Standard Backup Jobs Allowed:** **2**

Reload Mailer Preferences, Help & Troubleshooting

The Reload Mailer uses Postfix to send mail. Postfix must be running and configured for notifications to work correctly. This information is located under the 'Read Help' buttons.

Under this section, you may embed and configure a direct link to the Reload server web page in every notification message sent by the Reload server. For example, if you wish to put a link to the Profile Monitor page in the email, your link would look similar to this:

<http://192.168.0.101:5555/status.gt>

Except your Reload server ip address or host name would be referenced.

The rest of the notifications are configured in the next few sections.

 **Reload Mailer Preferences, Help & Troubleshooting**
 **Reload Can Send E-mailed Reports and Notifications**
 **Help Understanding What The Reload Mailer Settings Do**
 **Reload and Postfix Mailer Troubleshooting and Customization**
 **Reload Can Embed The Reload Server URL in All Mail Messages Sent by Reload**
 **Embed Reload Server URL in All Mail Messages** **Disabled**
 **Reload Server URL:** <http://reload.example.com>

Daily Status Report

Reload can send a daily status report at the given time and on the given schedule to the recipient of your choice. You can send the status report to any recipient and may also send to a CC recipient. Specify them here.

 **Daily Status Report**

- ! Reload Can Send a Daily Consolidated Status Report of All Reload Profiles
 - ▶ Send The Status Report Message Now
 - ⊖ Send a Daily Consolidated Status Report E-mail: Disabled
 - ⊖ Include Reload System Event Log: Disabled
 - ⊖ Daily Status Report FROM Address: joe@example.com
 - ⊖ Daily Status Report TO Recipient: joe@example.com
 - ⊖ Send Status Report to a CC Recipient: Disabled
 - ⊖ Daily Status Report CC Recipient: joe@example.com

Error Notification

Error notification sends a warning notification when errors occur in the system. With the error notification enabled, a warning message will be sent to the address specified in the settings.

Notifications are sent on the following events:

- Failed job
- Disk space threshold exceeded
- A Profile becomes disabled
- The latest backup for a profile is too old and exceeds the age threshold

Error thresholds are configured under each profile's preferences menu.



The screenshot shows a settings panel titled "Error Notification" with an envelope icon. It contains several configuration options, each with a blue circular icon and an "Edit" button:

- Reload Can Send E-mail Notification of Error Conditions** (indicated by a blue exclamation mark icon)
- Send A Test Error Message** with a "Send" button
- Send E-mail Notification of Error Conditions:** Disabled (with an "Edit" button)
- Include Reload Support Log:** Disabled (with an "Edit" button)
- Error Notification FROM Address:** joe@example.com (with an "Edit" button)
- Error Notification TO Recipient:** joe@example.com (with an "Edit" button)
- Send Error Notifications to a CC Recipient:** Disabled (with an "Edit" button)
- Error Notification CC Recipient:** joe@example.com (with an "Edit" button)

Warning Notification

The warning notification works the same as the error notification, and for the same events, but is set to a different threshold, the warning threshold, set in Reload Administration under each profile's preferences menu.

 **Warning Notification**

! Reload Can Send E-mail Notification of Warning Conditions

- ▶ Send A Test Warning Message
- ⊕ Send E-mail Notification of Warning Conditions: Disabled
- ⊕ Include Reload System Event Log: Disabled
- ⊕ Warning Notification FROM Address: joe@example.com
- ⊕ Warning Notification TO Recipient: joe@example.com
- ⊕ Send Warning Notifications to a CC Recipient: Disabled
- ⊕ Warning Notification CC Recipient: joe@example.com

Job Completion Notification

Reload can send a notification after each job is completed. The completion notification works the same way as the previous notifications, but is triggered when a job is completed.

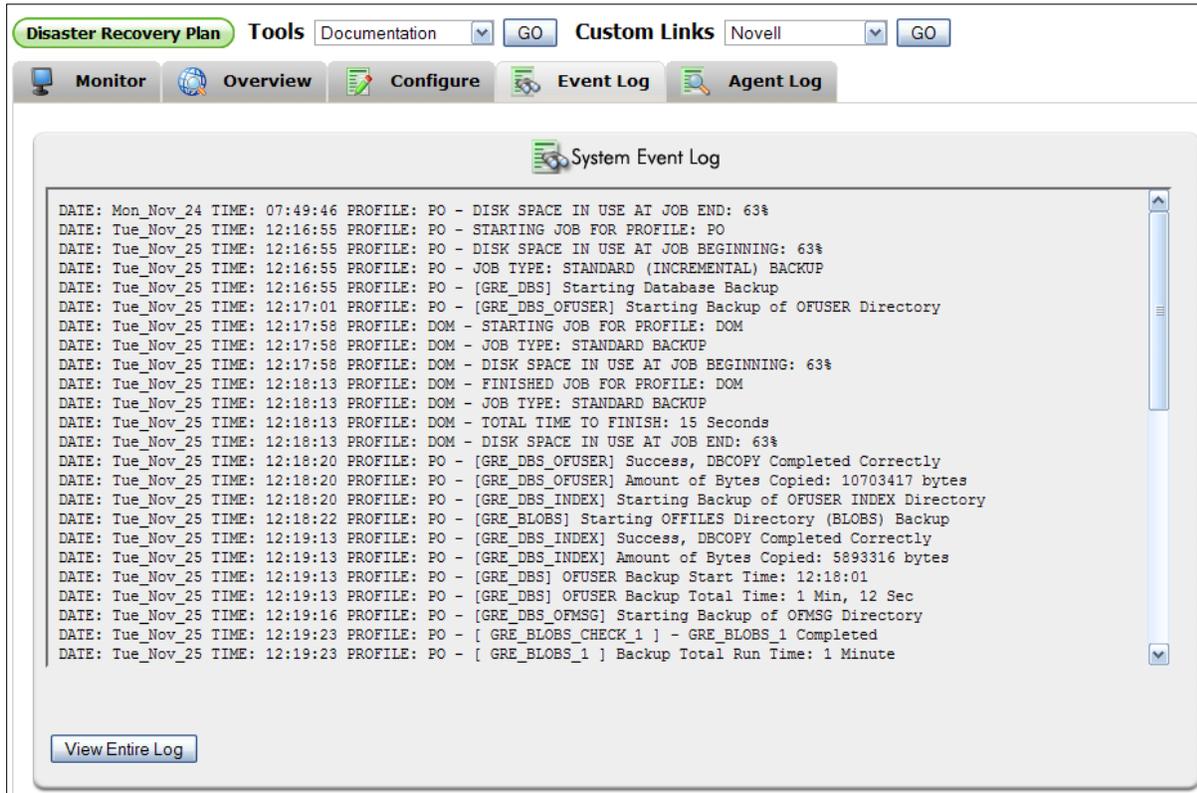
 **Job Completion Notification**

! Reload Can Send a Completion Message After Each Reload Job

- ▶ Send A Test Completion Message
- ⊕ Send Job Completion E-mail Notifications: Disabled
- ⊕ Include Reload System Event Log: Disabled
- ⊕ Completion Notification FROM Address: joe@example.com
- ⊕ Completion Notification TO Recipient: joe@example.com
- ⊕ Send Job Completion Notifications to a CC Recipient: Disabled
- ⊕ Completion Notification CC Recipient: joe@example.com

Event Log

The system event log contains all information on the Reload system actions. It is displayed here for convenience. The display here has a rolling cache that refreshed with the latest information. To view the entire log from this location, select the 'View Entire Log' button at the bottom of the screen. When selected, the entire log will be opened in a separate window or tab of your browser.



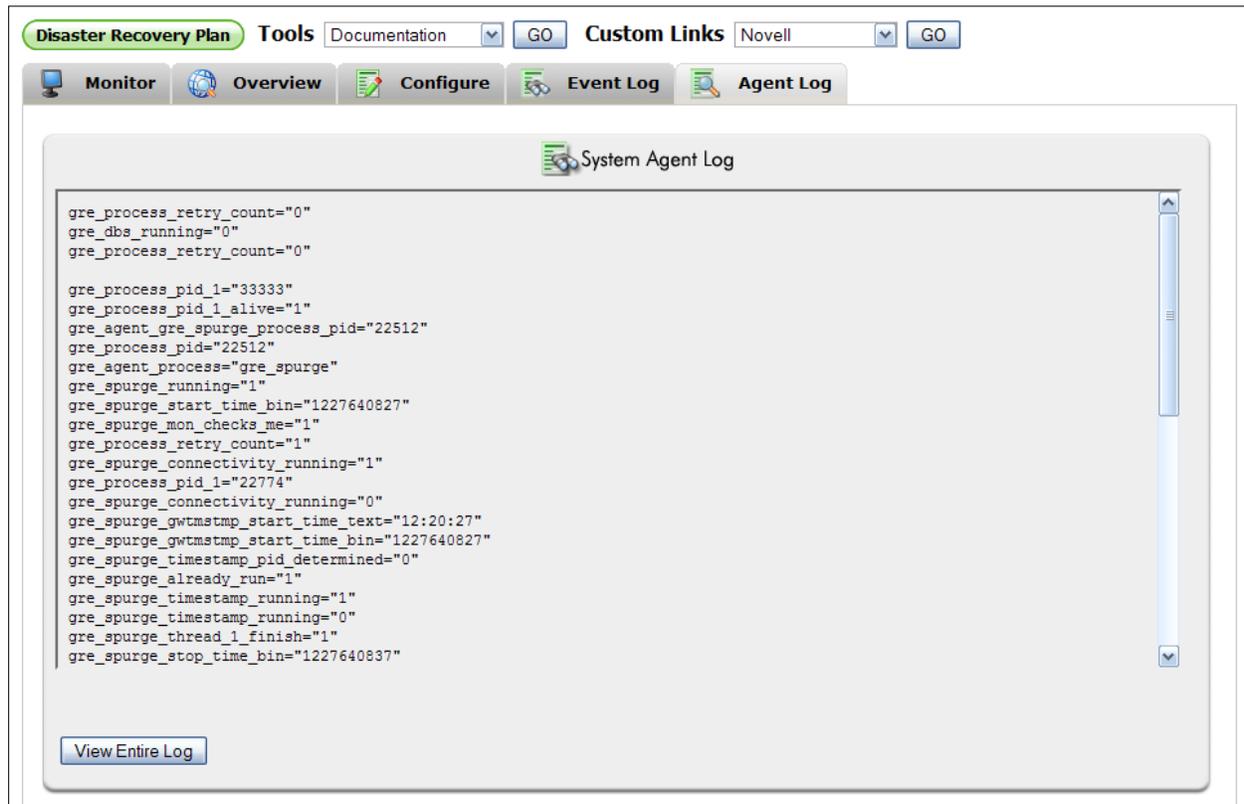
The screenshot shows a web-based interface for monitoring system events. At the top, there is a navigation bar with tabs for 'Monitor', 'Overview', 'Configure', 'Event Log', and 'Agent Log'. The 'Event Log' tab is currently selected. Below the navigation bar, there is a 'System Event Log' section with a scrollable text area containing the following log entries:

```
DATE: Mon_Nov_24 TIME: 07:49:46 PROFILE: PO - DISK SPACE IN USE AT JOB END: 63%
DATE: Tue_Nov_25 TIME: 12:16:55 PROFILE: PO - STARTING JOB FOR PROFILE: PO
DATE: Tue_Nov_25 TIME: 12:16:55 PROFILE: PO - DISK SPACE IN USE AT JOB BEGINNING: 63%
DATE: Tue_Nov_25 TIME: 12:16:55 PROFILE: PO - JOB TYPE: STANDARD (INCREMENTAL) BACKUP
DATE: Tue_Nov_25 TIME: 12:16:55 PROFILE: PO - [GRE_DBS] Starting Database Backup
DATE: Tue_Nov_25 TIME: 12:17:01 PROFILE: PO - [GRE_DBS_OFUSER] Starting Backup of OFUSER Directory
DATE: Tue_Nov_25 TIME: 12:17:58 PROFILE: DOM - STARTING JOB FOR PROFILE: DOM
DATE: Tue_Nov_25 TIME: 12:17:58 PROFILE: DOM - JOB TYPE: STANDARD BACKUP
DATE: Tue_Nov_25 TIME: 12:17:58 PROFILE: DOM - DISK SPACE IN USE AT JOB BEGINNING: 63%
DATE: Tue_Nov_25 TIME: 12:18:13 PROFILE: DOM - FINISHED JOB FOR PROFILE: DOM
DATE: Tue_Nov_25 TIME: 12:18:13 PROFILE: DOM - JOB TYPE: STANDARD BACKUP
DATE: Tue_Nov_25 TIME: 12:18:13 PROFILE: DOM - TOTAL TIME TO FINISH: 15 Seconds
DATE: Tue_Nov_25 TIME: 12:18:13 PROFILE: DOM - DISK SPACE IN USE AT JOB END: 63%
DATE: Tue_Nov_25 TIME: 12:18:20 PROFILE: PO - [GRE_DBS_OFUSER] Success, DBCOPY Completed Correctly
DATE: Tue_Nov_25 TIME: 12:18:20 PROFILE: PO - [GRE_DBS_OFUSER] Amount of Bytes Copied: 10703417 bytes
DATE: Tue_Nov_25 TIME: 12:18:20 PROFILE: PO - [GRE_DBS_INDEX] Starting Backup of OFUSER INDEX Directory
DATE: Tue_Nov_25 TIME: 12:18:22 PROFILE: PO - [GRE_BLOBS] Starting OFFFILES Directory (BLOBS) Backup
DATE: Tue_Nov_25 TIME: 12:19:13 PROFILE: PO - [GRE_DBS_INDEX] Success, DBCOPY Completed Correctly
DATE: Tue_Nov_25 TIME: 12:19:13 PROFILE: PO - [GRE_DBS_INDEX] Amount of Bytes Copied: 5893316 bytes
DATE: Tue_Nov_25 TIME: 12:19:13 PROFILE: PO - [GRE_DBS] OFUSER Backup Start Time: 12:18:01
DATE: Tue_Nov_25 TIME: 12:19:13 PROFILE: PO - [GRE_DBS] OFUSER Backup Total Time: 1 Min, 12 Sec
DATE: Tue_Nov_25 TIME: 12:19:16 PROFILE: PO - [GRE_DBS_OFMSG] Starting Backup of OFMSG Directory
DATE: Tue_Nov_25 TIME: 12:19:23 PROFILE: PO - [ GRE_BLOBS_CHECK_1 ] - GRE_BLOBS_1 Completed
DATE: Tue_Nov_25 TIME: 12:19:23 PROFILE: PO - [ GRE_BLOBS_1 ] Backup Total Run Time: 1 Minute
```

At the bottom of the log area, there is a button labeled 'View Entire Log'.

Agent Log

The agent log records all the actions of the Reload agent. The agent log tab displays a rolling cache of the Reload system agent log, which refreshes to show the latest information at the end of the log. If you wish to see the entire log, select the 'View Entire Log' button at the bottom of the window. When selected, the entire Agent Log is opened in a new window or tab of your browser.



The screenshot displays a web-based interface for monitoring system agent logs. At the top, there are navigation tabs: 'Monitor', 'Overview', 'Configure', 'Event Log', and 'Agent Log'. The 'Agent Log' tab is active, showing a window titled 'System Agent Log'. The log content consists of key-value pairs representing system state, such as process IDs, running status, and timestamps. A 'View Entire Log' button is located at the bottom left of the log window.

```
gre_process_retry_count="0"
gre_dbs_running="0"
gre_process_retry_count="0"

gre_process_pid_1="33333"
gre_process_pid_1_alive="1"
gre_agent_gre_spurge_process_pid="22512"
gre_process_pid="22512"
gre_agent_process="gre_spurge"
gre_spurge_running="1"
gre_spurge_start_time_bin="1227640827"
gre_spurge_mon_checks_me="1"
gre_process_retry_count="1"
gre_spurge_connectivity_running="1"
gre_process_pid_1="22774"
gre_spurge_connectivity_running="0"
gre_spurge_gwtmstp_start_time_text="12:20:27"
gre_spurge_gwtmstp_start_time_bin="1227640827"
gre_spurge_timestamp_pid_determined="0"
gre_spurge_already_run="1"
gre_spurge_timestamp_running="1"
gre_spurge_timestamp_running="0"
gre_spurge_thread_1_finish="1"
gre_spurge_stop_time_bin="1227640837"
```

[View Entire Log](#)

Profile page

To enter the profile page, you may either select the desired profile from the home page, or from the tree menu on the left. The two types of profiles, post office and domain, both have very similar pages. The difference is in the access to the backups. Domain profiles allow access to backups as a downloadable zipped file of the actual domain database, where the Post Office access to backups allows a post office agent to connect to the backup of the database to retrieve requested items for a Group Wise Client.

All changes to a profile are completed through the Reload Console Administration.

The profile page for a post office profile, shown below, provides detailed information about the individual profile not found on the status home page. The different tabs are explained.

PO - po
Normal - No backup is loaded

Overview Access Backups Disaster Recovery Event Log Agent Log

[Profile Information](#)

[Latest Backup Status Information](#)

[Reload Profile Configuration Summary](#)

[Disaster Recovery Configuration Summary](#)

[Hot Backup Configuration Summary](#)

[Tape Backup Enhancement Configuration Summary](#)

[Preferences Configuration Summary](#)

[Start a Backup Job](#)

Overview

The Overview page holds seven items:

- Profile Information
- Latest Backup Status Information
- Reload Profile Configuration Summary
- Disaster Recovery Configuration Summary
- Hot Backup Configuration Summary
- Preferences Configuration Summary
- Start a backup Job.

Of all the items on the Overview page, the only item with links to a system action is the last, start a backup job, which allows you to initiate a backup job for this specific profile.

Profile Information

Basic information about the functioning status of the profile is listed here.

 **Profile Information**

- **Profile Name:** PO
- **Profile Description:** po1 profile
- **Profile Status:** This profile is functioning correctly.
- **Disaster Recovery Testing:** Incomplete
- **Profile Path:** /data/po
- **Live Post Office Platform:** Local Post Office on Reload Server

The Profile data path and the platform of the target Post Office are notable here as different from the initial home page. Also, and most importantly, the Disaster Recovery Testing is also new. This item will only show 'Incomplete' until you have tested your disaster recovery post office by initiating a failover. **It is vitally important to test your disaster recovery plan before it is required.** Port and ip address conflicts all can be avoided before a disaster strikes to avoid needless anxiety in the event of a system failure. Setup your disaster recovery plan and test it. The Disaster recovery plan is configured through Reload Console Administration.

Latest Backup Status Information

This item provides useful information about the performance of your Reload system, and helps keep track of the latest backup of a post office or Domain Database.



Latest Backup Status Information

- **Name of Latest Backup:** THUDEC04
- **Time to Complete The Latest Backup:** 3 Minutes 47 Seconds
- **Average Time to Complete Backups:** 3 Minutes 53 Seconds
- **Backup Completion Date and Time:** Thu Dec 4 08:57:02 MST 2008

Reload Profile Configuration Summary

The Profile Configuration Summary shows which backup solution is currently configured for use with this profile. The six different backup options are listed, along with their active status.



Reload Profile Configuration Summary

- ! **Reload can provide six primary solutions for a post office profile:**
- 1. **Push-Button Disaster Recovery:** Enabled
- 2. **Hot Backups:** Enabled
- 3. **Quick Restore:** Enabled
- 4. **Tape Backup Enhancement:** Disabled
- 5. **GWAVA Retain Integration:** Disabled
- 6. **GWAVA Vertigo Integration:** Disabled

Disaster Recovery Configuration Summary

Other than actually creating backups, disaster recovery is the most important section and function of Reload. This item displays the status of your disaster recovery configuration. The disaster recovery testing item will be removed from the list when you have activated a failover, at least once, for this profile.

 **Disaster Recovery Configuration Summary**

 When the Disaster Recovery Failover option is enabled for this profile, this is what will happen:

-  Disaster Recovery Testing: **Incomplete**
-  Change to Disaster Recovery Mode and Disable Backups for This Profile: **Enabled**
-  Remove all Queued Backup Jobs for This Profile: **Enabled**
-  Run a Custom Command Before Loading The Disaster Recovery GroupWise POA: **Disabled**
-  Turn off Access Mode and Restore Mode POAs: **Disabled**
-  Load the Disaster Recovery GroupWise POA for This Profile: **Enabled**
-  Disaster Recovery GroupWise POA TCP/IP Address:
-  Disaster Recovery GroupWise POA TCP/IP Client/Server Port:
-  Run a Custom Command After Loading The Disaster Recovery GroupWise POA: **Disabled**
-  Monitor and Restart the Disaster Recover POA if it Stops: **Enabled**

All pertinent options for the automated disaster recovery are listed here. Ensure that this section shows all settings as you desire them before testing your disaster recovery plan. Test to make sure that there are no port or ip address conflicts in your system or network.

Hot Backup Configuration Summary

This item displays the settings which are active for this profile. Smart Purge requires settings in Console One, and the Reload configuration is accomplished through the Reload Console Administration.



Hot Backup Configuration Summary

- Backup Consistency/Quality:** Highest
- GroupWise SmartPurge Integration:** Enabled
- Number of Portable (Full/Weekly) Backups to Keep:** 2
- Backup DMS Libraries at Post Office:** Disabled

Tape Backup Enhancement Configuration Summary

This menu option displays the tape backup settings configured through the Reload Administration Console for the selected profile. Default is shown. This is a summary only and the values shown here are not configurable via Web Administration.



Tape Backup Enhancement Configuration Summary

- Tape Archive Storage Path:**
- Expire Old Tape Archive Files:** Enabled
- Build TAR File Before Moving to TAR Path:** Enabled
- Perform Customized Pre-TAR Command:** Disabled
- Perform Customized Post-TAR Command:** Disabled

Preferences Configuration Summary

The warning and error threshold settings are displayed here for disk space and backup age. These are the two most critical thresholds for your system. Ensure that they are set correctly to allow enough time to fix a problem before it affects the consistency of your backup plan.

 **Preferences Configuration Summary**
 **Preferences affect disk space thresholds, and monitoring and alerting thresholds**

-  **Disk Space Error Threshold Percentage: 90%**
-  **Disk Space Warning Threshold Percentage: 85%**
-  **Monitor Profile Enabled Status: Enabled**
-  **Backup Age Warning Threshold: 48 Hours**
-  **Backup Age Error Threshold: 72 Hours**

Start a Backup Job

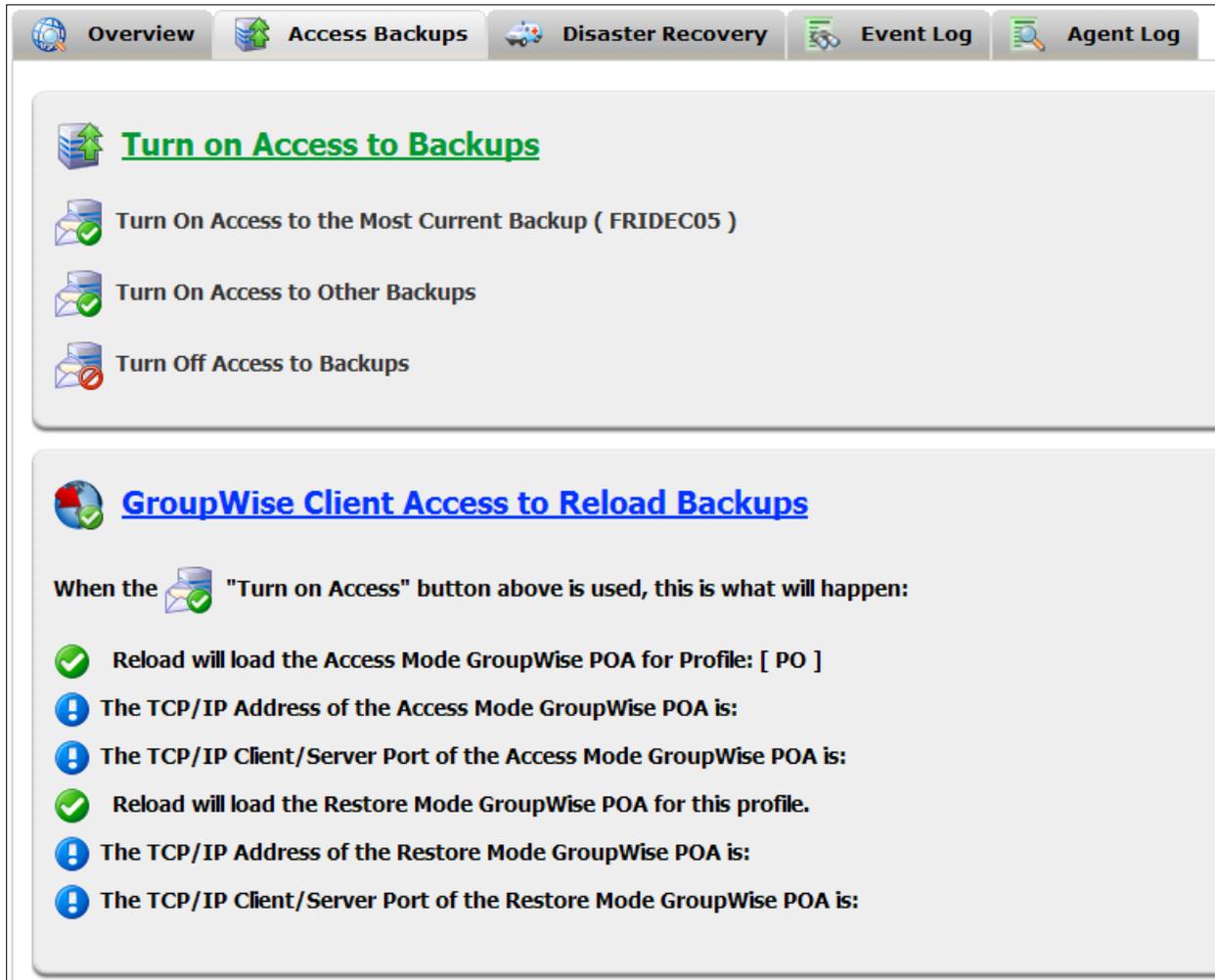
This section allows you to start a backup job. Post Office Profiles allow you to start a job without SmartPurge, as well as a standard job. The Domain does not have SmartPurge as the Domain does not actively contain mail. Only the option to initiate a standard backup job is available for the Domain Profile.

 **Start a Backup Job**

-  **Start a Standard Backup Job (SmartPurge Disabled)**
-  **Start a Standard Backup Job**

Access Backups

The Access Backups tab is where the main difference between the Post office profiles and the Domain profiles. The Post Office backups can be configured to allow access to the backed up post office by the GroupWise client. You may turn on access to the post office backup here, but it is configured in the Reload Console Administration. Before turning on access, check the settings to ensure that they are set correctly.



Turn on Access to Backups

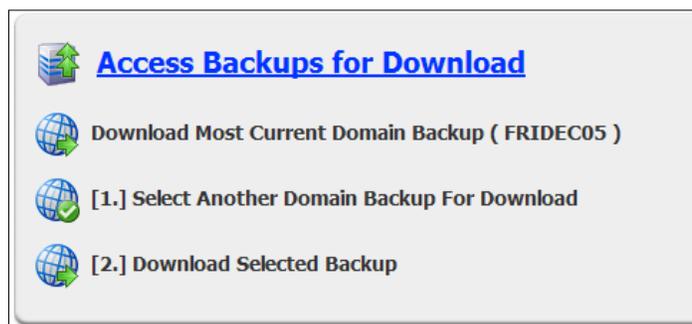
- Turn On Access to the Most Current Backup (FRIDEC05)
- Turn On Access to Other Backups
- Turn Off Access to Backups

GroupWise Client Access to Reload Backups

When the "Turn on Access" button above is used, this is what will happen:

- Reload will load the Access Mode GroupWise POA for Profile: [PO]
- The TCP/IP Address of the Access Mode GroupWise POA is:
- The TCP/IP Client/Server Port of the Access Mode GroupWise POA is:
- Reload will load the Restore Mode GroupWise POA for this profile.
- The TCP/IP Address of the Restore Mode GroupWise POA is:
- The TCP/IP Client/Server Port of the Restore Mode GroupWise POA is:

The Domain Access Backups works a little differently. Because there is no mail in the Domain databases that can be available to the client, the Domain database is simply offered as a zipped download. Select the appropriate domain and download the database if you wish access.



Access Backups for Download

- Download Most Current Domain Backup (FRIDEC05)
- [1.] Select Another Domain Backup For Download
- [2.] Download Selected Backup

Disaster Recovery

This tab allows the management of the Disaster Recovery process for either the Domain or the Post Office profiles. The Disaster Recovery steps are listed in order under the 'Push-Button Disaster Recovery' section.

Push-Button Disaster Recovery

**Push-Button Disaster Recovery**

-  1. [FAILOVER] - Enable Disaster Recovery Mode Using Current Backup (FRIDEC05)
-  2. [MIGRATE] - Migrate Post Office Contents Back to a Production Server
-  3. [FAILBACK] - Disable Disaster Recovery Mode And Return to Normal

You first enable the 'Failover', to keep your system running when the live Post Office is down. This loads a POA or a MTA against the latest Post Office or Domain backup, filling the gap in the system left by the missing live POA or MTA.

Once the live system is ready to have the backup data, if you so wish, returned to the live system, you enable the 'Migrate' function to copy the database files from the running Reload POA or MTA, back to the live server.

Once the live server is back to full operational status, you select 'Failback', which returns the Reload System back to normal functions, resuming the backup schedule.

Current automated disaster Recovery Plan

**Current Automated Disaster Recovery Plan**

When the  1. [FAILOVER] button above is pushed for this profile, this is what will happen:

-  This Profile will be Changed to Disaster Recovery Mode
-  Backups for This Profile will be Disabled While the Profile is in Disaster Recovery Mode
-  All Queued Backup Jobs for This Profile Will be Removed From the Job Queue
-  The Disaster Recovery GroupWise POA for This Profile Will be Loaded Against the Most Current Backup
-  The TCP/IP Address of the Disaster Recovery GroupWise POA is:
-  The TCP/IP Client/Server Port of the Disaster Recovery GroupWise POA is:
-  Reload Will Monitor and Restart the Disaster Recover POA if it Stops

The settings and process of what a Disaster Recovery POA or MTA are listed under this item. Settings that need attention or need to be filled-out will have an exclamation next to them. You should have this dialog filled-out before there is a need for disaster recovery. Configure and test the disaster recovery function of Reload by filling out the settings in the Reload Administration, and initiating the Disaster Recovery Failover for the Profile.

Additional Steps That May Need to be Taken

Even though the Disaster POA or MTA is up and running well, there are steps that the automated disaster recovery cannot take. These are listed under the 'additional steps that may need to be taken' section. These steps will be different and may or may not be necessary depending on your system, and differ in wording for the Domain and the Post Office. Read and review both.

This section should be represented heavily in your customized Disaster Recovery Plan. Any additional steps that should be taken for your system beyond the automated disaster recovery should be listed in detail in your disaster recovery plan. Review these questions and add them to your plan as appropriate.

 **Additional Steps That May Need to be Taken**

If a production post office is now running on the Reload Server, consider the following:

-  Make sure the GroupWise MTA for the Domain that owns the post office that this profile represents knows about the new TCP/IP Address of the Disaster Recovery POA. This can be as simple as editing the GroupWise POA object in ConsoleOne, and changing the TCP/IP address to reflect the TCP/IP Address of the Disaster Recovery POA on the Reload server.
-  If the POA for the GroupWise Post Office that is now hosted on the Reload server is registered in DNS, are changes needed?
-  If GroupWise WebAccess is used, change the post office link to reflect the correct TCP/IP address of the post office that is now hosted on the Reload server.
-  If the GWIA is providing POP3 or IMAP client connections, change the post office link to reflect the correct TCP/IP address of the post office that is now hosted on the Reload server.
-  Are there other services, such as BlackBerry Enterprise Server for example, that need to know about the new TCP/IP address of the post office that is now hosted on the Reload server?

When the Disaster Recovery Post Office or Domain are hosted on the Reload server, they will be reached on a different address in the network than the live POA or MTA was located at. For your system to function correctly with the Reload agents, the rest of the GroupWise and mail system must be informed of the change.

Once the rest of the system has been informed, there will be plenty of time to sort out the live system and resolve any problems there.

Event Log

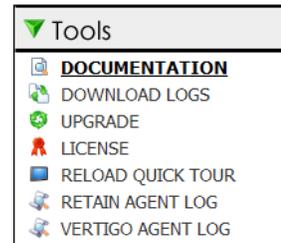
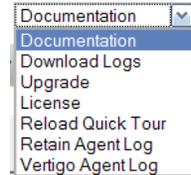
The Event Log is a rolling cache of the Profile Event Log which shows all actions associated with this profile. The log shown is the last few lines of the latest information. If you wish to view the entire log, select the 'View Entire Log' button and the log will be displayed in a new window or tab.

Agent Log

The Agent Log, like the Event Log, is a rolling cache of the Profile Agent Log which shows all actions associated with this profile. The log shown is the last few lines of the latest information. If you wish to view the entire log, select the 'View Entire Log' button and the log will be displayed in a new window or tab.

Tools menu

The Tools menu, located either at the top of the home page as a dropdown menu, or always on the navigation window, on the left of the page as a tree menu, contains valuable information and tools for your system. All the links and tools work with no further configuration except the Retain and Vertigo agent logs, which must be configured to point to the Retain or Vertigo system.



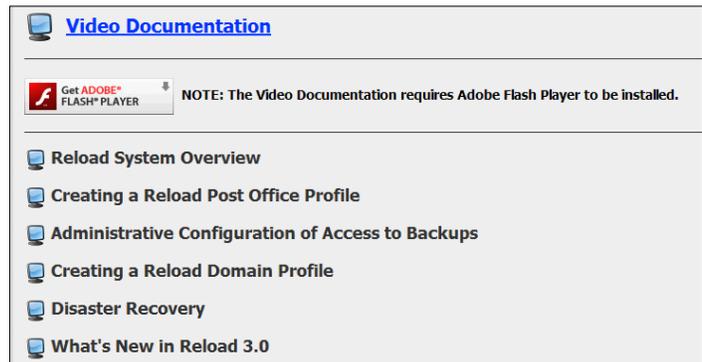
Documentation

Online documentation is easily accessible through this link. Reload comes with Video documentation, the entire guide available for download, and links to the online Reload knowledgebase and consulting resources.

The Video Documentation requires Adobe Flash Player and has step by step information that will guide you through your Reload system on the following topics:

- Reload System Overview
- Creating a Reload Post Office Profile
- Administrative configuration of Access to Backups
- Creating a Reload Domain Profile
- Disaster Recovery
- What's new in Reload 3.0

All videos are helpful and recommended to help you be accustomed to, and comfortable with your Reload System.



Download Logs

When troubleshooting, working with Reload Support, or simply monitoring the processes of Reload, the logs are invaluable. The Reload Support log can be downloaded from this section in a compressed or uncompressed form. The Reload Support Log is a plain text file, but to ensure that your browser downloads the file instead of displaying it, the file has been given the suffix .lug. This can be opened with any text editor, but it is recommended to view the file using WordPad instead of Notepad on Windows workstations.

Upgrade

Upgrading your system just became much easier with the upgrade tool. The upgrade tool offers two ways to upgrade your Reload system.

Automated Software Download and Automated Upgrade requires HTTP access to the internet on port 80 to function, but simply requires a click on the 'upgrade now' button, and your Reload system will automatically check, download, and install the latest full release version of Reload. You will be prompted to exit all administrative instances you have open, to allow the Reload Daemon to restart after the upgrade is complete.

The automated upgrade section also displays the currently installed version and links to Reload Forums to allow you to check the latest released version.

Manual Software Download and Automated Upgrade requires you to manually download the latest Reload release, and then place it in the /opt/beginfinite/reload/upgrade folder on the Reload Server. After the install file has been placed in the correct folder, select the 'Upgrade Now' button which checks for newer versions in that folder. When Reload finds the newer code, it will automatically upgrade the system to the updated build.

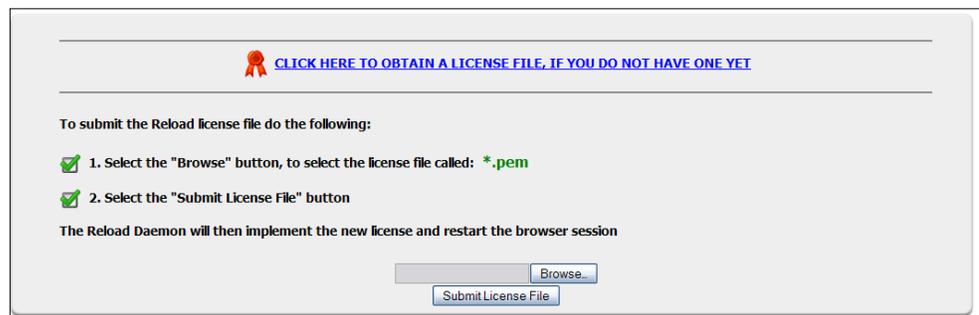
Advanced Upgrade Options

The advanced upgrade options require HTTP internet access on port 80. This option is for upgrading to field test code or a beta release. Simply selecting the 'Upgrade to Field Test code Now' option will initiate an upgrade. The same is true of the 'Roll Back Code Now' option, which checks for the latest full release code and installs that version of Reload on your server.

The last option allow you to update the Reload system to a specific release, beta or otherwise. If you wish to use this option, you must know the code name of the new beta build. This should only be selected in conjunction with, and under the instruction of GWAVA Reload Support, who will give you the specific build name. Enter the build name in the provided field and select 'Submit' to upgrade to the specified build name.

License

Reload must be licensed to function, and Reload Web Administration allows you to upload your license to your Reload Server. You may obtain a trial license by following the link at the top. When you have your license, follow the instructions to browse to, and upload your license to the system. Reload will automatically recognize and accept the license after it has been uploaded to the server.



The screenshot shows a web interface for uploading a license file. At the top, there is a red ribbon icon and a blue link: [CLICK HERE TO OBTAIN A LICENSE FILE, IF YOU DO NOT HAVE ONE YET](#). Below this, the text reads: "To submit the Reload license file do the following:" followed by two numbered steps: "1. Select the 'Browse' button, to select the license file called: *.pem" and "2. Select the 'Submit License File' button". Below the steps, it says: "The Reload Daemon will then implement the new license and restart the browser session". At the bottom, there are two buttons: "Browse..." and "Submit License File".

Reload Quick Tour

The quick tour gives a basic slideshow-style overview of Reload and the solutions' it provides. Take the tour to better understand how Reload can work to improve the message infrastructure for your organization.

Understanding Reload's potential and function will help you plan how to implement Reload in your system to provide the best solution possible for your system setup.

Custom links

Reload comes with a set of preconfigured links to web pages inside the Reload Web Administration. Several convenient links are located here, including links to GWAVA Support, Novell, and Linux documentation.

You may also modify the custom links. There are 8 customizable links which can be configured from within Reload Administration by selecting System Web. Custom links might be designed to do one of the following:

- Create a link to another Reload server in your network
- Create a link to a disaster recovery document
- The Reload Daemon can serve up HTML pages and images that are located in the following directory: `/opt/beginfinite/reload/web/custom`

The URL to a page called index.htm in the custom directory would be similar to the following syntax:

`http://10.1.1.100:5555/custom/index.htm`

If the Reload Daemon cannot serve up a certain page, please do not contact GWAVA Technical support, as this is not an official feature of the product, but was included for convenience.

- Create a link to enable a VNC session (assuming you have VNC running). The way you might do this is make the link to be: `http://serveraddress:58<VNC PORT SPECIFIED>`
For example: <http://reload.gwava.com:5801>
- Create a second link to a profile that is already defined on the local reload server. Let's say you have a Domain profile on the Reload server, and you want to make a link to that Domain profile. This is how you could do it. If the Domain profile is the first profile listed then its actual link page is called "dprofile1.gt". So in the web link that you want to create for this profile, type in just the name of the file, which is: **dprofile1.gt**. The Reload Web Server will know to look for this file in its standard root documents directory that it uses by default, and will display the profile through the custom link that you create.

APPENDIX A

Restoring an Entire GroupWise Mailbox

Reload creates a method for assuring that backed up data in the recent past is quickly available. This is done through the "Access" menu in Reload Administration, or within Reload Mobile and also from Profiles section on the Reload Daemon HTTP Page. Within a matter of a couple of minutes, you can make backed up Reload data available to a user.

If a user's mailbox was completely deleted, they you will still need to restore the user, preferably with their original "FID". If you have the **Novell Press GroupWise 6.5 or GroupWise 7 Administrator's guide**, you will need to follow the steps in Chapter 28 relative to restoring the user in the GroupWise directory. Then you must access the user's mailbox through Reload and archive off the items and un-archive them as explained in Chapter 28.

Good news, if you do not have the Novell Press GroupWise Administrator's guide, Chapter 28 is on-line and downloadable at <http://www.taykratzer.com>

Appendix B

Reload and Post Offices That Use LDAP

Here is some guidance from the experience of one of the Reload customers that is using LDAP Authentication with GroupWise.

[PROBLEM]

We use LDAP authentication against a different tree for our "real" GroupWise users. Since LDAP cannot successfully compare a DN because the tree and contexts are different; it compares the email address instead. In Netware I always have to rename the ldapx.nlm to make this work, otherwise I get an LDAP 34 error on the PO when a user tries to login. Here is a link to the Novell tid in case you aren't familiar with the way we are using LDAP.

<http://support.novell.com/cgi-bin/search/searchtid.cgi?10067272.htm>

The problem is that I am seeing the same error when I try to login against the PO that Reload has created and I do not know how to fix it as I can obviously find no LDAP.NLM on the linux server.

[SOLUTION]

1. On the Linux server, open up a Terminal session
2. Make a directory for housing code that will be moved in a moment:
`mkdir /opt/novell/groupwise/agents/nldap.old`
2. Change to the /opt/novell/groupwise/agents/lib/nldap directory.
`cd /opt/novell/groupwise/agents/lib/nldap`
3. Move the following ldapx library with the following commands:
`mv libldapx.so /opt/novell/groupwise/agents/nldap.old`
`mv libldapx.so.0.0.0 /opt/novell/groupwise/agents/nldap.old`

Reload and Post Offices That Use LDAP and SSL

If a GroupWise post office is configured for LDAP and SSL is configured in conjunction with LDAP authentication, then you need to do the following:

- In ConsoleOne, do the following.
 - Highlight the GroupWise system object
 - Select Tools|GroupWise System Operations|LDAP Servers
 - Edit the LDAP server object that services the post office that is being backed up by Reload
 - Confirm the following:
 - The SSL Key file should be specified as follows:
 - Specify the keyfile name as a *.der file with a name that is all lowercase
 - Make sure that the path to the keyfile IS NOT SPECIFIED. All that should be in this field is the actual keyfile name. This will be a file with a *.der file extension
 - On your live production server that houses your GroupWise post office, make sure that the *.der file is in the program root directory. On a NetWare server this is: o sys:system - By default or – Wherever the GroupWise Agent software installed to on the live server (On a Linux server this is:
/opt/novell/groupwise/agents/bin)
 - Get the *.der file mentioned in the LDAP server definition in ConsoleOne, and place at the following path on the Reload server:
/opt/novell/groupwise/agents/bin

Appendix C

Configuring Redline Integration

GWAVA Redline can monitor your Reload Server(s). To enable this ability from within Reload Administration do the following:

- From the Main Menu, select **System | Integrations**.
- Enable the **Redline** integration.
- Make sure the Reload Daemon has HTTP monitoring enabled, as this is the way that the Redline Agent gets its information from Reload.

The Redline system also needs to be configured with the information needed to discover and monitor the Reload Server. Please consult the latest Redline documentation on how to do this.