



GroupWise Reporting and Monitoring 18 Install Guide

January 2020

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2020 Micro Focus Software, Inc. All Rights Reserved.

Contents

Overview	5
1 Release Notes	9
About New Features	9
About This Release	9
New Features	9
Bug Fixes and Enhancements	9
General Note	9
2 System Requirements	11
Control Center Requirements	11
Agent Requirements	12
3 Installation	13
Installing the Control Center on Linux	13
Installing the Control Center on Windows	14
Accessing Control Center	17
Installing the License	17
Installing the Agent on Linux	18
Installing the Agent on a Linux Cluster	18
Installing the Agent on Windows	19
Running Multiple GWRM Agents on Windows	20
Update GWRM	20
Uninstall GWRM	20
Windows	20
Linux	21
4 Configuring GroupWise Reporting and Monitoring	23
GroupWise Agents	23
GroupWise Post Office Agent (POA)	23
GroupWise Message Transfer Agent (MTA)	31
GroupWise Internet Agent (GWIA)	34
GroupWise Document Viewer Agent	39
GroupWise WebAccess Application	42
GroupWise Messenger Agents	46
GroupWise Messenger Messaging Agent	46
GroupWise Messenger Archive Agent	49
GroupWise Disaster Recovery	52
GroupWise Forensics	53
GroupWise Mailbox Management	54
Micro Focus Retain	55
GWAVA 6.5 and Secure Messaging Gateway	55

Advansys Archive2Go	55
Blackberry Enterprise Server	56
GroupWise Requirements	56

Overview

About GroupWise Reporting and Monitoring

GroupWise Reporting and Monitoring (GWRM) is a reporting and monitoring solution for Micro Focus GroupWise® that provides a Dashboard for quick access to the most critical areas of GroupWise®, a real time monitoring solution, and a System viewer that allows you to see all of the details of your GroupWise components in a single view. GroupWise Reporting and Monitoring produces reports for system analysis, capacity planning, and security auditing.

GWRM monitors system-critical modules and processes in the targeted mail and server environment, sends alerts, compiles statistical reports, and logs activity for informational analysis. GWRM provides a complete and comprehensive status picture and real time monitoring solution for the supported systems.

GWRM works to monitor systems with two different parts: the Agents, and the Control Center.

The Agents gather the information from the different managed systems and sends the pertinent information over encrypted channels to the Control Center. As such, the Agents are best installed, and designed to be installed, on the different monitored systems, to allow secure file access to the pertinent logs and file systems that need to be monitored.

The Control Center aggregates and interprets information from all the monitored systems and presents it in a functional manner to the user, with options to manage the information into meaningful presentations. Because the Control Center combines the data while monitoring the active systems, it is best for the Control Center to be separate from the monitored systems.

Intended Audience

This manual is intended for IT administrators in their use of GroupWise Reporting and Monitoring or anyone wanting to learn more about GroupWise Reporting and Monitoring. It includes installation instructions for various scenarios. This manual expects you to have an understanding of GroupWise and GWCheck.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the on-line documentation.

Additional Documentation

Online documentation can be found on the [Micro Focus](https://www.microfocus.com/products/) website.

Knowledge Base articles can be found on the [Micro Focus Knowledge Base](https://www.microfocus.com/support-and-services/knowledge-base/) website.

Technical Support

If you have a technical support question, please consult the Micro Focus Technical Support at [our website](https://www.microfocus.com/support-and-services/) and enter Retain Unified Archiving.

Sales

Micro Focus contact information and office locations: www.microfocus.com

To contact a Micro Focus sales team member, please e-mail info@gwava.com or call 866-GO-GWAVA ((866) 464-9282), or +1 (514) 639-4850 in North America.

Professional Services

There are certain activities, for example large data migrations, that you may contract with Micro Focus Professional Services with to do for you.

North America: sales@microfocus.com or call (877) 772-4450.

About Micro Focus

Micro Focus is the world's largest infrastructure software company. Micro Focus a pure play software company with a portfolio that spans IT operations, security, information management, big data analytics, cloud, open source and development. Micro Focus focuses on creating world-class software that brings long-term value to our customers. To provide that long-term value Micro Focus does not shut down products, even when there are similar products in the subcategory, because that serves the long-term needs of the customer.

Copyright Notices

The content of this manual is for informational use only and may change without notice. Micro Focus assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

© 2018 GWAVA Inc., a Micro Focus company. All rights reserved.

Micro Focus, Retain, the Retain logo, GWAVA, and GroupWise, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

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 WebAccess are registered trademarks of Novell, and copyrighted by Novell. Windows is copyrighted by Microsoft. © 2005 Beginfinite Inc. All rights reserved. ® GWAVA is a registered trademark.
- ♦ Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, and 2004 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.
- ♦ Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Boutell.Com, Inc.
- ♦ Portions relating to GD2 format copyright 1999, 2000, 2001, 2002, 2003, 2004 Philip Warner
- ♦ Portions relating to PNG copyright 1999, 2000, 2001, 2002, 2003, 2004 Greg Roelofs
- ♦ Portions relating to gdtft.c copyright 1999, 2000, 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org)
- ♦ Portions relating to gdft.c copyright 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org)
- ♦ Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, 2003, 2004, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information
- ♦ Portions relating to GIF compression copyright 1989 by Jef Poskanzer and David Rowley, with modifications for thread safety by Thomas Boutell
- ♦ Portions relating to GIF decompression copyright 1990, 1991, 1993 by David Koblas, with modifications for thread safety by Thomas Boutell
- ♦ Portions relating to WBMP copyright 2000, 2001, 2002, 2003, 2004 Maurice Szmurlo and Johan Van den Brande
- ♦ Portions relating to GIF animations copyright 2004 Jaakko Hyvätti (jaakko.hyvatti@iki.fi). This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation
- ♦ Although their code does not appear in the current release, the authors also wish to thank Hutchison Avenue Software Corporation for their prior contributions
- ♦ Toffa SyncWise 2005 is produced by Toffa International
- ♦ Blackberry is produced by Research in Motion LTD
- ♦ NotifyLink is produced by Notify Technology Corporation.

1 Release Notes

About New Features

The document communicates the major new features and changes in this release of GroupWise Reporting and Monitoring. It also documents known problems and workarounds.

About This Release

GroupWise Reporting and Monitoring 18 has added a number of new features as well as fixed a number of bugs from previous versions.

New Features

GWRM 18.0.1

- ♦ Support for GroupWise 18.2.
- ♦ Support for SLES 12.4, SLES 15.1, and Windows 2019.
- ♦ Added a button that links to the Ideas Exchange for submitting suggestions.

GWRM 18.0

- ♦ Rename “Redline” to “GroupWise Reporting and Monitoring”.
- ♦ Replace occurrences of GWAVA (the company) with Micro Focus.
- ♦ Rename other products referenced in GroupWise Reporting and Monitoring.
- ♦ Support for GroupWise 18.
- ♦ Support for SSL connections to agents.

Bug Fixes and Enhancements

General Note

All bug fixes and enhancements will be listed here. These enhancements are not limited to the previous version of GroupWise Reporting and Monitoring and could affect other versions. Please refer to the [online documentation \(https://www.microfocus.com/documentation/groupwise/\)](https://www.microfocus.com/documentation/groupwise/) for further clarification or contact [Micro Focus \(https://support.microfocus.com/contact/gwava.html\)](https://support.microfocus.com/contact/gwava.html)

GWRM 18.0.1

- ♦ Addressed several issues reported by the FortifyOnDemand analysis.
- ♦ Updated the SQLite and OpenSSL libraries.
- ♦ Updated the copyright.

- ♦ Fixed an occasional Control Center crash.
- ♦ Fixed crash reported during the systemctl stop of the ragent.
- ♦ Fixed max CPU utilization of ragent running on a GWDR server.
- ♦ Fixed the Too many open files error for the ragent on SLES 12 & 15.
- ♦ Fixed the Current C/S Users Connected value.
- ♦ Changed the RAgent to retry correctly when the RLCC shuts down.
- ♦ Fixed the GWMM Usage Analysis report to show the Most Audited Accounts.

2 System Requirements

The optimal setup for GWRM, which should be used in all setups except perhaps the smallest systems, consists of the GWRM Control Center on a dedicated Windows or Linux server, connected to, and monitoring, the rest of the system by agents.

This setup is also recommended for clustered systems, with the GWRM Control Center as a standalone dedicated server, separate from the monitored system or systems.

- ♦ [“Control Center Requirements” on page 11](#)
- ♦ [“Agent Requirements” on page 12](#)

Control Center Requirements

GroupWise Reporting and Monitoring (GWRM) Control Center should be installed on a dedicated server.

- ❑ **Operating System Requirements:** Any of the following OS's.

- ♦ Linux: SLES 11 x86_64, SLES 12 x86_64, SLES 15 x86_64

IMPORTANT: SLES 12 SP4 and SLES 15 SP1 are supported in GWRM 18.0.1 or later.

- ♦ Windows: 2012 64 bit, 2016 64 bit, 2019 64 bit

IMPORTANT: Windows 2019 is supported in GWRM 18.0.1 or later.

- ❑ **Disk Space Requirements:** Minimum 30 MB Hard Drive Space. Additional disk space is required for the database. The database can grow several GB depending on how the system is used.

- ❑ **Memory Requirements:** 40 MB + (number of agents * 4 MB for each agent) + (largest GroupWise Log file in MB * 1.5).

Example: A system with 100 GW Agents registered and GroupWise Log file with up to 1GB:

$40\text{MB} + (100 * 4) + (1000 * 1.5) = 1940\text{MB}$.

- ❑ **Supported Internet Browsers:** The following browsers can be used to access the GWRM Control Center:

- ♦ Microsoft Edge
- ♦ Firefox
- ♦ Safari
- ♦ Chrome

- ❑ (Optional) If you want to run the Control Center using SSL, you must obtain a certificate for the server and provide it during the install.

Agent Requirements

GWRM Agents should be installed on the servers where the monitored agent are located.

☐ **Operating System Requirements:** Any of the following OS's

- ♦ Linux: SLES 11 x86_64, SLES 12 x86_64, SLES 15 x86_64

IMPORTANT: SLES 12 SP4 and SLES 15 SP1 are supported in GWRM 18.0.1 or later.

- ♦ Windows: 2012 64 bit, 2016 64 bit, 2019 64 bit

IMPORTANT: Windows 2019 is supported in GWRM 18.0.1 or later.

☐ **Disk Space Requirements:** 10MB Hard Drive Space and 5MB free system memory.

☐ **Supported Agents:** The following agents can be monitored:

- ♦ GroupWise Messenger 18
- ♦ GroupWise Messenger Archive Agent 18
- ♦ GroupWise Message Transfer Agent
- ♦ GroupWise Post Office Agent
- ♦ GroupWise Internet Agent
- ♦ GroupWise Document Viewer Agent
- ♦ GroupWise WebAccess Application
- ♦ GroupWise Disaster Recovery
- ♦ GroupWise Forensics
- ♦ GroupWise Mailbox Management
- ♦ BlackBerry Enterprise Server 4.0 SP2, and 5x
- ♦ Advansys Archive 2 Go
- ♦ Micro Focus Retain
- ♦ Micro Focus Secure Messaging Gateway

3 Installation

GroupWise Reporting and Monitoring (GWRM) requires the GWRM Control Center and at least one GWRM Agent to be installed. The GWRM Control Center should be installed on a dedicated server which meets the System Requirements. The GWRM Agent needs to be installed on the GroupWise servers with agents you want monitored.

- ♦ [“Installing the Control Center on Linux” on page 13](#)
- ♦ [“Installing the Control Center on Windows” on page 14](#)
- ♦ [“Accessing Control Center” on page 17](#)
- ♦ [“Installing the License” on page 17](#)
- ♦ [“Installing the Agent on Linux” on page 18](#)
- ♦ [“Installing the Agent on Windows” on page 19](#)
- ♦ [“Update GWRM” on page 20](#)
- ♦ [“Uninstall GWRM” on page 20](#)

Installing the Control Center on Linux

The Control Center should be installed on a dedicated server. If you want to run the Control Center using SSL, you must obtain a certificate for the Control Center server and specify the path to the certificate during the install.

- ☐ Download the GWRM zip file on the server.
- ☐ Extract the contents of the `gwrp-18.0.0.xxx.zip` file.
- ☐ Open a terminal and browse to the unzipped folder.

NOTE: Make sure you are logged in as `root` or use `su` to switch to `root`.

- ☐ Run `./install.sh` in the terminal to run the install.
- ☐ Follow the prompts to install the GWRM Control Center software. Keep in mind the following:
 - ♦ If you want to use SSL, make sure your certificate is available on the server during the install so you can specify the path to the certificate.
 - ♦ While you can install the Control Center and Agent on the same machine, this is only recommended for small installations of GWRM. We recommend you select the `Control Center only` install option.

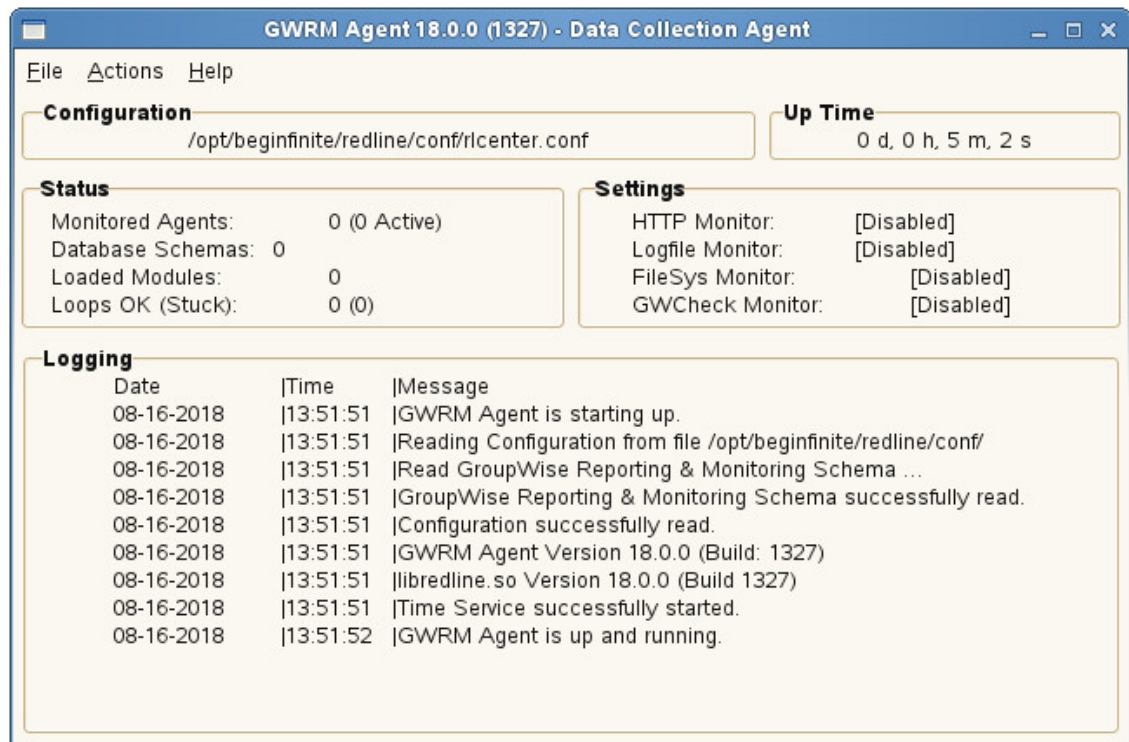
The Control Center agents on Linux can run as a background process and, mostly for debugging purposes, as a foreground process with a screen. You can manually start and stop the Control Center using `rlcenter` in `/etc/init.d`.

To start the Control Center with a GUI screen:

- ☐ In a terminal (either logged in as `root` or using `su`), browse to `/opt/beginfinite/redline/bin/`.
- ☐ Run the following command:

```
./rlcenter -c /opt/beginfinite/redline/conf/rlcenter.conf --show
```

The Control Center Screen on Linux shows up with a couple of options available through the main menu.



Installing the Control Center on Windows

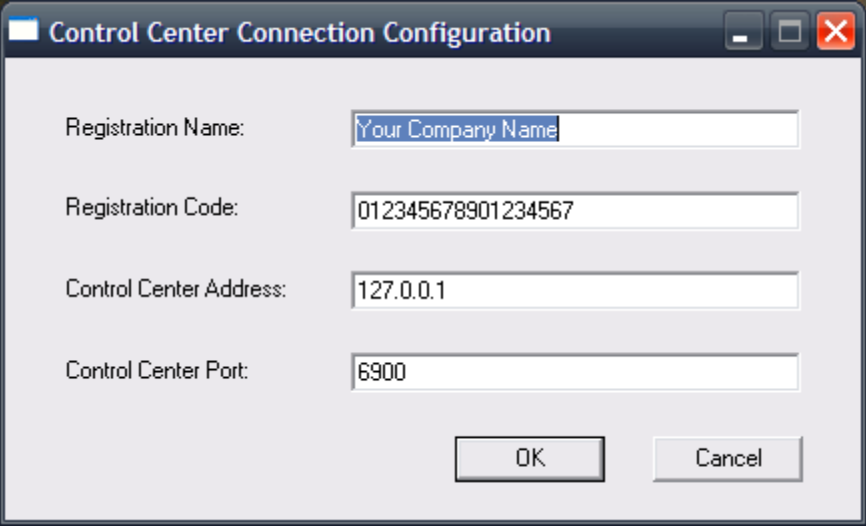
The Control Center should be installed on a dedicated server. If you want to run the Control Center using SSL, you must obtain a certificate for the Control Center server and specify the path to the certificate during the install.

- ☐ Download the GWRM zip file on the server.
- ☐ Extract the contents of the `GWRM_18.0.0.xxx_WINx64` zip file and browse to the extracted files.
- ☐ Run the `Setup.exe` file.
- ☐ When prompted, select the drive where you want to install the Control Center.
(Optional) Browse to the certificate key file

GWRM on Windows can run as a Windows Service and, mostly for debugging purposes, as a foreground process with or without a screen like the Linux screen. It is recommended to first launch GWRM 'with screen' to ensure that the configuration is correct. After configuring, shut down the application and restart without the screen. To start GWRM as an application, double click on one of it's icons on the desktop.

If you installed GWRM as a service, the agent is not started. It is important to start the agent manually after installation. To start GWRM as a service, start it from the Windows Services interface.

If the Agent is started the very first time and the Registration Name is still the default, you will be asked for Registration Name, Registration Code, Control Center IP address and port. If you start the Agent as a service, this dialog does not show up. Everything else can be configured through the Control Center web interface.



The image shows a Windows dialog box titled "Control Center Connection Configuration". It contains four text input fields with labels to their left: "Registration Name:" with the text "Your Company Name", "Registration Code:" with the text "012345678901234567", "Control Center Address:" with the text "127.0.0.1", and "Control Center Port:" with the text "6900". At the bottom right of the dialog are two buttons: "OK" and "Cancel". The dialog has a standard Windows window border with minimize, maximize, and close buttons in the top right corner.

The Agent and Control Center screens on Windows show up with all the log entries, like the Linux screens.

Control Center

File Action Help																																																						
<div> <div>Configuration</div> <div> \opt\beginfinite\redline\conf\rlcenter.conf </div> </div>		<div>Up Time</div> <div> 0 d 1 h 24 m 45 s </div>																																																				
<div>Status</div> <div> <div>Active Agents: 34 (6 Hosts)</div> <div>Active Users: 0</div> <div>DB Schemas: 30 (16 Loaded)</div> <div>Log Level: 2</div> </div>		<div>Settings</div> <div> <div>Agent Listener: [Enabled]</div> <div>Listen on Host: 10.1.35.2:6900</div> <div>HTTP Server: [Enabled]</div> <div>Listen on Host: 10.1.35.2:6910</div> </div>																																																				
<div>Log Messages</div> <table border="1"> <thead> <tr> <th>Date</th> <th>Time</th> <th>[Thrd]</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>11-20-2012</td> <td>09:25:34</td> <td>[B54]</td> <td>Agent gwdva.EBM-GW2012-WIN2 didn't report data for 2768541 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:34</td> <td>[B54]</td> <td>Agent gwdva.ebmglw12wa didn't report data for 2768532 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:35</td> <td>[B54]</td> <td>Agent JEDI.THEFORCE didn't report data for 2768641 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:35</td> <td>[B54]</td> <td>Agent NEWREPUBLIC didn't report data for 2768519 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:35</td> <td>[B54]</td> <td>Agent REBELS.NEWREPUBLIC didn't report data for 2768505 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:35</td> <td>[B54]</td> <td>Agent Serenity.Firefly didn't report data for 2767448 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:36</td> <td>[B54]</td> <td>Agent SITH.THEFORCE didn't report data for 2768620 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:36</td> <td>[B54]</td> <td>Agent TAZ-GWAVA didn't report data for 318227 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:36</td> <td>[B54]</td> <td>Agent THEFORCE.GWIA didn't report data for 2768752 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:36</td> <td>[B54]</td> <td>Agent THEFORCE didn't report data for 2768708 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:37</td> <td>[B54]</td> <td>Agent WebAcc.EBM-GW2012-WIN2 didn't report data for 2768599 seconds.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:37</td> <td>[B54]</td> <td>Agent WebAcc.ebmglw12wa didn't report data for 2768560 seconds.</td> </tr> </tbody> </table>			Date	Time	[Thrd]	Message	11-20-2012	09:25:34	[B54]	Agent gwdva.EBM-GW2012-WIN2 didn't report data for 2768541 seconds.	11-20-2012	09:25:34	[B54]	Agent gwdva.ebmglw12wa didn't report data for 2768532 seconds.	11-20-2012	09:25:35	[B54]	Agent JEDI.THEFORCE didn't report data for 2768641 seconds.	11-20-2012	09:25:35	[B54]	Agent NEWREPUBLIC didn't report data for 2768519 seconds.	11-20-2012	09:25:35	[B54]	Agent REBELS.NEWREPUBLIC didn't report data for 2768505 seconds.	11-20-2012	09:25:35	[B54]	Agent Serenity.Firefly didn't report data for 2767448 seconds.	11-20-2012	09:25:36	[B54]	Agent SITH.THEFORCE didn't report data for 2768620 seconds.	11-20-2012	09:25:36	[B54]	Agent TAZ-GWAVA didn't report data for 318227 seconds.	11-20-2012	09:25:36	[B54]	Agent THEFORCE.GWIA didn't report data for 2768752 seconds.	11-20-2012	09:25:36	[B54]	Agent THEFORCE didn't report data for 2768708 seconds.	11-20-2012	09:25:37	[B54]	Agent WebAcc.EBM-GW2012-WIN2 didn't report data for 2768599 seconds.	11-20-2012	09:25:37	[B54]	Agent WebAcc.ebmglw12wa didn't report data for 2768560 seconds.
Date	Time	[Thrd]	Message																																																			
11-20-2012	09:25:34	[B54]	Agent gwdva.EBM-GW2012-WIN2 didn't report data for 2768541 seconds.																																																			
11-20-2012	09:25:34	[B54]	Agent gwdva.ebmglw12wa didn't report data for 2768532 seconds.																																																			
11-20-2012	09:25:35	[B54]	Agent JEDI.THEFORCE didn't report data for 2768641 seconds.																																																			
11-20-2012	09:25:35	[B54]	Agent NEWREPUBLIC didn't report data for 2768519 seconds.																																																			
11-20-2012	09:25:35	[B54]	Agent REBELS.NEWREPUBLIC didn't report data for 2768505 seconds.																																																			
11-20-2012	09:25:35	[B54]	Agent Serenity.Firefly didn't report data for 2767448 seconds.																																																			
11-20-2012	09:25:36	[B54]	Agent SITH.THEFORCE didn't report data for 2768620 seconds.																																																			
11-20-2012	09:25:36	[B54]	Agent TAZ-GWAVA didn't report data for 318227 seconds.																																																			
11-20-2012	09:25:36	[B54]	Agent THEFORCE.GWIA didn't report data for 2768752 seconds.																																																			
11-20-2012	09:25:36	[B54]	Agent THEFORCE didn't report data for 2768708 seconds.																																																			
11-20-2012	09:25:37	[B54]	Agent WebAcc.EBM-GW2012-WIN2 didn't report data for 2768599 seconds.																																																			
11-20-2012	09:25:37	[B54]	Agent WebAcc.ebmglw12wa didn't report data for 2768560 seconds.																																																			

Agent

File Action Help																																																						
<div>Configuration</div> <div> \opt\beginfinite\redline\conf\rlagwin.conf </div>		<div>Up Time</div> <div> 0 d 1 h 24 m 45 s </div>																																																				
<div>Status</div> <div> <div>Monitor Loops: 33 (0 Stuck)</div> <div>Monitored Agents: 9 (9 Active)</div> <div>Database Schemas: 30 (24 Loaded)</div> <div>Log Level: 2</div> </div>		<div>Settings</div> <div> <div>HTTP Monitor: [Enabled]</div> <div>Logfile Monitor: [Enabled]</div> <div>FileSys Monitor: [Enabled]</div> <div>GWCheck Monitor: [Enabled]</div> </div>																																																				
<div>Log Messages</div> <table border="1"> <thead> <tr> <th>Date</th> <th>Time</th> <th>[Thrd]</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>11-20-2012</td> <td>09:23:09</td> <td>[11E4]</td> <td>Send Agent furya.helion (5) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:23:11</td> <td>[11E4]</td> <td>Send Agent RetainServer(PARAMETER name= (47) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:23:12</td> <td>[11E4]</td> <td>Send Agent Worker-Retain-Windows (46) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:23:33</td> <td>[11E4]</td> <td>Send Agent WEBAC80A.helion (13) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:23:34</td> <td>[11E4]</td> <td>Send Agent webapp.WEBAC80A.helion (15) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:23:34</td> <td>[12A0]</td> <td>Agent Monitor Loop finished.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:34</td> <td>[12A0]</td> <td>Agent Monitor Loop running ... (timeout is 120 seconds).</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:35</td> <td>[11E4]</td> <td>Send Agent RLAgent-GWAVADEVPC (2) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:37</td> <td>[11E4]</td> <td>Send Agent gwdva.WEBAC80A.helion (14) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:38</td> <td>[11E4]</td> <td>Send Agent GWAVADEVPC (3) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:39</td> <td>[11E4]</td> <td>Send Agent helion (4) Update to Control Center.</td> </tr> <tr> <td>11-20-2012</td> <td>09:25:40</td> <td>[11E4]</td> <td>Send Agent furya.helion (5) Update to Control Center.</td> </tr> </tbody> </table>			Date	Time	[Thrd]	Message	11-20-2012	09:23:09	[11E4]	Send Agent furya.helion (5) Update to Control Center.	11-20-2012	09:23:11	[11E4]	Send Agent RetainServer(PARAMETER name= (47) Update to Control Center.	11-20-2012	09:23:12	[11E4]	Send Agent Worker-Retain-Windows (46) Update to Control Center.	11-20-2012	09:23:33	[11E4]	Send Agent WEBAC80A.helion (13) Update to Control Center.	11-20-2012	09:23:34	[11E4]	Send Agent webapp.WEBAC80A.helion (15) Update to Control Center.	11-20-2012	09:23:34	[12A0]	Agent Monitor Loop finished.	11-20-2012	09:25:34	[12A0]	Agent Monitor Loop running ... (timeout is 120 seconds).	11-20-2012	09:25:35	[11E4]	Send Agent RLAgent-GWAVADEVPC (2) Update to Control Center.	11-20-2012	09:25:37	[11E4]	Send Agent gwdva.WEBAC80A.helion (14) Update to Control Center.	11-20-2012	09:25:38	[11E4]	Send Agent GWAVADEVPC (3) Update to Control Center.	11-20-2012	09:25:39	[11E4]	Send Agent helion (4) Update to Control Center.	11-20-2012	09:25:40	[11E4]	Send Agent furya.helion (5) Update to Control Center.
Date	Time	[Thrd]	Message																																																			
11-20-2012	09:23:09	[11E4]	Send Agent furya.helion (5) Update to Control Center.																																																			
11-20-2012	09:23:11	[11E4]	Send Agent RetainServer(PARAMETER name= (47) Update to Control Center.																																																			
11-20-2012	09:23:12	[11E4]	Send Agent Worker-Retain-Windows (46) Update to Control Center.																																																			
11-20-2012	09:23:33	[11E4]	Send Agent WEBAC80A.helion (13) Update to Control Center.																																																			
11-20-2012	09:23:34	[11E4]	Send Agent webapp.WEBAC80A.helion (15) Update to Control Center.																																																			
11-20-2012	09:23:34	[12A0]	Agent Monitor Loop finished.																																																			
11-20-2012	09:25:34	[12A0]	Agent Monitor Loop running ... (timeout is 120 seconds).																																																			
11-20-2012	09:25:35	[11E4]	Send Agent RLAgent-GWAVADEVPC (2) Update to Control Center.																																																			
11-20-2012	09:25:37	[11E4]	Send Agent gwdva.WEBAC80A.helion (14) Update to Control Center.																																																			
11-20-2012	09:25:38	[11E4]	Send Agent GWAVADEVPC (3) Update to Control Center.																																																			
11-20-2012	09:25:39	[11E4]	Send Agent helion (4) Update to Control Center.																																																			
11-20-2012	09:25:40	[11E4]	Send Agent furya.helion (5) Update to Control Center.																																																			

It is recommended to run the agent as a Windows Service. A Service is started without logging in to the server, just by booting the machine. That way the GWRM Agent is started every time the server is restarted.

Accessing Control Center

GWRM is a full Web Based Application. By default, GWRM is listening on port 6910. After Installation, the default administrator username is admin, and the password is password.

To access the Web Interface, type

```
http://a.b.c.d:6910
```

Where a.b.c.d is the IP address of your Control Center.

You will be asked for the username and password.

The first page you will see is the Dashboard. The Dashboard gives an overview of your System, which includes GWRM itself and all registered GroupWise components.

Installing the License

Upon installation, a 30-day Registration Code was generated for temporary use on all the Control Centers, along with evaluation entries for the 'Registration Name' and 'Registration Code' fields. If the Control Center is running with the 30-day evaluation license, there are NO limitations in functionality; however, the GWRM system will become completely inactive after the evaluation expires.

When you purchase GWRM, you will receive a new PEM license file. This file contains all your license information and needs to be installed.

When you purchase GWRM, you will receive an email with a license key. You may also find your license key in the GWAVA Customer Center Portal (<https://gwava.microfocus.com/customercenter/>). Copy the key into the License Registration page (<https://licenses.gwava.com/>) making sure to choose the correct product. Fill in your information and download the PEM license file.

Log in using the web interface:

- ♦ Click the Configure and select 'Control Center', to open the dropdown menu
- ♦ Select 'License'
- ♦ Enter the Registration information.
- ♦ Ensure all GWRM Agents are updated with this information as well
- ♦ Install the license file, by selecting Browse, browse to the PEM file, press OK, and press Install License.

The Registration Name and Code must be configured on all GWRM Control Center and Agent installs. The Name and Code are used to authenticate the agents to the Control Center every time an Agent wants to send data. Both the GWRM Agent and the GWRM Control Center use the Registration Name and Registration Code information for two purposes:

- ♦ The GWRM Agent uses these values as an encryption key when communicating with the Control Center. The GWRM Agent has its own copy of the above information, stored in `RLAGENT.CONF`. If the two do not match, the GWRM Agent is unable to contact the Control Center and generates an error on the GWRM Agent console.
- ♦ These values are also used for license enforcement by the GWRM Control Center. The Control Center may determine a license is invalid or the evaluation license has expired. In this case, the GWRM Agent will not be able to contact the Control Center any longer, because the Control Center shuts down the listening port for the GWRM Agents. An error is generated on the GWRM Agent console.

Installing the Agent on Linux

You may install only the agent on another Linux server by choosing the agent install.

Once the agent is installed:

1. Navigate to the conf folder, by default: `opt/beginfinite/redline/conf`.
2. Edit the file `rlagent.conf`.
3. Remove the `NEWINSTALL` line from the file.
4. Save the file.
5. Start the GWRM agent.

Installing the Agent on a Linux Cluster

To install GWRM agent into a Linux Cluster environment, a few things need to be changed, mainly, where GWRM is installed.

- ♦ Install GWRM to one of the cluster nodes according to the normal procedure for Linux.
- ♦ GWRM installs to `/opt/beginfinite/redline` by default. Copy the entire GWRM directory to each of the resources. (`resourcevol/GWRM`)
- ♦ Navigate to `/etc/init.d` directory on the machine you installed GWRM, and rename the `rlagent` file to `rlag`.

NOTE: The default installation installs both GWRM Agent and Control Center. It is recommended to run the command: `"chkconfig --del rlcenter"` to stop the Control Center from automatically loading. Once the GWRM Agent has been copied to all the resources in the cluster, the default installation folder on the node can be removed.

- ♦ Copy the newly renamed `rlag` file to the `resourcevol/GWRM/bin` on each resource.
- ♦ Edit the newly renamed `rlag` file. Every listed directory in that file must now point to the resource directory. (Defaults will look like: `/opt/beginfinite/redline/bin`) Modify the path to reflect the resource volume, ie. `/resourcevol/GWRM/bin`. There will be 5 to 6 paths to modify. Save the file. Edit the `rlag` file for each resource.

- ♦ Open the rlagent.conf file that was copied over to the cluster volume. In the "conf" folder, the "rlagent.conf" file needs to be edited. Remove the "NEWINSTALL" line at the top. Input the correct Control Center information in the [CCenter1] section, (IP, Port, Registration information needs to match the information put into the Control Center configuration file.) There are two other special settings that need to be set for the cluster environment. The [HOST] and [GLOBAL] sections must be modified. For the [HOST] section under the Agent=enabled, add a line: AgentName=HOST_RESOURCE_NAME

Modify each cluster resource appropriate name; the name can be anything desired, but it is recommended to name it the resource so it is easily recognized in the Control Center. The [GLOBAL] section is very similar, the GWRMAgentName parameter is commented out, enable it and specify: GWRMAgentName=RLAgent_RESOURCE_NAME. You'll want to change the volume name for each cluster.

- ♦ Startup the individual agent by specifying the path to: /resourcevol/GWRM/bin/rlag start
Unload the individual agents by referencing the same path: /resourcevol/GWRM/bin/rlag stop

These are the start and stop scripts.

- ♦ Finally make sure that you have the GWRM libraries installed on each node. Locate the GWRM.tar.gz file, located in the install folder where GWRM was downloaded. Go to GWRM/linux.suse< 32 or 64 as appropriate>/GWRM

You should find two files:

GWRM-<version number>-1.<platform>.rpm

GWRM.tar.gz

Unzip the GWRM.tar.gz file. A new directory called 'bintree' will appear which will contain a file called "libGWRM.so.4.0.0". Copy the 'libGWRM.so.4.0.0' file to the lib directory (/lib or /lib64) of each of the nodes.

- ♦ On each of the nodes, run the command: ldconfig

NOTE: ldconfig must be run in order to create the necessary links and cache, (used by the run-time linker, ld.so), to the most recent shared libraries found in the directories specified on the command line, in the file /etc/ld.so.conf, and in the trusted directories, (/usr/lib and /lib).

Installing the Agent on Windows

- ♦ Unzip the GWRM package onto your Windows server.
- ♦ From the /GWRM/windows/ folder run the setup.exe. Click Next.
- ♦ Accept the license agreement. Click Next.
- ♦ Select the drive letter where you want to install the agent. This is necessary if you want to install the agent in a Windows Cluster.
- ♦ Select the **Agent Only** install. We recommend you also select to install the agent as a service so it starts automatically if the server reboots. You also need to specify the information for your Control Center and license so the agent can contact the control center.

Running Multiple GWRM Agents on Windows

It is possible to run multiple instances of the GWRM Agent on a Windows box as a server. To set this up, you need to do the following:

- ♦ Copy the folder `c:\opt\beginfinite\GWRM` to `c:\beginfinite\GWRM2` (or another folder like `GWRM3`, `GWRM 4` etc.)
- ♦ Open a cmd prompt
- ♦ Go to the folder where you've copied your new GWRM Agent installation conf folder (`c:\opt\beginfinite\GWRM\conf2`)
- ♦ Edit `rlagwin.conf` and adjust the folders for `LogFilePath`, `DataPath`, `BinPath` and `SoftwarePath`
- ♦ Go to the bin folder of your new GWRM Agent installation
- ♦ Run `rlagent install GWRMAgent2` (or any other unique name for this service)
- ♦ Wait a moment until a message appears that the agent has been installed successfully.
- ♦ (Optional) To uninstall the service, type `rlagent uninstall GWRMAgent2` (or whatever name you've given the service).

Now you can run the GWRM Agent multiple times on your Windows Server:

Update GWRM

GWRM may be automatically updated online as well as with an installation file. Online installation is performed through the Control Center UI, and is covered in the Administration guide.

The installation file Update process is the same as the installation process. All installers detect if a previous version is there and make sure that all customer settings aren't touched.

After an update GWRM should work immediately as it has done before. No GWRM Agent and GWRM Control Center configuration files are overwritten. Sometimes new values will be added.

Uninstall GWRM

GWRM's ability to drill deep into even the most complex GroupWise message system offers network administrators, and business owners an ability to understand the inner workings of their e-mail system. We sincerely hope that GWRM has provided powerful functionality that you cannot find elsewhere.

If you are uninstalling GWRM, and have questions about your trial, please feel free to contact us at info@gwava.com.

Windows

- ♦ Stop the GWRM Agent and Control Center
- ♦ Start the Windows Setup.exe and click through the prompts. On the last page select Uninstall.
- ♦ Uninstalling the GWRM Control Center will also uninstall the Agent.

Linux

Automatically

In a graphical Linux environment, use the YaST command. From the command line do the following:

- ♦ Login as root or use su to switch to root.
- ♦ Run the `./install.sh` from the extracted GWRM software and select the option to uninstall.
- ♦ For complete uninstall, delete the `/opt/beginfinite/redline` directory.

Manually

- ♦ Stop both GWRM programs: To stop RLAGENT, type `/etc/init.d/rlagent stop` at the command line and to stop the Control Center, type `/etc/init.d/rlcenter stop` at the command line

```
/etc/init.d/rlagent stop  
/etc/init.d/rlcenter stop
```

- ♦ Delete the `/opt/beginfinite/redline` tree
- ♦ Remove `/etc/init.d/rlcenter` and `/etc/init.d/rlagent`
- ♦ Remove `/lib/libGWRM.so.4.0.0`

4 Configuring GroupWise Reporting and Monitoring

After you install GroupWise Reporting and Monitoring (GWRM), you need to configure the agents you want to monitor and connect to them through GWRM:

- ♦ [“GroupWise Agents” on page 23](#)
- ♦ [“GroupWise Messenger Agents” on page 46](#)
- ♦ [“GroupWise Disaster Recovery” on page 52](#)
- ♦ [“GroupWise Forensics” on page 53](#)
- ♦ [“GroupWise Mailbox Management” on page 54](#)
- ♦ [“Micro Focus Retain” on page 55](#)
- ♦ [“GWAVA 6.5 and Secure Messaging Gateway” on page 55](#)
- ♦ [“Advansys Archive2Go” on page 55](#)
- ♦ [“Blackberry Enterprise Server” on page 56](#)

GroupWise Agents

Use the following section to configure the GroupWise agents you want to monitor using GWRM:

- ♦ [“GroupWise Post Office Agent \(POA\)” on page 23](#)
- ♦ [“GroupWise Message Transfer Agent \(MTA\)” on page 31](#)
- ♦ [“GroupWise Internet Agent \(GWIA\)” on page 34](#)
- ♦ [“GroupWise Document Viewer Agent” on page 39](#)
- ♦ [“GroupWise WebAccess Application” on page 42](#)

GroupWise Post Office Agent (POA)

Before adding a POA to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the POA server. Use the sections below to configure and add the POA to GWRM to monitor:

- ♦ [“Configuring the POA” on page 24](#)
- ♦ [“Adding the POA to GWRM” on page 29](#)
- ♦ [“POA Worksheet” on page 31](#)

Configuring the POA

- ❑ In the GroupWise Admin Console > **Post Office Agents**, select the POA and go to the **Agent Settings** tab.

Post Office Agent : POA

Provo1 Development POA

Delete Diagnostics

General **Agent Settings** Log Settings SSL Settings Scheduled Events Maintenance QuickFinder Document Viewer Agent

Message Processing

Message File Processing: All

Message Handler Threads: 6

Message Transfer Port: 7101 SSL: Enabled

☒ Enable caching

☐ Disable Administration Task Processing

Network Address

TCP/IP Address:

External IP Address:

☒ Bind exclusively to TCP/IP Address

Admin Port: 9711

Client/Server

☒ Enabled

Client/Server Handler Threads: 10

Max App Connections: 2048

Max Physical Connections: 2048

Max Thread Usage for Priming and Moves: 30 percent

Internal Port: 1677 SSL: Enabled

External Port: 0

HTTP

HTTP User Name:

HTTP Password:

Confirm Password:

- ❑ In the **HTTP** section, specify an **HTTP User Name** and **HTTP Password**. Do not use an eDirectory or Active Directory user name and password for the HTTP User Name and Password.

NOTE: While we recommend you use the default HTTP Port of 7181 and leaving SSL enabled, you can change the HTTP Port and disable SSL if you desire.

- ❑ In the **SNMP** section, enable SNMP.
(Optional) Assign a community string to SNMP for enhanced security.
- ❑ Change to the **Log Settings** tab. Make sure the **Logging Level** is set to **Verbose**.
- ❑ GWRM uses 3 GWCheck logs (gwaudit.log, gwstats.log, and mbstats.log) to get user information from GroupWise POA. These logs are not created by default. To create the GWCheck logs for GWRM, you need to create a scheduled event on the POA that gathers the information and puts it into the log files. Follow the steps below to create the scheduled event:
 - ◆ Go to the **Scheduled Events** tab on the POA.

- ♦ Create a new event and call it `GWRM Logs`.
- ♦ Change the **Event Type** to **Mailbox/Library Maintenance**.
- ♦ Change the **Trigger** to **Daily** and we recommend leaving the run time at 12:30 AM.
- ♦ Create a new event action. Call it `gwaudit.log`. Change the **Actions** field to **Audit Report**. On the **Logging** tab at the bottom, specify `gwaudit.log` in the **Log File Path** and make sure **Verbose Logging** is selected. Your event should match the screen shot below (the important area is highlighted):

The screenshot shows a configuration window titled "gwaudit.log" with a "Close" button in the top right corner. The window contains the following fields and controls:

- Name:** A text field containing "gwaudit.log".
- Actions:** A dropdown menu showing "Audit Report".
- Log accounts without activity for previous:** A numeric spinner set to "60" followed by the text "Days".
- Tabs:** Four tabs are located at the bottom: "Databases", "Logging" (which is selected and highlighted with a blue border), "Results", and "Misc".
- Logging Tab Content:**
 - Log File Path:** A text field containing "gwaudit.log", which is highlighted with a red rectangular box.
 - Verbose logging:** A checkbox that is checked, also highlighted with a red rectangular box.
- Footer:** A bar containing a help icon (question mark), and "OK" and "Cancel" buttons.

- ♦ Create another new event action. Call it `gwstats.log`. Change the **Actions** field to **Mailbox Statistics**. On the **Logging** tab at the bottom, specify `gwstats.log` in the **Log File Path** and make sure **Verbose Logging** is selected. Leave all other settings as their defaults. Your event should match the screen shot below (the important areas are highlighted):

The screenshot shows a configuration window titled "gwstats.log" with a "Close" button in the top right corner. The "Name" field is set to "gwstats.log". The "Actions" dropdown menu is set to "Mailbox Statistics", which is highlighted with a red box. Below this, the "Mailbox Statistics" radio button is selected, and the "Box Limit" is set to "500 items". The "Expire Statistics" section is unselected. The "Include" section has several unchecked checkboxes: "Received items", "Sent items", "Calendar items", "Only backed-up items", and "Only retained items". At the bottom, the "Logging" tab is selected and highlighted with a blue box. The "Log File Path" is set to "gwstats.log", and the "Verbose logging" checkbox is checked, both of which are highlighted with a red box. The bottom of the window shows a status bar with a question mark icon, the text "1-11 of 11", and "OK" and "Cancel" buttons.

gwstats.log

Name: gwstats.log

Actions: Mailbox Statistics

☒ Mailbox Statistics

Box Limit: 500 items

☐ Expire Statistics

☐ Items older than 60 Days

☐ Downloaded items older than 30 Days

☐ Items larger than 1000 KB

☐ Reduce mailbox to 5 MB

☐ Reduce mailbox to limited size

Include

☐ Received items

☐ Sent items

☐ Calendar items

☐ Only backed-up items

☐ Only retained items

Databases Logging Results Misc Exclude

Log File Path: gwstats.log

☒ Verbose logging

OK Cancel

1-11 of 11

- ♦ Create the last new event action. Call it `mbstats.log`. Change the **Actions** field to **Mailbox Statistics**. Select the **Expire Statistics** radial button. Select the **Items larger than** option and deselect the **Reduce mailbox to** option. On the **Logging** tab at the bottom, specify `mbstats.log` in the **Log File Path** and make sure **Verbose Logging** is selected. Your event should match the screen shot below (the important areas are highlighted):

The screenshot shows the configuration window for a mailbox statistics event. The 'Name' field is set to 'mbstats.log'. The 'Actions' dropdown is set to 'Mailbox Statistics'. The 'Mailbox Statistics' section is expanded, showing 'Box Limit' set to 500 items. The 'Expire Statistics' section is selected with a radio button. It contains several checked options: 'Items older than' (60 Days), 'Downloaded items older than' (30 Days), and 'Items larger than' (1000 KB). The 'Reduce mailbox to' and 'Reduce mailbox to limited size' options are unchecked. The 'Include' section has 'Received items', 'Sent items', and 'Calendar items' checked, while 'Only backed-up items' and 'Only retained items' are unchecked. At the bottom, the 'Logging' tab is selected, showing 'Log File Path' set to 'mbstats.log' and 'Verbose logging' checked. The window has 'OK' and 'Cancel' buttons at the bottom right.

- ♦ Once you have created all of the events, make sure they are all enabled by selecting them in the **GWRM Logs** scheduled event. You do not need to enable any of the default reports. You can delete them if you desire.
- ♦ Click **OK** to complete the scheduled event. Make sure it is enabled on the **Scheduled Events** tab or your logs will not be created.

NOTE: Below is a list of what each report provides to GWRM about the GroupWise users:

gwaudit.log	gwstats.log	mbstats.log
<ul style="list-style-type: none">◆ User Name◆ Post Office Name◆ UserDB file◆ Last Active date/time◆ Inactive Days◆ License Type	<ul style="list-style-type: none">◆ User Name◆ Post Office Name◆ Full Name◆ Mailbox Size◆ Last DRN◆ User MSG file◆ Data Records◆ SetupRecords◆ Record Bytes	<ul style="list-style-type: none">◆ User Name◆ Post Office Name◆ Full Name◆ UserDB file◆ Last Active date/time◆ License Type◆ Messages Total◆ Messages InBox◆ Messages OutBox◆ Messages Basket◆ Number of Mail items◆ Number of Notes◆ Number of Tasks◆ Number of Appointments◆ Number of Phone Messages◆ Number of Profiles◆ Number of Attachments◆ Number of Search folders◆ Mailbox Size◆ Last DRN◆ Data Records◆ Record Bytes◆ Maximum Mailbox Size◆ Mailbox Size Threshold

- ☐ Save the changes to the POA.
- ☐ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ☐ Write down the GWRM agent you are going to use to monitor the POA, POA IP address, HTTP User Name, Password, Port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [POA Worksheet](#).
(Optional) If you want GWRM to monitor the POA SOAP connection, write down the POA SOAP Port and SSL setting along with a test user GWRM can use to connect through SOAP.
- ☐ Repeat the steps above for each POA you want to monitor.

Adding the POA to GWRM

IMPORTANT: Make sure you have the following information written down on the [POA Worksheet](#) before adding the POA to GWRM:

- ♦ Name of the GWRM agent you are going to use to monitor the POA (usually the one on the POA server).
- ♦ POA IP address.
- ♦ HTTP User Name, Password, Port, and SSL setting for the POA.
- ♦ (Optional) The POA SOAP port and SSL setting along with a test user that GWRM can use to connect through SOAP to monitor the SOAP connection.

-
- ☐ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the POA (usually the one installed on the POA server) from the GWRM Agent list in the main panel.

- ❑ Go to the **Manage** tab.

Summary Status Settings Alerts Reports Graphs Configure Manage

GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1568), Platform: Linux 64bit 3.0.75-0.11-default, Uptime: 0d 21h 30m

Agent Information

Description

Global Unique ID (GUID)

Monitored Agents

Type	Description	Unique ID	Agent Name
HOST	Host	3	-

Add or Edit Monitored Agent

Agent Type:

Status: ☐ Enabled

HTTP Address:

HTTP Port:

HTTP Username:

HTTP Password:

Use SSL: ☐ Yes

Agent Name:

Agent Name Suffix:

Connection Test

The POA will be checked against the SOAP port and a login/logout to the defined account will be done.

Address:

Port:

Use SSL: ☐

Username:

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW Post Office Agent**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the POA IP address, HTTP port, user name, password, and SSL setting.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ (Optional) In the **Connection Test** section, you can have GWRM run a regular, automated SOAP connection test to see if SOAP is running on the POA. The connection test runs every 2 minutes. Enter the following for the test to run:
 - ◆ The POA IP address, SOAP Port, and SSL setting.
 - ◆ Specify a test user name and password GWRM can use to test the SOAP connection.
- ❑ Repeat the steps above to add all of the POAs you want to monitor to GWRM.

POA Worksheet

Use the following worksheet to record the necessary information to be able to add the POA to GWRM. Use this worksheet for each POA you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the POA.
POA IP Address		Specify the IP Address of the GroupWise POA.
HTTP User Name		Specify the user name entered for the HTTP web console in GroupWise.
HTTP Password		Specify the password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. The default is 7181.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.
(Optional) Connection Test		The connection test lets GWRM monitor the SOAP connection on the POA. Specify the SOAP connection information along with a test user for GWRM to use to test the connection.
♦ POA IP Address		
♦ SOAP Port		
♦ SOAP SSL Setting		
♦ SOAP Test user name and password		

GroupWise Message Transfer Agent (MTA)

Before adding a MTA to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the MTA server. Use the sections below to configure and add the MTA to GWRM to monitor:

- ♦ [“Configuring the MTA” on page 32](#)
- ♦ [“Adding the MTA to GWRM” on page 33](#)
- ♦ [“MTA Worksheet” on page 34](#)

Configuring the MTA

- ❑ In the GroupWise Admin Console > **Message Transfer Agents**, select the MTA and go to the **Agent Settings** tab.

The screenshot shows the 'MTA : MTA' configuration page. At the top, there are tabs for 'General', 'Agent Settings' (which is selected), 'Log Settings', 'SSL Settings', 'Scheduled Events', 'LDAP', and 'Exchange Synchronization'. Below the tabs, there are several sections of settings:

- Scan Cycle:** 15 seconds
- Scan High:** 5 seconds
- Attach Retry:** 60 seconds
- ☒ Enable Automatic Database Recovery
- ☒ Use 2nd High Priority Scanner
- ☒ Use 2nd Mail Priority Scanner
- SNMP Community "Get" String:** (empty text box)
- Network Address:**
 - TCP/IP Address:** prv-gwdoc2.provo.novell.com
 - Admin Port:** 9710
 - ☒ Bind exclusively to TCP/IP Address
- Message Transfer:**
 - Port:** 7100
 - SSL:** Enabled
- HTTP:**
 - HTTP User Name:** (empty text box)
 - HTTP Password:** (empty text box)
 - Confirm Password:** (empty text box)
 - Port:** 7180
 - SSL:** Enabled

At the bottom, there are 'Save' and 'Close' buttons.

- ❑ In the **HTTP** section, specify and **HTTP User Name** and **HTTP Password**. Do not use an eDirectory or Active Directory user name and password for the HTTP User Name and Password.

NOTE: While we recommend you use the default HTTP Port of 7180 and leaving SSL enabled, you can change the HTTP Port and disable SSL if you desire.

- ❑ SNMP is enabled by default on the MTA. You can assign a community string to SNMP for enhanced security.
- ❑ Change to the **Log Settings** tab. Make sure the **Logging Level** is set to **Verbose**.
- ❑ (Optional) If you want to use Message Tracking, change **Message Logging Level** to **Full**, select **Track Administrative Message**, and make sure **Delete Reports After** is not set to 0. We recommend setting it to 7 - 14 days.
- ❑ Save the changes to the MTA.
- ❑ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ☐ Write down the GWRM agent you are going to use to monitor the MTA, MTA IP address, HTTP User Name, Password, Port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [MTA Worksheet](#).
- ☐ Repeat the steps above for each MTA you want to monitor.

Adding the MTA to GWRM

IMPORTANT: Make sure you have the following information written down on the [MTA Worksheet](#) before adding the MTA to GWRM:

- ♦ Name of the GWRM agent you are going to use to monitor the MTA (usually the one on the MTA server).
- ♦ MTA IP address.
- ♦ HTTP User Name, Password, Port, and SSL setting for the MTA.

- ☐ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the MTA (usually the one installed on the MTA server) from the GWRM Agent list in the main panel.
- ☐ Go to the **Manage** tab.

The screenshot shows the 'Manage' tab in the GWRM Control Center. At the top, there's a status bar with 'Summary', 'Status', 'Settings', 'Alerts', 'Reports', 'Graphs', 'Configure', and 'Manage' tabs. Below this, a green status bar shows '99.97 %' and 'GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1508), Platform: Linux 64bit 3.0.78-0.11-default, Upt...'. The main content area is divided into two sections: 'Agent Information' and 'Monitored Agents'. The 'Agent Information' section shows 'Description' and 'Global Unique ID (GUID)'. The 'Monitored Agents' section is a table with columns 'Type', 'Description', 'Unique ID', and 'Agent Name'. Below this is the 'Add or Edit Monitored Agent' form. The form has fields for 'Agent Type' (set to 'GW Message Transfer Agent'), 'Status' (with an 'Enabled' checkbox), 'HTTP Address', 'HTTP Port', 'HTTP Username', 'HTTP Password', 'Use SSL' (with a 'Yes' checkbox), 'Agent Name', and 'Agent Name Suffix'. An 'OK' button is at the bottom.

Type	Description	Unique ID	Agent Name
HOST	Host	3	-

- ☐ In the **Add or Edit Monitored Agent** section, do the following:
 - ♦ Change the **Agent Type** to **GW Message Transfer Agent**.
 - ♦ Enable the agent in the **Status** field.

- ♦ Enter the MTA IP address, HTTP port, user name, password, and SSL setting.
 - ♦ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ☐ Repeat the steps above to add all of the MTAs you want to monitor to GWRM.

MTA Worksheet

Use the following worksheet to record the necessary information to be able to add the MTA to GWRM. Use this worksheet for each MTA you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the MTA.
MTA IP Address		Specify the IP Address of the GroupWise MTA.
HTTP User Name		Specify the user name entered for the HTTP web console in GroupWise.
HTTP Password		Specify the password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. The default is 7180.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.

GroupWise Internet Agent (GWIA)

Before adding a GWIA to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the GWIA server. Use the sections below to configure and add the GWIA to GWRM to monitor:

- ♦ [“Configuring the GWIA” on page 34](#)
- ♦ [“Adding the GWIA to GWRM” on page 36](#)
- ♦ [“GWIA Worksheet” on page 38](#)

Configuring the GWIA

- ☐ In the GroupWise Admin Console > **Internet Agents**, select the GWIA.

- ❑ On the GroupWise > General page (the default page) you can assign a community string to SNMP for enhanced security. SNMP is enabled by default on the GWIA.

The screenshot shows the 'Internet Agent : GWIA' configuration interface. The left sidebar has a 'General' tab selected, with other options like 'Agent Settings', 'Log Settings', 'SSL Settings', 'Time Settings', 'Optional Settings', 'Administrators', and 'Gateway Aliases'. The main content area has several input fields: 'Description' (text box), 'Subdirectory' (dropdown menu showing 'gwia'), 'Time Zone' (dropdown menu showing '(GMT-07:00) Mountain Time (US & Canada)'), 'Platform' (dropdown menu showing 'Linux'), 'Gateway Alias Type' (text box), and 'SNMP Community "Get" String' (text box). Below these fields, the status is 'Running' with a green dot icon, and there is a 'Stop Agent' button and a 'Launch GWIA Console' link. At the bottom of the page are 'Save' and 'Close' buttons.

- ❑ Change to the **Agent Settings** subsection in the GroupWise tab.
- ❑ In the **HTTP** section, specify an **HTTP User Name** and **HTTP Password**. Do not use an eDirectory or Active Directory user name and password for the HTTP User Name and Password.

NOTE: While we recommend you use the default HTTP Port of 9850 and leaving SSL enabled, you can change the HTTP Port and disable SSL if you desire.

- ❑ Change to the **Log Settings** subsection in the **GroupWise** tab. Make sure the **Logging Level** is set to **Verbose**.
- ❑ Change to the **Administrators** subsection in the **GroupWise** tab. You need to add a GWIA Administrator and give them the **Accountant** role. This user receives a file in their email nightly from the GWIA that is used for GWRM reports. The GWRM Control Center checks this mailbox hourly for new files and imports them for reports. We suggest that you create a user for GWRM to use and use the same user for all of your GWIAs. You also need to know the Post Office where this user resides, the Post Office SOAP port, and if SSL is enabled for SOAP.
- ❑ Save the changes to the GWIA.
- ❑ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ☐ Write down the GWRM agent you are going to use to monitor the GWIA, GWIA IP address, HTTP User Name, Password, Port, SSL setting, GWIA Administrator User Name and Password, and GWIA Administrator Post Office IP Address, SOAP port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [GWIA Worksheet](#).
(Optional) If you want GWRM to monitor the GWIA SMTP connection, write down the GWIA SMTP Port and SSL setting along with a test user GWRM can use to connect through SMTP.
- ☐ Repeat the steps above for each GWIA you want to monitor.

Adding the GWIA to GWRM

IMPORTANT: Make sure you have the following information written down on the [GWIA Worksheet](#) before adding the GWIA to GWRM:

- ♦ Name of the GWRM agent you are going to use to monitor the GWIA (usually the one on the GWIA server).
- ♦ GWIA IP address.
- ♦ HTTP User Name, Password, Port, and SSL setting for the GWIA.
- ♦ GWIA Administrator with Accountant role User Name and Password. Post Office IP address, SOAP port, and SOAP SSL setting for the GWIA Administrator.
- ♦ (Optional) The GWIA SMTP port and SSL setting along with a test user that GWRM can use to connect through SMTP to monitor the SMTP connection.

-
- ☐ In the GWRM Control Center > [Dashboard](#) > [Quick Health](#), select the GWRM Agent that you want to use to monitor the GWIA (usually the one installed on the GWIA server) from the GWRM Agent list in the main panel.

- ❑ Go to the **Manage** tab.

The screenshot shows the 'Manage' tab in the GWRM Control Center. At the top, there's a navigation bar with tabs: Summary, Status, Settings, Alerts, Reports, Graphs, Configure, and Manage. Below the navigation bar, the 'Agent Information' section displays 'GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1568), Platform: Linux 64bit 3.0.75-0.11-default, Uptime: 0d 21h 30m'. The 'Monitored Agents' section contains a table with the following data:

Type	Description	Unique ID	Agent Name
HOST	Host	3	-

Below the table is the 'Add or Edit Monitored Agent' form. It includes fields for Agent Type (set to 'GW Post Office Agent'), Status (with an 'Enabled' checkbox), HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL (with a 'Yes' checkbox), Agent Name, and Agent Name Suffix. At the bottom is the 'Connection Test' section, which includes a description: 'The POA will be checked against the SOAP port and a login/logout to the defined account will be done.' and fields for Address, Port, Use SSL, and Username.

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW Internet Agent**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the GWIA IP address, HTTP port, user name, password, and SSL setting.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ Go to GWRM Control Center > **Tracking** > **Tracking Setup**. In the **Gateway Accounting Logfiles** section do the following:
 - ◆ Change the **Status** to **Enabled**.
 - ◆ Specify the Post Office IP Address, SOAP Port, and SSL setting.
 - ◆ Specify the GWIA Administrator user name and password.
- ❑ (Optional) In the **Connection Test** section, you can have GWRM run a regular, automated SMTP connection test to see if SMTP is running on the POA. The connection test runs every 2 minutes. Enter the following for the test to run:
 - ◆ The POA IP address, SMTP Port, and SSL setting.
 - ◆ Specify a test user name and password GWRM can use to test the SMTP connection.
- ❑ Repeat the steps above to add all of the GWIAs you want to monitor to GWRM.

GWIA Worksheet

Use the following worksheet to record the necessary information to be able to add the GWIA to GWRM. Use this worksheet for each GWIA you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the GWIA.
GWIA IP Address		Specify the IP Address of the GroupWise GWIA.
HTTP User Name and Password		Specify the user name and password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. The default is 9850.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.
GWIA Administrator User Name and Password		Specify the user name and password for the GWIA Administrator user with the Accountant role. We recommend you create a user for GWRM and use the same user for all of your GWIAs.
GWIA Administrator Post Office IP Address and SOAP Port		Specify the IP address of the Post Office where the Accountant Administrator user resides and the SOAP Port. If SSL is enabled for SOAP, note that as well.
(Optional) Connection Test		The connection test lets GWRM monitor the SMTP connection on the GWIA. Specify the SMTP connection information along with a test user for GWRM to use to test the connection. The SMTP default port is 25.
♦ GWIA IP Address		
♦ SMTP Port		
♦ SMTP SSL Setting		
♦ SMTP Test user name and password		

GroupWise Document Viewer Agent

Before adding a DVA to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the DVA server. Use the sections below to configure and add the DVA to GWRM to monitor:

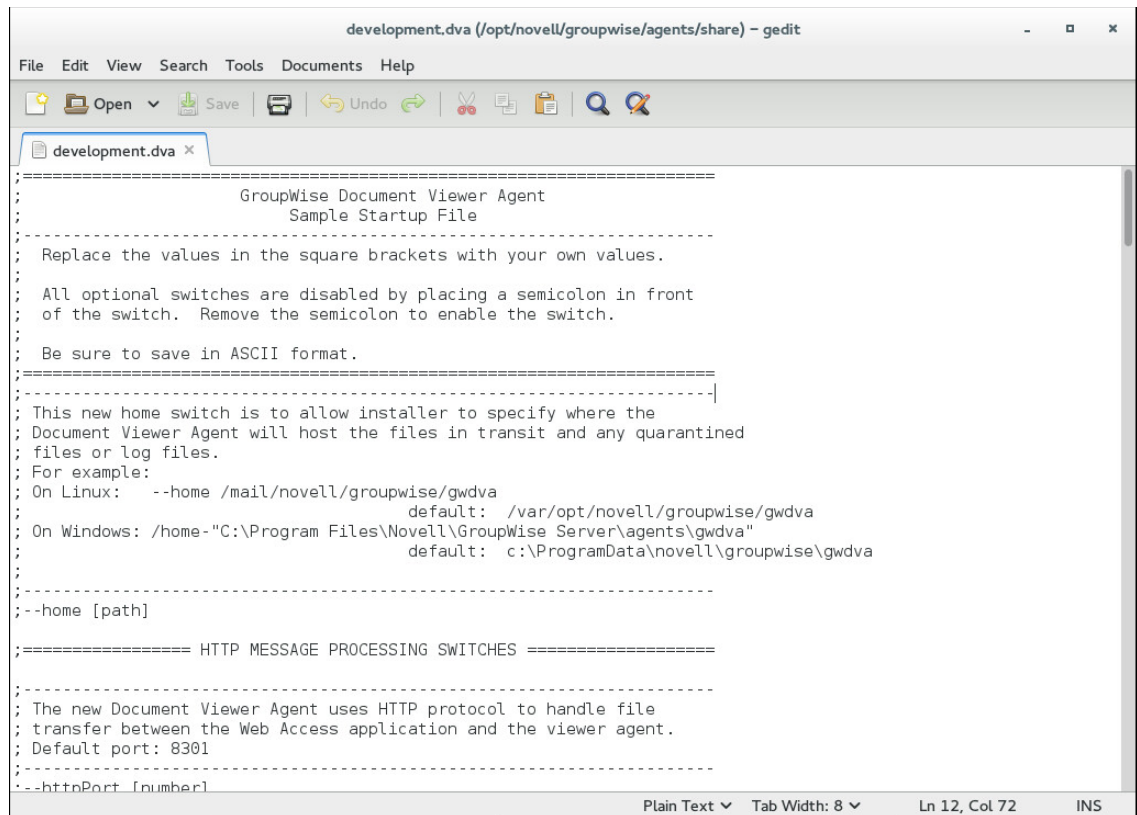
- ◆ “Configuring the DVA” on page 39
- ◆ “Adding the DVA to GWRM” on page 40
- ◆ “DVA Worksheet” on page 42

Configuring the DVA

The Document Viewer Agent (GWDVA) is used to convert attachments for viewing in GroupWise. There is no GroupWise Administration interface for this agent. Instead, you must edit the GWDVA configuration file in a text editor. The file is named after your POA (*poa_name.dva*) and is found on the POA server in the following location:

Linux:	/opt/novell/groupwise/agents/share
Windows:	C:\Program Files\Micro Focus\GroupWise Server\Agents

- ❑ Open the DVA file in an editor on your POA server.



The screenshot shows a text editor window titled "development.dva (/opt/novell/groupwise/agents/share) - gedit". The window contains the following text:

```
=====
GroupWise Document Viewer Agent
Sample Startup File
=====
; Replace the values in the square brackets with your own values.
;
; All optional switches are disabled by placing a semicolon in front
; of the switch. Remove the semicolon to enable the switch.
;
; Be sure to save in ASCII format.
=====
; This new home switch is to allow installer to specify where the
; Document Viewer Agent will host the files in transit and any quarantined
; files or log files.
; For example:
; On Linux:  --home /mail/novell/groupwise/gwdva
;              default: /var/opt/novell/groupwise/gwdva
; On Windows: /home-"C:\Program Files\Novell\GroupWise Server\agents\gwdva"
;              default: c:\ProgramData\novell\groupwise\gwdva
;
; ===== HTTP MESSAGE PROCESSING SWITCHES =====
;
; The new Document Viewer Agent uses HTTP protocol to handle file
; transfer between the Web Access application and the viewer agent.
; Default port: 8301
;
; --httpPort [number]
```

- ☐ Edit the following lines, removing the semicolon (;) at the front of each line:

httpPort	Replace [number] with a port number. We recommend using port 7439.
httpuser	Replace [name] with a user name for the HTTP interface.
httppassword	Replace [password] with a password for the HTTP interface.
loglevel	Replace [Normal Verbose Diagnostic Off] with Verbose.

If you want to configure SSL for the DVA HTTP web console, edit the following lines, removing the semicolon(;) at the front of each line:

https	The semicolon just needs to be removed from the front of the line.
sslCert	Replace [file name] with the path to an SSL Certificate. You can use the same certificate that you are using for the GW POA.
sslKey	Replace [file name] with the path to the SSL key file if your cert uses a key file.
sslKeyPassword	Replace [key password] with the password for your key file.

- ☐ Save the DVA file.
- ☐ Restart the DVA to put the settings into effect.
- ☐ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ☐ Write down the GWRM agent you are going to use to monitor the DVA, DVA IP address, HTTP User Name, Password, Port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [DVA Worksheet](#).
- ☐ Repeat the steps above for each DVA you want to monitor.

Adding the DVA to GWRM

IMPORTANT: Make sure you have the following information written down on the [DVA Worksheet](#) before adding the DVA to GWRM:

- ◆ Name of the GWRM agent you are going to use to monitor the DVA (usually the one on the DVA server).

- ◆ DVA IP address.
- ◆ HTTP User Name, Password, Port, and SSL setting for the DVA.

- ❑ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the DVA (usually the one installed on the DVA server) from the GWRM Agent list in the main panel.
- ❑ Go to the **Manage** tab.

The screenshot shows the 'Manage' tab in the GWRM Control Center. At the top, there are tabs for Summary, Status, Settings, Alerts, Reports, Graphs, Configure, and Manage. Below the tabs, a status bar shows '99.98 %' and 'GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1558), Platform: Linux 64bit 3.0.76-0.1'. The main content area is divided into two sections: 'Agent Information' and 'Monitored Agents'. The 'Monitored Agents' section contains a table with columns 'Type', 'Description', 'Unique ID', and 'Agent'. Below this, the 'Add or Edit Monitored Agent' form is visible, featuring fields for Agent Type (set to 'GW DocView Agent'), Status (with an 'Enabled' checkbox), HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL (with a 'Yes' checkbox), Agent Name, and Agent Name Suffix. An 'OK' button is at the bottom of the form.

Type	Description	Unique ID	Agent
HOST	Host	3	-

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW DocView Agent**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the DVA IP address, HTTP port, user name, password, and SSL setting.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ Repeat the steps above to add all of the DVAs you want to monitor to GWRM.

DVA Worksheet

Use the following worksheet to record the necessary information to be able to add the DVA to GWRM. Use this worksheet for each DVA you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the DVA.
DVA IP Address		Specify the IP Address of the GroupWise DVA.
HTTP User Name		Specify the user name entered for the HTTP web console in GroupWise.
HTTP Password		Specify the password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. We recommend 7439.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.

GroupWise WebAccess Application

Before adding a WebAccess Application to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the WebAccess server. Use the sections below to configure and add the WebAccess Application to GWRM to monitor:

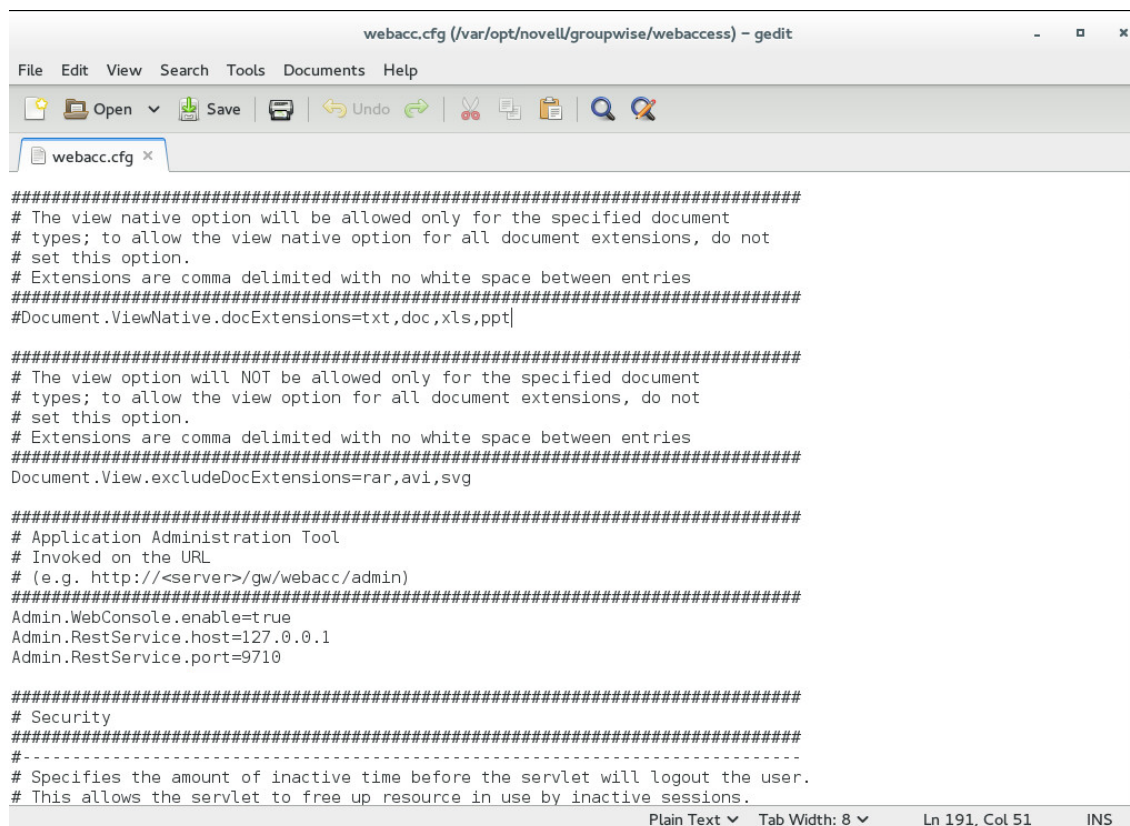
- ♦ [“Configuring the WebAccess Application” on page 43](#)
- ♦ [“Adding the WebAccess Application to GWRM” on page 44](#)
- ♦ [“WebAccess Application Worksheet” on page 46](#)

Configuring the WebAccess Application

There is no GroupWise Administration interface for the WebAccess Application. Instead, you must edit the `webacc.cfg` file in a text editor. It is found on the WebAccess server in the following location:

Linux:	<code>/var/opt/novell/groupwise/webaccess/</code>
Windows:	<code>C:\Program Files\Micro Focus\webaccess</code>

- ☐ Open the `webacc.cfg` file in an editor on your WebAccess server.

A screenshot of a text editor window titled 'webacc.cfg (/var/opt/novell/groupwise/webaccess) - gedit'. The window shows the contents of the webacc.cfg file, which is a configuration file for the WebAccess application. The file contains several sections of comments and configuration parameters. The visible text includes: '#####', '# The view native option will be allowed only for the specified document', '# types; to allow the view native option for all document extensions, do not', '# set this option.', '# Extensions are comma delimited with no white space between entries', '#####', '#Document.ViewNative.docExtensions=txt,doc,xls,ppt|', '#####', '# The view option will NOT be allowed only for the specified document', '# types; to allow the view option for all document extensions, do not', '# set this option.', '# Extensions are comma delimited with no white space between entries', '#####', 'Document.View.excludeDocExtensions=rar,avi,svg', '#####', '# Application Administration Tool', '# Invoked on the URL', '# (e.g. http://<server>/gw/webacc/admin)', '#####', 'Admin.WebConsole.enable=true', 'Admin.RestService.host=127.0.0.1', 'Admin.RestService.port=9710', '#####', '# Security', '#####', '# Specifies the amount of inactive time before the servlet will logout the user.', '# This allows the servlet to free up resource in use by inactive sessions.', '#####'. The editor's status bar at the bottom indicates 'Plain Text', 'Tab Width: 8', 'Ln 191, Col 51', and 'INS'.

- ☐ Edit the following lines:

<code>Admin.WebConsole.enable=false</code>	Change <code>false</code> to <code>true</code> .
<code>Log.level=normal</code>	Change <code>normal</code> to <code>verbose</code> .
<code>httppassword</code>	Replace <code>[password]</code> with a password for the HTTP interface.

- ☐ Save the `webacc.cfg` file.
- ☐ Restart GroupWise tomcat to put the settings into effect.
- ☐ GWRM needs to use a GroupWise Administrator user to login to the WebAccess HTTP web console. You can either create a new account for GWRM to use or identify a GroupWise Admin account that you already have that you can use.

- ❑ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:webaccess_port/gw/webacc?action=Admin.Open`.
- ❑ Write down the GWRM agent you are going to use to monitor WebAccess, WebAccess IP address, WebAccess port, SSL setting, GroupWise Admin User Name, and Password to enter into GroupWise Reporting and Monitoring on the [WebAccess Application Worksheet](#). If you are using GW 18.0.1 or later, SSL is required for WebAccess. Earlier versions did not require SSL.
(Optional) If you want GWRM to monitor the WebAccess SOAP connection, write down the WebAccess SOAP Port and SSL setting along with a test user GWRM can use to connect through SOAP.

NOTE: All of these values (besides the GroupWise Admin user name and password) can be found in the `webacc.cfg` file.

- ❑ Repeat the steps above for each WebAccess Application you want to monitor.

Adding the WebAccess Application to GWRM

IMPORTANT: Make sure you have the following information written down on the [WebAccess Application Worksheet](#) before adding the WebAccess Application to GWRM:

- ♦ Name of the GWRM agent you are going to use to monitor WebAccess (usually the one on the WebAccess server).
- ♦ WebAccess IP address, Port, and SSL setting.
- ♦ GroupWise Admin User Name and Password.
- ♦ (Optional) The WebAccess IP address, SOAP port, and SSL setting along with a test user that GWRM can use to connect through SOAP to monitor the SOAP connection.

-
- ❑ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the WebAccess Application (usually the one installed on the WebAccess server) from the GWRM Agent list in the main panel.

- ❑ Go to the **Manage** tab.

The screenshot shows the GWRM Manage tab interface. At the top, there's a navigation bar with tabs: Summary, Status, Settings, Alerts, Reports, Graphs, Configure, and Manage. Below the navigation bar, a status bar shows a green progress indicator at 99.98% and the text 'GW WebAccess: RLAgent-prv-gwdoc4, Version: 18.0.0 (1568), Platform: Linux 64bit 3.0.76-0.11-default'.

The main content area is divided into sections:

- Agent Information:** A section with a 'Description' field containing 'Global Unique ID (GUID)'.
- Monitored Agents:** A table listing monitored agents.

Type	Description	Unique ID	Agent Name
HOST	Host	3	-
WEBAC2	GW WebAccess	4	-
- Add or Edit Monitored Agent:** A form for adding or editing an agent.
 - Agent Type: **GW WebAccess** (dropdown menu)
 - Status: ☒ **Enabled**
 - HTTP Address: **137.65.67.218**
 - HTTP Port: **443**
 - HTTP Username: **admin**
 - HTTP Password: *********
 - Use SSL: ☒ **Yes**
 - Agent Name: (empty text field)
 - Agent Name Suffix: (empty text field)
- Connection Test:** A section for testing the connection.
 - The WebAccess test will do a web based login to the defined account. Default is Port 80.
 - Address: (empty text field)
 - Port: (empty text field)
 - Use SSL: ☐
 - Username: (empty text field)

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW WebAccess**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the WebAccess IP address, port, SSL setting and GroupWise Admin user name, password.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ (Optional) In the **Connection Test** section, you can have GWRM run a regular, automated SOAP connection test to see if SOAP is running on the WebAccess Application. The connection test runs every 2 minutes. Enter the following for the test to run:
 - ◆ The WebAccess IP address, SOAP Port, and SSL setting.
 - ◆ Specify a test user name and password GWRM can use to test the SOAP connection.
- ❑ Repeat the steps above to add all of the WebAccess Applications you want to monitor to GWRM.

WebAccess Application Worksheet

Use the following worksheet to record the necessary information to be able to add the DVA to GWRM. Use this worksheet for each DVA you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the WebAccess Application.
WebAccess IP Address		Specify the IP Address of the GroupWise WebAccess Application.
GroupWise Admin User Name		Specify the GroupWise Admin user name.
GroupWise Admin Password		Specify the GroupWise Admin password.
WebAccess Port		Specify the WebAccess port.
WebAccess SSL Setting		Specify the SSL setting WebAccess.
(Optional) Connection Test		The connection test lets GWRM monitor the SOAP connection to the WebAccess Application.
♦ WebAccess IP Address		Specify the SOAP connection information along with a test user for GWRM to use to test the connection. The SOAP information can be found in the <code>webacc.cfg</code> file under <code>Provider.SOAP</code> .
♦ SOAP Port		
♦ SOAP SSL Setting		
♦ SOAP Test user name and password		

GroupWise Messenger Agents

- ♦ [“GroupWise Messenger Messaging Agent” on page 46](#)
- ♦ [“GroupWise Messenger Archive Agent” on page 49](#)

GroupWise Messenger Messaging Agent

Before adding a Messenger Messaging Agent to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the Messaging Agent server. Use the sections below to configure and add the Messaging Agent to GWRM to monitor:

- ♦ [“Configuring the Messaging Agent” on page 47](#)
- ♦ [“Adding the Messaging Agent to GWRM” on page 48](#)
- ♦ [“Messaging Agent Worksheet” on page 49](#)

Configuring the Messaging Agent

- ❑ In the GroupWise Admin Console > **Messenger** > **MessengerService** > **Objects** tab > **Messaging Agents**, verify that **Enable SNMP** is checked on the General tab. select the Messaging Agent and go to the **Agent Settings** tab.

Messaging Agent : prv-gwdoc6Server_MessagingAgent

General Agent Settings Log Settings SSL Settings

Name: prv-gwdoc6Server_MessagingAgent

Description:

Version: 18.1.0

Work Path: /var/opt/novell/messenger/temp

☒ Enable Messenger Services

☒ Enable SNMP

Restart Agent

Save Close

- ❑ Switch to the Agent Settings tab.
- ❑ In the **HTTP** section, specify and **HTTP User Name** and **HTTP Password**. Do not use an eDirectory or Active Directory user name and password for the HTTP User Name and Password. We recommend that you enable SSL for the HTTP web console.

NOTE: While we recommend you use the default HTTP Port of 8311 and enabling SSL, you can change the HTTP Port and leave SSL disabled if you desire.

- ❑ Change to the **Log Settings** tab. Make sure the **Logging Level** is set to **Verbose**.
- ❑ Save the changes to the Messaging Agent.
- ❑ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ❑ Write down the GWRM agent you are going to use to monitor the Messaging Agent, Messaging Agent IP address, HTTP User Name, Password, Port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [Messaging Agent Worksheet](#).
- ❑ Repeat the steps above for each Messaging Agent you want to monitor.

Adding the Messaging Agent to GWRM

IMPORTANT: Make sure you have the following information written down on the [Messaging Agent Worksheet](#) before adding the Messaging Agent to GWRM:

- ◆ Name of the GWRM agent you are going to use to monitor the Messaging Agent (usually the one on the Messaging Agent server).
- ◆ Messaging Agent IP address.
- ◆ HTTP User Name, Password, Port, and SSL setting for the Messaging Agent.

- ❑ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the Messaging Agent (usually the one installed on the Messaging Agent server) from the GWRM Agent list in the main panel.
- ❑ Go to the **Manage** tab.

The screenshot shows the 'Manage' tab in the GWRM Control Center. At the top, there are tabs for Summary, Status, Settings, Alerts, Reports, Graphs, Configure, and Manage. Below the tabs, a status bar shows 'GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1568), Platform: Linux 64bit 3.0.7' with a 99.99% CPU usage indicator. The main content area is divided into sections: 'Agent Information' (with a description and Global Unique ID), 'Monitored Agents' (a table with columns Type, Description, Unique ID, and Actions), and 'Add or Edit Monitored Agent' (a form with fields for Agent Type, Status, HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL, Agent Name, and Agent Name Suffix, plus an OK button).

Type	Description	Unique ID	Actions
HOST	Host	3	-

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW Messenger Agent**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the Messaging Agent IP address, HTTP port, user name, password, and SSL setting.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ Repeat the steps above to add all of the Messaging Agents you want to monitor to GWRM.

Messaging Agent Worksheet

Use the following worksheet to record the necessary information to be able to add the Messaging Agent to GWRM. Use this worksheet for each Messaging Agent you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the Messaging Agent.
Messaging Agent IP Address		Specify the IP Address of the GroupWise Messaging Agent.
HTTP User Name		Specify the user name entered for the HTTP web console in GroupWise.
HTTP Password		Specify the password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. The default is 8311.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.

GroupWise Messenger Archive Agent

Before adding a GroupWise Messenger Archive Agent (Archive Agent) to GroupWise Reporting and Monitoring (GWRM), you must have a GWRM agent installed on the Archive Agent server. Use the sections below to configure and add the Archive Agent to GWRM to monitor:

- ♦ [“Configuring the Archive Agent” on page 50](#)
- ♦ [“Adding the Archive Agent to GWRM” on page 50](#)
- ♦ [“Archive Agent Worksheet” on page 51](#)

Configuring the Archive Agent

- ❑ In the GroupWise Admin Console > **Messenger** > **MessengerService** > **Objects** tab > **Archive Agents**, select the Archive Agent. Verify that **Enable SNMP** is checked on the General tab.

Archive Agent : prv-gwdoc6Server_ArchiveAgent

General Agent Settings Log Settings SSL Settings File Module Retain Settings

Name: prv-gwdoc6Server_ArchiveAgent

Description:

Version: 18.1.0

Work Path: /var/opt/novell/messenger/temp

☒ Enable Messenger Services

☒ Enable SNMP

Restart Agent

Save Close

- ❑ Switch to the Agent Settings tab.
- ❑ In the **HTTP** section, specify and **HTTP User Name** and **HTTP Password**. Do not use an eDirectory or Active Directory user name and password for the HTTP User Name and Password. We recommend that you enable SSL for the HTTP web console.

NOTE: While we recommend you use the default HTTP Port of 8313 and enabling SSL, you can change the HTTP Port and leave SSL disabled if you desire.

- ❑ Change to the **Log Settings** tab. Make sure the **Logging Level** is set to **Verbose**.
- ❑ Save the changes to the Archive Agent.
- ❑ In a new web browser tab, test the HTTP web console setting by going to `https://server_ip_address:http_port`. Make sure you can login with the user name and password you specified.

NOTE: Use `http` if you do not have SSL enabled for the HTTP web console.

- ❑ Write down the GWRM agent you are going to use to monitor the Archive Agent, Archive Agent IP address, HTTP User Name, Password, Port, and SSL setting to enter into GroupWise Reporting and Monitoring on the [MTA Worksheet](#).
- ❑ Repeat the steps above for each Archive Agent you want to monitor.

Adding the Archive Agent to GWRM

IMPORTANT: Make sure you have the following information written down on the [Archive Agent Worksheet](#) before adding the Archive Agent to GWRM:

- ♦ Name of the GWRM agent you are going to use to monitor the Archive Agent (usually the one on the Archive Agent server).

- ◆ Archive Agent IP address.
- ◆ HTTP User Name, Password, Port, and SSL setting for the Archive Agent.

- ❑ In the GWRM Control Center > **Dashboard** > **Quick Health**, select the GWRM Agent that you want to use to monitor the Archive Agent (usually the one installed on the Archive Agent server) from the GWRM Agent list in the main panel.
- ❑ Go to the **Manage** tab.

The screenshot shows the 'Manage' tab in the GWRM Control Center. At the top, there's a status bar with '99.99%' and 'GWRM Agent: RLAgent-prv-gwdoc4, Version: 18.0.0 (1558), Platform: Linux 64bit 3.0.78-0.11'. Below this is the 'Agent Information' section with fields for 'Description' and 'Global Unique ID (GUID)'. The 'Monitored Agents' section contains a table with columns 'Type', 'Description', 'Unique ID', and 'Agent Name'. The table has one row: 'HOST', 'Host', '3', and '-'. Below the table is the 'Add or Edit Monitored Agent' section with various input fields: 'Agent Type' (dropdown menu showing 'GW Messenger Arch Agent'), 'Status' (checkbox for 'Enabled'), 'HTTP Address', 'HTTP Port', 'HTTP Username', 'HTTP Password', 'Use SSL' (checkbox for 'Yes'), 'Agent Name', and 'Agent Name Suffix'. An 'OK' button is at the bottom.

- ❑ In the **Add or Edit Monitored Agent** section, do the following:
 - ◆ Change the **Agent Type** to **GW Messenger Arch Agent**.
 - ◆ Enable the agent in the **Status** field.
 - ◆ Enter the Archive Agent IP address, HTTP port, user name, password, and SSL setting.
 - ◆ (Optional) Specify an alias for the agent in GWRM using the Agent Name and Agent Name Suffix fields.
- ❑ Repeat the steps above to add all of the Archive Agents you want to monitor to GWRM.

Archive Agent Worksheet

Use the following worksheet to record the necessary information to be able to add the MTA to GWRM. Use this worksheet for each Archive Agent you want to monitor using GWRM.

Key	Value	Explanation
GWRM Agent		Specify the GWRM agent to monitor the Archive Agent.

Key	Value	Explanation
Archive Agent IP Address		Specify the IP Address of the GroupWise Archive Agent.
HTTP User Name		Specify the user name entered for the HTTP web console in GroupWise.
HTTP Password		Specify the password entered for the HTTP web console in GroupWise.
HTTP Port		Specify the port for the HTTP web console in GroupWise. The default is 8313.
HTTP SSL Setting		Specify the SSL setting for the HTTP web console in GroupWise. We recommend you leave SSL enabled.

GroupWise Disaster Recovery

GroupWise Disaster Recovery (GWDR) powered by Reload is a tool for backing up, and accessing multiple data sets of your post offices on NetWare, Linux, and Windows. GWDR creates 'Hot Backups' that can be accessible to a GroupWise client within minutes.

To configure GWDR to operate with GWRM, administrators should know the IP address and port of the GWDR server's HTTP/HTTPS monitoring port. GWDR has everything you need for GWRM automatically available, and you don't need to configure anything in GWDR.


For full monitoring capabilities and reports, you need to run a GWRM Agent on the GWDR box, because it needs access to some log files.


From the GWRM Control Center, go to the System View and pick the GWRM Agent which will monitor the GWDR Agent. Specify IP address and port of your GWDR server. Username and password only are utilized if GWDR has been configured to require authentication for the web user interface.

After 2-3 minutes, a message should appear on the GWRM Agent that the GWDR agent has been registered to the Control Center and shows up in the Control Center.

GroupWise Forensics

GroupWise Forensics is a powerful tool for examining the contents of a live GroupWise system and a GroupWise Disaster Recovery System. Authorized administrators may access any mailbox without special rights. To enable auditing security, GroupWise Forensics provides an option to produce auditing information and send it to the GWRM Control Center automatically.

 GroupWise Forensics ×

 **Configure auditing**
GroupWise Forensics will not work without proper auditing. This, to enforce existing business and legal policies.

Decide which auditing method to use

☐ Use GW Reporting & Monitoring for auditing. If it becomes unavailable, auto-fallback to textfile auditing.


☐ Use GW Reporting & Monitoring for auditing. If it becomes unavailable, shutdown GroupWise Forensics.


☒ Use simple textfile auditing only.


Note: If no auditing is possible, GroupWise Forensics will shutdown immediately!

Configure GW Reporting & Monitoring (Redline) auditing settings

Server IP address:


Server port: 


Server timeout (ms): 


Registration name: 

Registration code:

Configure textfile auditing settings

Auditing directory: 

Maximum logfile size (kb): 

Minimum free disk space (MB): 

Note: Make sure users have read/write access to the chosen auditing directory.

After GWRM is installed, in GWRM, go to Administration/Auditing Settings, and click the Lookup button. Provide the path to RLCENTER.CONF file of the server running the GWRM Control Center. This is typically in /opt/beginfinite/redline/conf and should automatically populate the rest of the page. Otherwise one must manually enter information such as the GWRM Control Center IP Address and Port, as well the Registration Name and Code for GWRM.

Reveal can automatically communicate directly with the GWRM Control Center. It does not need to use a GWRM Agent at all.

GroupWise Mailbox Management

GWRM monitoring in GroupWise Mailbox Management (GWMM) is accomplished without any GWRM agent. GWMM reports and connects directly to GWRM. All configuration required for GWMM monitoring is contained inside GWMM.

To configure GWMM to connect to GWRM:

- ♦ Start GWMM and connect to the GroupWise system.
- ♦ Select 'Auditing' from the 'Settings' menu.
- ♦ From the 'Configure Auditing' menu, select the desired one of the two options:
 1. Use GWRM for Auditing. If unavailable, auto fall-back to text auditing.
 2. Use GWRM for Auditing. If unavailable, shutdown GWMM.

Configure Auditing

Configure auditing
GroupWise Mailbox Management can store an audit trail in in order to enforce existing business and legal policies.

Decide which auditing method to use

☐ Use GWRM for auditing. If unavailable, auto-fallback to textfile auditing.

☐ Use GWRM for auditing. If unavailable, shutdown GroupWise Mailbox Management.

☐ Use simple textfile auditing only. If unavailable, shutdown GroupWise Mailbox Management.

☒ No Auditing

Configure GWRM auditing settings

Server DNS name or IP address:

Server port:

Server timeout (ms):

Registration details:

Registration name:

Registration code:

Configure textfile auditing settings

Auditing directory:

Maximum logfile size (MB):

Minimum free disk space (MB):

Ok Cancel

- ♦ Enter the IP address or host name of the GWRM Server
- ♦ Select the port that the Control Center is currently listening on (default port 6900)

- ♦ Specify the timeout, set in number of seconds (300 is default and recommended)
- ♦ The registration must match the registration code and company name configured in GWRM. (The registration code and name is used by the Control Center to communicate with agents.)

The registration may be configured in two different methods: automatic, or manual. If manual: input the registration code and company name, leaving the registration details blank. If automatic: upload the `rlcenter.conf` file from the Control Center by using the browse button on the 'registration details' line. The correct information will be added automatically.

After filling out registration, GWMM will register and appear in GWRM automatically.

Micro Focus Retain

Retain is an archiving solution for GroupWise, which is based on two components: Retain Server and Retain Worker. Both components can be monitored with GWRM, and all you need to do is enable monitoring in GWRM.

Because Retain is a Java application and uses Tomcat for the web interface, you need to use port 48080 for monitoring. Specify IP address, port, username and password.

After 2-3 minutes, a message should appear on the GWRM Agent that the Retain Server or Worker has been registered to the Control Center and shows up in the Control Center. Make sure to configure both, Retain Server and Worker separately in GWRM.

GWAVA 6.5 and Secure Messaging Gateway

GWAVA 6.5 and Secure Messaging Gateway (SMG) are entirely web based and all that is necessary is to create an administrator account for GWRM. Log into the web interface, go to System Management/Administrator accounts and specify the new username and password.

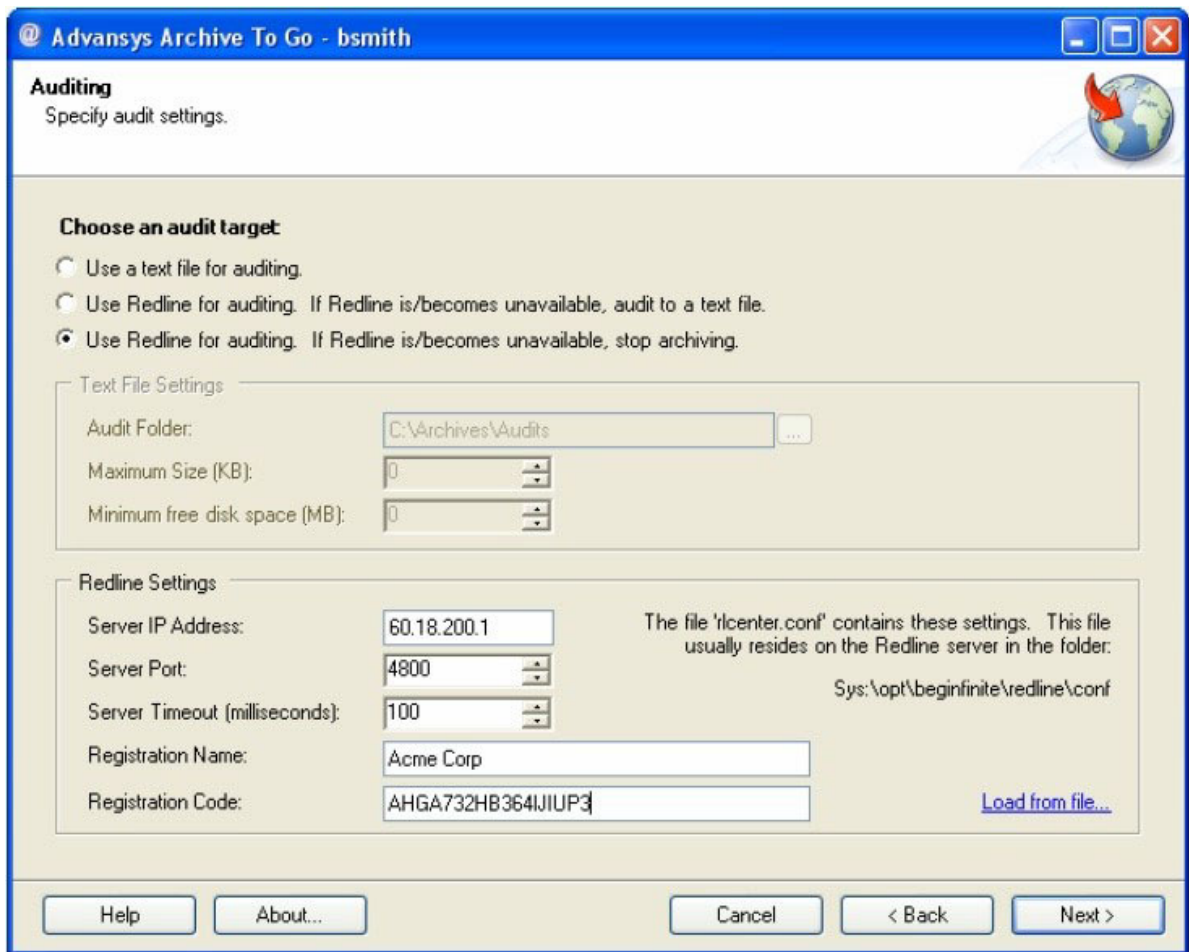
From the GWRM Control Center, go to the System View and pick the GWRM Agent which will monitor the SMG agent. Specify the IP address, port, username and password. SMG requires a username and a password.

After 2-3 minutes, a message should appear on the GWRM Agent that the SMG agent has been registered to the Control Center and shows up in the Control Center.

Advansys Archive2Go

Archive2Go from Advansys is one of the Applications which does not require a GWRM Agent. It talks directly to the Control Center. GWRM is used as the auditing tool for Archive2Go in order to meet requirements enforced by laws or other regulations.

Choose an option for auditing the archiving process in the auditing dialog.



There are two ways where GWRM is involved in the auditing process. One is where auditing to GWRM is enforced, and Archive2Go doesn't work if GWRM is not available, and another option where auditing can fall back to a text file as soon as GWRM is not available.

It is important to specify the Control Center IP Address, Port, Registration Name and Registration Code. You can find this information in the GWRM Control Center Configuration/License tab.

Blackberry Enterprise Server

The BlackBerry Enterprise Server components can be installed on one server, or on multiple servers. Obviously, the installation and configuration of BlackBerry servers and clients are beyond the scope of this manual; some basic GroupWise requirements for BES are:

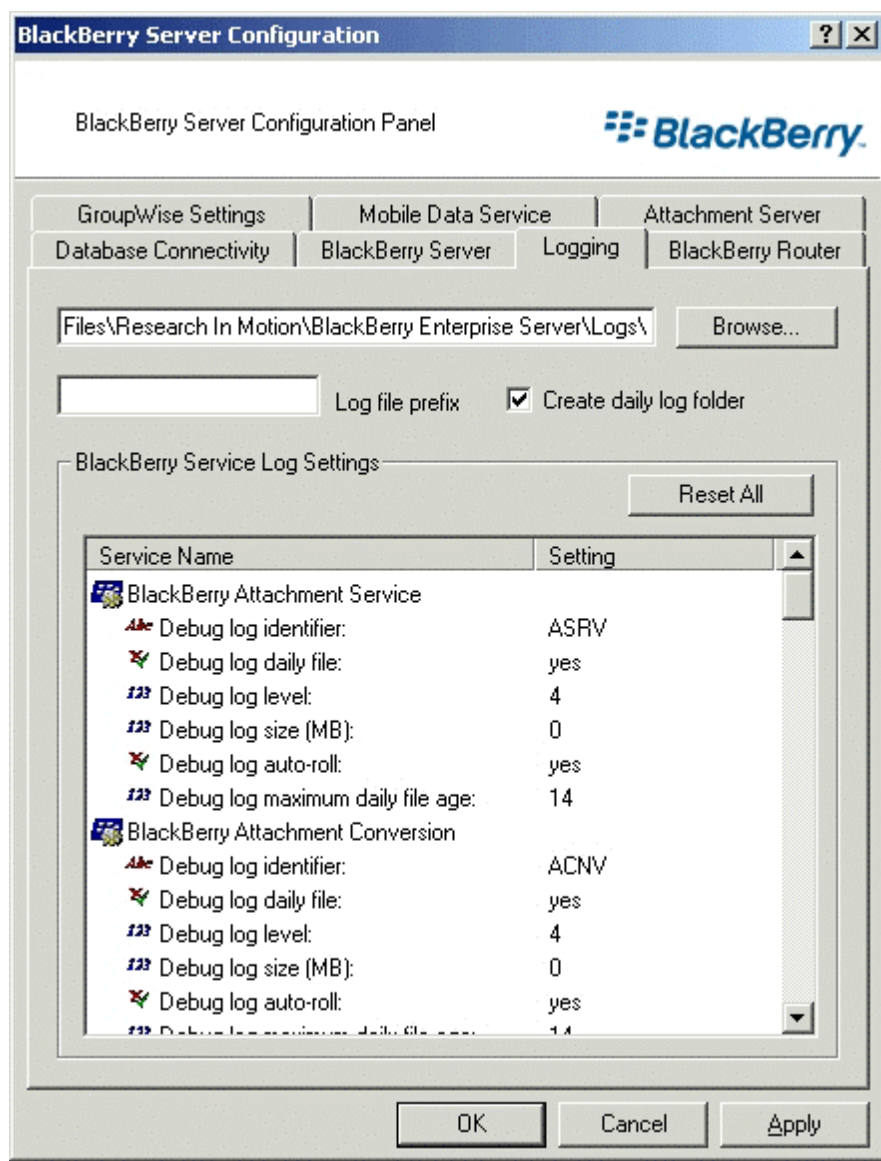
GroupWise Requirements

- ♦ Novell GroupWise system version 6.5 SP1 or later for post offices containing BlackBerry users. The GroupWise system must be installed on a computer different than the computer running the BlackBerry Enterprise Server.

- ♦ A trusted application key is generated to enable communication between the BlackBerry Enterprise Server and the primary domain of the GroupWise system. The trusted application key is used by subsequent secondary domains. If there are multiple BlackBerry Enterprise Servers in a BlackBerry Domain, each BlackBerry Enterprise Server uses the same trusted application key to access GroupWise.
- ♦ The trusted application key must be provided during the BlackBerry Enterprise Server installation. If a new trusted application key is generated after installing the BlackBerry Enterprise Server, update the BlackBerry Enterprise Server configuration with the new key.

Configuring Blackberry Enterprise Server

In the Windows Control Panel, select the BlackBerry Server Configuration panel. Note the Logs directory shown at the top. This is the location that must be specified as the PATH parameter in GWRM.



Leave Log File Prefix blank, and ensure the Create Daily Log Folders check box is enabled

Scroll through the BlackBerry Service Log Settings and set the various services as follows:

- ♦ Debug log identifier -Leave unchanged
- ♦ Debug log daily file - Yes
- ♦ Debug log level - 4
- ♦ Debug Log Size (MB) - 0 (unlimited size)
- ♦ Debug log auto-roll - Yes
- ♦ Debug log maximum daily file age - 7-14 days (0 keeps logs forever)

Reboot the BES server. The log file settings take effect only after reboot, or after restarting all BlackBerry services.

From the GWRM Control Center, go to the System View and pick the GWRM Agent which will monitor the Blackberry Enterprise Server. Specify the path to the log folder.

After 2-3 minutes, a message should appear on the GWRM Agent that the Blackberry Enterprise server has been registered to the Control Center and shows up in the Control Center.