



Redline 4

Installation Guide

© 2012 GWAVA Inc.

Contents

Minimum System Requirements	5
Installation	6
How Redline Works	6
Recommended Implementation of Redline	6
Linux Installation.....	6
RPM Installation	7
Install with the tar.gz file.....	7
Start Control Center on Linux.....	9
Start Agent on Linux	10
Linux Cluster Installation	11
NetWare Installation	12
The Windows Installer.....	12
The NetWare Install Script.....	14
Install Control Center to a non SYS Volume on NetWare	16
Start Control Center on NetWare.....	17
Start Agent on NetWare	18
Netware Cluster Installation.....	20
Control Center	20
Agent	21
Windows Installation.....	23
Start Redline on Windows	24
Multiple Redline Agents on Windows	25
Access Control Center	26
Install License	27
Update Redline	28
Uninstall Redline.....	28
NetWare	28
Windows.....	28
Linux	28
Configure Redline Agent; Monitor GroupWise	29
Advansys Archive2Go	30
GroupWise API Gateway	31
GroupWise Async Gateway	32
GroupWise Document Viewer Agents (GroupWise 8 and 2012)	34
GroupWise Message Transfer Agent.....	36

GroupWise Exchange Gateway	38
GroupWise Internet Agent (GWIA).....	40
Novell Messenger Agent	42
Novell Messenger Archive Agent	44
GroupWise Mobile Server	46
GroupWise Notes Gateway	48
GroupWise Post Office Agent.....	50
GWCHECK Scheduled Events in the GroupWise POA.....	52
Creating the GWCHECK events.....	53
Audit Report (GWAUDIT.LOG).....	54
Mailbox Statistics (GWSTATS.LOG).....	54
Mailbox analysis (MBSTATS.LOG).....	55
GroupWise WebAccess Agent	56
GroupWise WebAccess Application	58
GroupWise WebAccess 2012.....	59
GWAVA 4x / 5x / 6x	60
GWAVA Reload.....	61
GWAVA Retain.....	62
GWAVA Reveal	63
Host Platform.....	64
NotifyLink 4.....	65
Blackberry Enterprise Server	66
Vertigo	68
Appendix.....	69
POSIX, UNC, and NetWare Paths.....	69
NetWare and POSIX Path Conversion	70
How is this relevant to Redline?.....	71
Installation Worksheet	72

This manual is intended for IT administrators in their use of Redline or anyone wanting to learn more about Redline. It includes installation instructions for various scenarios.

Technical Support

If you have a technical support question, please consult the GWAVA Technical Support section of our website at www.gwava.com. For technical support, call 801-437-5678.

Sales

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

Suite 500, 100 Alexis Nihon Blvd., Montreal, Quebec, H4M 2P1, Canada

About Redline

Redline is a reporting and monitoring solution for Novell 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. Redline produces reports for system analysis, capacity planning, and security auditing.

Obtaining Redline

Redline can be downloaded for trial at the main GWAVA website: www.gwava.com

Or the direct link to the download form http://www.gwava.com/trial_downloads.php

Copyright Notices

The content of this manual is for informational use only and may change without notice. Beginfinite Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation. GroupWise and 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 gdttf.c copyright 1999, 2000, 2001, 2002, 2003, 2004 John Ellson (ellson@graphviz.org)
- Portions relating to gdfc.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.

Minimum System Requirements

Core Requirements:

GroupWise 5.5EP, 6.0, 6.5, 7, 8, 2012 (GW 7 or later is recommended for full functionality)

Agent: 10MB Hard Drive Space and 5MB free system memory.

Control Center: Minimum 30 MB Hard Drive Space. DB storage will require additional space, (see specific instructions below).

—There is a bug in GroupWise 6.5 SP2 preventing correct operation of Redline. This version is NOT supported.—

Specific Operating System requirements:

Netware: NW 6.5 with SP 6 --Older NetWare systems which may work but are no longer tested or supported: 5.1 with SP 8; 6.0 with SP5 and the latest FTF LibC update

Linux: SLES 10 all SP on 32/64 bit; SLES 11 32/64 bit; Linux OES2 32/64 bit

For all Linux systems, the EXT3 file system is highly recommended.

Windows: Windows 2000 SP4, 2003, 2008

Servers running the Redline Control center should have free memory based on this calculation:

40MB + 4MB for every agent + largest GWCheck file * 1.5. Example:

A system with 100 GW Agents registered and GWCheck file with up to 1GB:

$40MB + (100 * 4) + (1000 * 1.5) = 1940MB$.

Ensure the system has enough disk space for the Control Center database. The DB can grow to several GB depending on how the GroupWise system is used.

Supported internet browser

IE, Firefox, Safari, Chrome

It is recommended, that wherever possible, the Redline Control Center be run from a dedicated server.

The following component integrations are supported

- GroupWise Exchange Gateway
- GroupWise Notes Gateway
- GroupWise API Gateway
- GroupWise Messenger 1.0 SP4 or higher
- GroupWise Messenger Archive Agent 1.0 SP4 or higher
- GWAVA 4/5/6
- GWAVA Reveal 1.1 +
- GWAVA Reload 1.x and 2.x
- GroupWise Message Transfer Agent
- GroupWise Post Office Agent
- GroupWise Internet Agent
- GroupWise WebAccess Agent
- GroupWise Document Viewer Agent
- GroupWise WebAccess Application
- GroupWise Mobile Server 2 and 3 (Windows and Linux)
- GroupWise Async Gateway 2.0
- BlackBerry Enterprise Server 4.0 SP2, and 5x
- GWAVA Retain Server and Worker
- GWAVA Vertigo
- Notifylink 4
- Advansys Archive 2 Go
- Linux, NetWare and Windows Host
- Redline Self-monitoring including the Redline Database

Installation

The Redline Installation copies the files needed for both the Redline Control Center and the Redline Agent, but the configuration and startup are different for both. To install either, running the single install on Linux and Netware will install all Redline components.

The simplest way to install and configure Redline is to follow three steps:

1. Copy over and install Redline
2. Open the appropriate configuration file in the preferred editor. Remove the 'new install' line from the Redline Agent configuration file, enter the company name and create a registration code. (The company name and registration code is used to communicate between agents and the Control Center. It can be any created code.)
3. Start the Control Center and then the agents individually. Check to ensure that the agents have connected and are reporting to the Control Center. It is recommended to start the agents one at a time then to check for them in the Control Center to avoid confusion.

All additional configuration of the Redline agent for different monitored elements may be completed through the Control Center from the system view tab.

How Redline Works

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

Redline works to monitor systems with two different parts: the Control Center, and the Agent. 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. For a further discussion on the function of Redline, see the Administration Guide.

Recommended Implementation of Redline

The optimal setup for Redline, which should be used in all setups except perhaps the smallest systems, consists of the Redline 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 Redline Control Center as a standalone dedicated server, separate from the monitored system or systems. For specific questions on placement in a clustered environment, contact GWAVA Support. In the move to full 64-bit support for both Windows and Linux for the Control Center, it is recommended to move Redline to a dedicated 64-bit server.

Windows, Linux, and NetWare agents will still be able to be installed and connect to the Redline Control Center, and having the server separate from the monitored system supports the integrity of the reporting scheme in case of a monitored system failure.

Linux Installation

Redline provides a RPM file for automatic installation and update and a tar.gz file for manual installation.

With the RPM file you need root access during installation. It is possible to run Redline as a user as well. Redline ships in 2 versions for Linux: 32-bit and 64-bit versions, ensure that you use the appropriate version for your installation.

RPM Installation

- Login as root or use su to switch to root.

```
gwava@linux-o3in:/root> su
Password:
```

- Go to the folder where Redline was unpacked. Here go to the subfolder linux.suse64/redline. (Or linux.suse32/redline as system appropriate

```
-rw-r--r-- 1 gwava users 4898866 Oct  3 09:28 redline-4.0.0-1.i586.rpm
-rw-r--r-- 1 gwava users 5087794 Oct  3 09:28 redline.tar.gz
gwava@redline4:~/Desktop/redline400-1016/redline/linux.suse32/redline>
```

- Install the RPM with the rpm command: rpm -U redline-<version number>-1.<platform>.rpm i.e.

```
rpm -U redline-4.0.0-1.i586.rpm
```

- If you see errors that some xml or html files conflict, Install the RPM with the rpm command:

```
rpm -U --force redline-4.0.0-1.i586.rpm
```

RLCENTER and RLAGENT startup scripts will automatically be copied to /etc/init.d and set up with the appropriate run level symbolic links

Install with the tar.gz file

- Login as root or use su to switch to root.

```
gwava@linux-o3in:/root> su
Password:
```

- Create the folder /opt/beginfinite/redline

```
mkdir /opt/beginfinite/redline/
```

- Give the user who will run Redline read and write permissions to that folder. You can do this by switching the owner of the folder to that user.

```
chown uli /opt/beginfinite/redline/
```

- Login as a regular user or exit from root user access

```
redline4:/home/gwava/Desktop/bintree/lib # exit
exit
gwava@redline4:~>
```

- Go to the folder where Redline was unpacked

```
cd ~/Redline/linux.suse10/redline/
```

- Unpack the tar.gz file

```
tar -zxvf redline.tar.gz
```

- Go to the subfolder bintree/opt/beginfinite
`cd bintree/opt/beginfinite/`
- Copy Redline to /opt/beginfinite/redline
`cp -r redline/ /opt/beginfinite/`
- Switch to root again

```
gwava@linux-o3in:/root> su
Password:
```
- Copy bintree/lib/libredline.so.4.0.0 to /lib or /lib64 as appropriate
`se10/redline/bintree/lib> cp libredline.so.4.0.0 /lib/`
- Go to the /lib or /lib64 folder
`cd /lib/`
- Create a link to libredline.so.4 in the /lib or /lib64 folder
`ln -s libredline.so.4 libredline.so.4.0.0`
- run ldconfig to import the new library symbols
`ldconfig`
- (Optional) Copy rcenter and ragent from redline/linux.suseXX/redline/bintree/etc/init.d to /etc/init.d

Start Control Center on Linux

Redline on Linux can run as a background process and, mostly for debugging purposes, as a foreground process with a screen similar to the NetWare screen. There is a start/stop script in the folder /etc/init.d. To start the Control Center, go to /etc/init.d and type rlcenter start.

```
gwava@linux-o3in:/root> su
Password:
linux-o3in:~ # cd /etc/init.d
linux-o3in:/etc/init.d # ./rlcenter start
```

In order to start the Control Center with a GUI screen, make sure you have the GNOME desktop installed. It is possible to use the KDE desktop as well, but the GTK libraries need to be installed on your system. To start the Control Center with a screen:

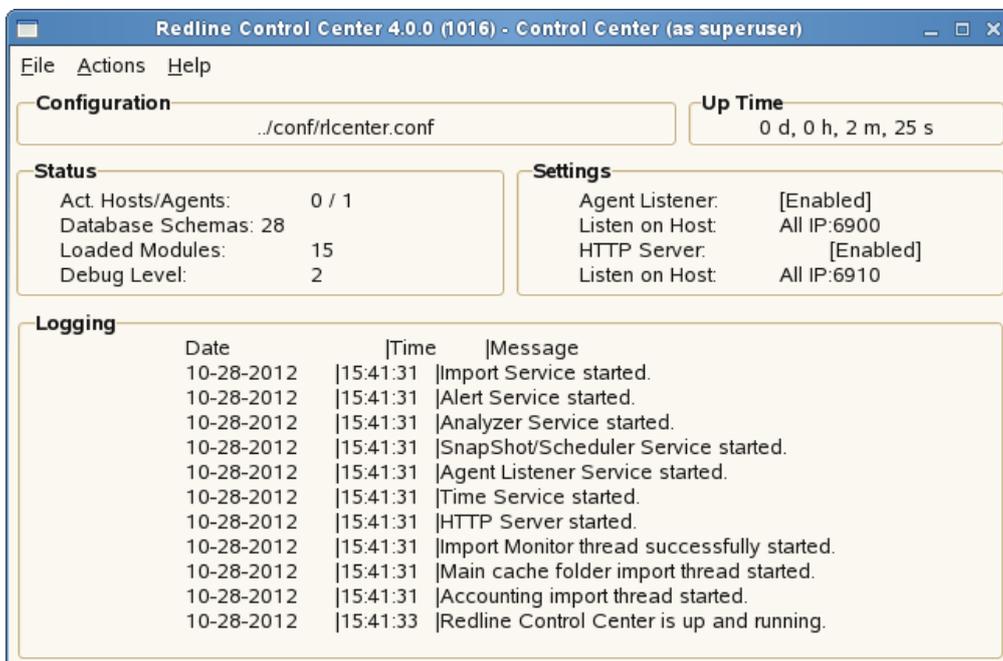
- go to the folder /opt/beginfinite/redline/bin

```
cd /opt/beginfinite/redline/bin/
```

- start the control center with the command line switch --show

```
./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.



Start Agent on Linux

Redline on Linux can run as a background process and, mostly for debugging purposes, as a foreground process with a screen similar to the NetWare screen. There is a start/stop script in the folder /etc/init.d. To start the Agent, go to /etc/init.d and type ./rlagent start.

```
gwava@linux-o3in:~> su
Password:
linux-o3in:/home/gwava # cd /etc/init.d
linux-o3in:/etc/init.d # ./rlagent start
```

In order to start the Agent with a GUI screen, make sure you have the GNOME desktop installed. It is possible to use the KDE desktop as well, but the GTK libraries need to be installed on your system. In order to start the Agent with a screen:

- go to the folder /opt/beginfinite/redline/bin

```
cd /opt/beginfinite/redline/bin/
```

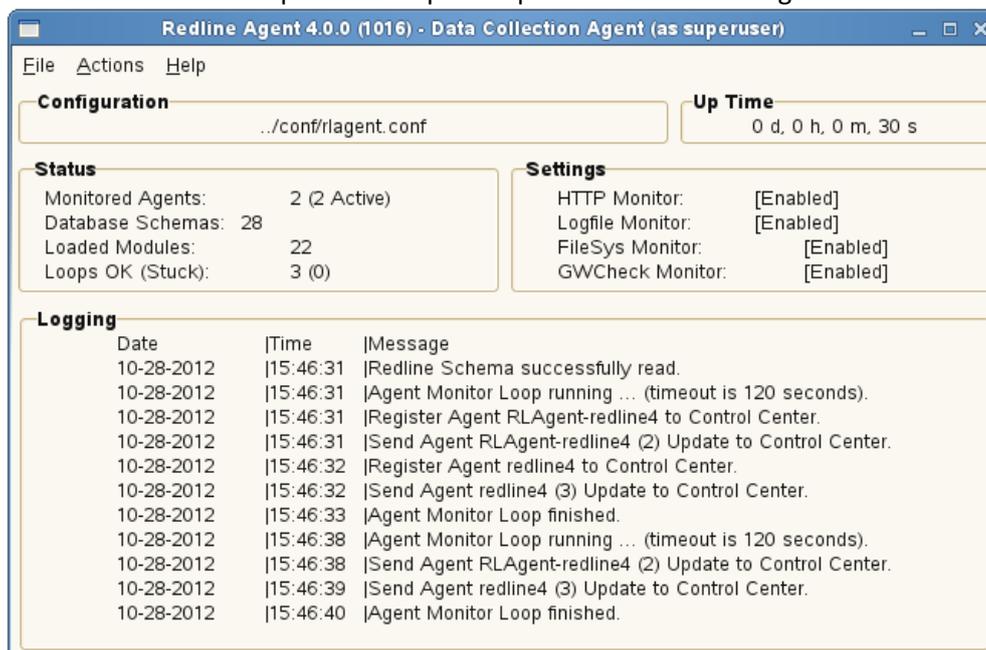
- start the agent with the command line switch --show

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

The agent configuration file (listed above) holds a 'NEWINSTALL' switch and requires the registration name, code, address and port for the Control Center. This can be edited manually, or, if desired, the agent may be started in the GUI. (This does not work over SSH) You will be asked for Registration Name, Registration Code, Control Center IP address and port. Everything else can be configured through the Control Center web interface.



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



Date	Time	Message
10-28-2012	15:46:31	Redline Schema successfully read.
10-28-2012	15:46:31	Agent Monitor Loop running ... (timeout is 120 seconds).
10-28-2012	15:46:31	Register Agent RAgent-redline4 to Control Center.
10-28-2012	15:46:31	Send Agent RAgent-redline4 (2) Update to Control Center.
10-28-2012	15:46:32	Register Agent redline4 to Control Center.
10-28-2012	15:46:32	Send Agent redline4 (3) Update to Control Center.
10-28-2012	15:46:33	Agent Monitor Loop finished.
10-28-2012	15:46:38	Agent Monitor Loop running ... (timeout is 120 seconds).
10-28-2012	15:46:38	Send Agent RAgent-redline4 (2) Update to Control Center.
10-28-2012	15:46:39	Send Agent redline4 (3) Update to Control Center.
10-28-2012	15:46:40	Agent Monitor Loop finished.

Linux Cluster Installation

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

- Install Redline to one of the cluster nodes according to the normal procedure for Linux.
(rpm -U redline-<version number>-1.<platform>.rpm)
- Redline installs to /opt/beginfinite/redline by default. Copy the entire Redline directory to each of the resources. (resourcevol/redline)
- Navigate to /etc/init.d directory on the machine you installed Redline, and rename the rlagent file to rlag.

NOTE: The default installation installs both Redline Agent and Control Center. It is recommended to run the command: "chkconfig --del rcenter" to stop the Control Center from automatically loading. Once the Redline 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/redline/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/redline/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 RedlineAgentName parameter is commented out, enable it and specify: RedlineAgentName=RLAgent_RESOURCE_NAME. You'll want to change the volume name for each cluster.
- Startup the individual agent by specifying the path to: /resourcevol/redline/bin/rlag start
Unload the individual agents by referencing the same path: /resourcevol/redline/bin/rlag stop
These are the start and stop scripts.
- Finally make sure that you have the Redline libraries installed on each node. Locate the Redline.tar.gz file, located in the install folder where Redline was downloaded. Go to redline/linux.suse< 32 or 64 as appropriate>/redline
You should find two files:
redline-<version number>-1.<platform>.rpm
redline.tar.gz

Unzip the redline.tar.gz file. A new directory called 'bintree' will appear which will contain a file called "libredline.so.4.0.0". Copy the 'libredline.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).

NetWare Installation

There are two ways to install Redline on a NetWare Server. The Windows based installer and the NetWare based install script. The Windows install script is, by far, the preferred and best method. With the NetWare install script you can install Redline to any NetWare Server through any remote console like RCONSOLE, SSH or RCONJ. The Windows Installer requires an up to date NetWare client, logged into each server that Redline is to be installed onto with a user with sufficient rights to the SYS volume.

The Windows Installer

- From the /redline/netware/ folder run the setup.exe. Click Next.



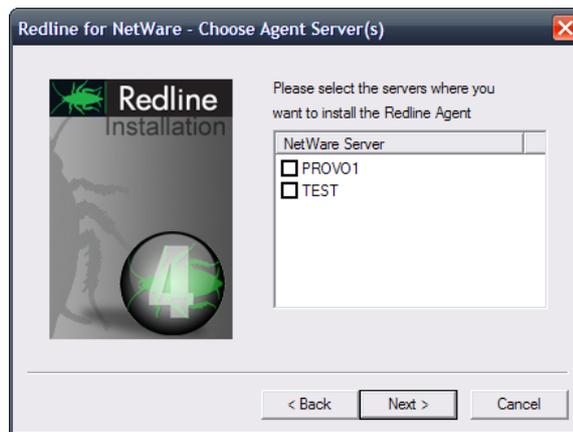
- Accept the license agreement. Click Next.



- Select the server that the Control Center will run on. Click Next.



- Select the server or servers that the Agents will run on. It is possible to install the Control Center and Agents with one setup on multiple machines. Click Next.



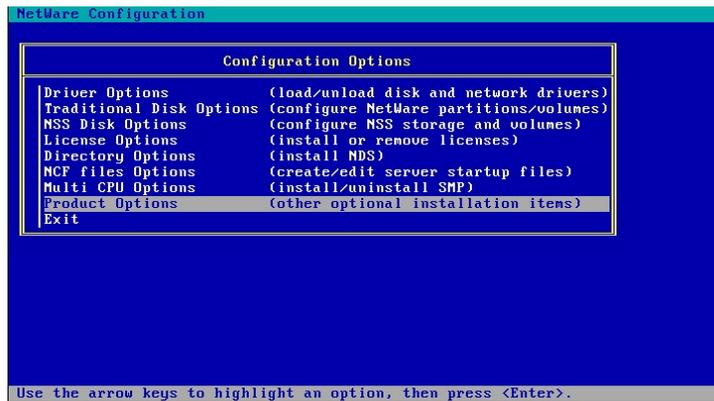
- Select Install / Update and click Finish. It is possible to have the installer configure Redline to run in a protected address space. That way it isn't necessary to modify the NCF files to start Redline in protected memory. By default, Redline installs two files, RLCCP.NCF and RLAGP.NCF which can be used to start the Control Center or Redline Agent into a protected address space at any time.



- The Windows Installer updates your AUTOEXEC.NCF file after successful installation automatically.

The NetWare Install Script

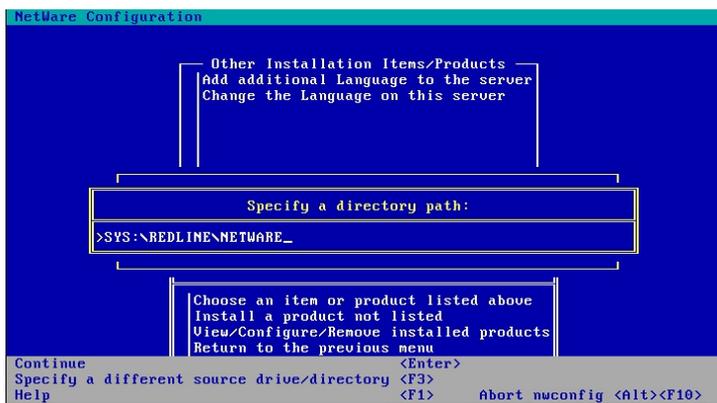
- Run NWCONFIG from the NetWare System Console and select Product Options.

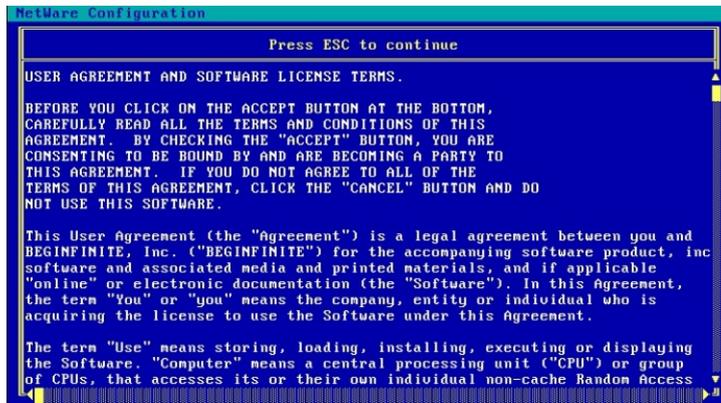


- Select Install a product not listed from the menu



- Specify a directory path where Redline was unpacked after download.





- Accept the license agreement.
- Update AUTOEXEC.NCF after installation.



- After Installation you can start the Control Center from the installation script.



After successful installation Redline shows up in the list of installed products.

Install Control Center to a non SYS Volume on NetWare

Redline expects to be installed on the SYS volume in a NetWare system. To move Redline to another volume requires several steps. The example assumes that the new volume is named MYRL, and Redline is to be moved directly under the root. (e.g. MYRL:\opt\Beginfinite\Redline is the product path)

- Stop the Redline Control Center. If an Agent is running on the same server, stop the agent as well.
- Check your search paths and look for the Redline search path with the SEARCH command. Look which search number the redline path has. In our case the Redline search path is number 18. It is likely that this number is different in your environment.

```
ULIX:search
Search 1: [Server Path] SYS:\SYSTEM\
Search 2: [DOS Path] C:\NWSERVER\ (default directory)
Search 3: [Server Path] SYS:\JAVA\NWGF\
Search 4: [Server Path] SYS:\JAVA\NJCLUZ\BIN\
Search 5: [Server Path] SYS:\JAVA\BIN\
Search 6: [Server Path] SYS:\NSEARCH\
Search 7: [Server Path] SYS:\BIN\
Search 8: [Server Path] SYS:\LIB\
Search 9: [Server Path] SYS:\USR\LOCAL\BIN\
Search 10: [Server Path] SYS:\TOMCAT\33\BIN\
Search 11: [Server Path] SYS:\XTIER\
Search 12: [Server Path] SYS:\APACHE\
Search 13: [Server Path] SYS:\PHP\
Search 14: [Server Path] SYS:\APACHE\IFOLDER\SERVER\
Search 15: [Server Path] SYS:\TESTKITS\TC\
Search 16: [Server Path] SYS:\APACHE2\
Search 17: [Server Path] SYS:\SYSTEM\
Search 18: [Server Path] SYS:\OPT\BEGINFINITE\REDLINE\BIN\
ULIX:~
```

- Remove the current search path

SEARCH DEL 18 (Or whatever the number is in your environment)

- Move the entire SYS:\opt\beginfinite\redline tree to MYRL:\opt\beginfinite\redline, including all subdirectories.
- Create an empty folder on SYS, which will be a placeholder. It is recommended to create a folder SYS:\mnt\posix\myrl. Do not create any subfolders in this new folder. This is necessary because Redline is a POSIX application on NetWare, and SYS is the virtual root on Netware, comparable with / on Linux or UNIX.
- Type EDIT SYS:\etc\pathtab at the system console. If prompted to create a new file, do so. Add the following line to PATHTAB and save it:

/mnt/posix/myrl <space> myrl:\, where <space> is a space character. This step enables POSIX mapping between the /mnt/posix/myrl mount point on SYS and the real Netware volume where Redline was copied to.

- Type EDIT myrl:\opt\Beginfinite\redline\bin\rlcc.ncf . Correct the path, which currently points to SYS. Be aware that you need to specify a NetWare style path here; which means you need a path in the form VOLUME:\opt\beginfinite\redline\conf\rlcenter.conf.
- Add the new search path

SEARCH ADD MYRL:\opt\beginfinite\redline\bin

- EDIT AUTOEXEC.NCF, and add the same search path. Remove any old obsolete search path.
- On NetWare 6.5 and OES you can test if POSIX paths are working, if BASH is installed on your system. type:

```
BASH
cd /mnt/posix/myrl
ls
```

You should see the content of MYRL:\ in the folder sys:\mnt\posix\myrl..

- Edit myrl:\opt\beginfinite\redline\conf\rlcenter.conf and change all path names. add /mnt/posix/myrl to all path names:

```
...
LogFilePath=/mnt/posix/myrl/opt/beginfinite/redline/logs
DataPath=/mnt/posix/myrl/opt/beginfinite/redline/db
ConfigPath=/mnt/posix/myrl/opt/beginfinite/redline/conf
ImportPath=/mnt/posix/myrl/opt/beginfinite/redline/imp
SoftwarePath=/mnt/posix/myrl/opt/beginfinite/redline/software
...
CCTemplatePath=/mnt/posix/myrl/opt/beginfinite/redline/CC-Templates
```

You should now be able to run the Control Center from volume MYRL by typing RLCC. If more information on pathTAB and POSIX path names is needed, check the Appendix of this manual.

Start Control Center on NetWare

During installation a search path to SYS:\OPT\BEGINFINITE\REDLINE\BIN was added to AUTOEXEC.NCF and executed on the command line.

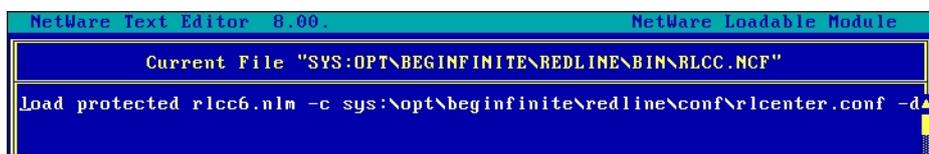
To start the Control Center, type RLCC on the System Console:

```
ULIX:rlcc
Loading Module RLCCLOAD.NLM

Loading Module RLCC6.NLM
  Auto-Loading Module NWSNUT.NLM
  Auto-Loading Module LIBREDLL.NLM
ULIX:_
```

RLCC is a NCF file which loads RLCCLOAD.NLM. This is a NLM which checks whether LIBC.NLM, the NetWare Version, and Support Pack Version are current enough. If this check fails, the Redline Control Center will not start and returns a message to the user that the system needs to be updated. This avoids possible ABENDs on the NetWare server. RLCCLOAD.NLM loads RLCC6.NLM, which is the main Control Center binary.

If you want to run the Control Center in a protected address space on NetWare, it is possible to simply use RLCCP.NCF instead of RLCC.NCF. Alternatively, you can edit RLCC.NCF and replace rlccload.nlm with load protected rlcc6.nlm. In protected memory, Redline needs its own address space; you can't start it with another application in the same address space.



```
NetWare Text Editor 8.00. NetWare Loadable Module
Current File "SYS:OPT\BEGINFINITE\REDLINE\BIN\RLCC.NCF"
Load protected rlcc6.nlm -c sys:\opt\beginfinite\redline\conf\rlcenter.conf -d
```

If the Control Center was loaded successfully on NetWare, you can see the Control Center screen.

```
Redline Control Center 3.5.0 (999) NetWare Loadable Module

Configuration : sys:\opt\beginfinite\redline\conf\rlcenter.conf
Agent Listener : [Enabled] HTTP Server : [Enabled]
Listen on Host : All IP HTTP Listen Host: All IP
Listen on Port : 6900 HTTP Listen Port: 6910
Act. Hosts/Agents: 0 / 1 Uptime : 0d 0h 0m 2s

Date | Time | Message
11-16-2010 | 14:51:41 | Graph Service started.
11-16-2010 | 14:51:41 | Import Service started.
11-16-2010 | 14:51:41 | MTA Message Import Service started.
11-16-2010 | 14:51:41 | SnapShot/Scheduler Service started.
11-16-2010 | 14:51:41 | Agent Listener Service started.
11-16-2010 | 14:51:41 | HTTP Server started.
11-16-2010 | 14:51:41 | Time Service started.
11-16-2010 | 14:51:41 | Import Monitor successfully started.
11-16-2010 | 14:51:41 | Main cache folder import thread started.
11-16-2010 | 14:51:41 | Accounting import thread started.
11-16-2010 | 14:51:43 | Redline Control Center is up and running.

ShF4-Purge F6-Restart F7-Exit (Sh)F8-Dr/Cr Index F9-Info F10-List Agents
```

Start Agent on NetWare

During installation a search path to SYS:\OPT\BEGINFINITE\REDLINE\BIN was added to AUTOEXEC.NCF and executed on the command line.

To start the Agent, type RLAG on the System Console:

```
ULIX:rlag
Loading Module RLAGLOAD.NLM

Loading Module RLAG6.NLM
Auto-Loading Module NWSNUT.NLM
Auto-Loading Module LIBREDLL.NLM
ULIX: _
```

RLAG is a NCF file which loads RLAGLOAD.NLM. This is a NLM which checks if LIBC.NLM, the NetWare Version and Support Pack Version are current enough. If not, the Redline Agent will not start and returns a message to the user that the system needs to be updated. This avoids possible ABENDs on the NetWare Server. RLAGLOAD.NLM loads RLAG6.NLM, which is the main Agent binary.

If you want to run the Agent in a protected address space on NetWare, edit RLAG.NCF and replace rlagload.nlm with load protected rlag6.nlm. When run alone, Redline needs a dedicated address space. You can't start it with another application in the same address space.

```
NetWare Text Editor 8.00. NetWare Loadable Module

Current File "SYS:OPT\BEGINFINITE\REDLINE\BIN\RLAG.NCF"

load protected rlag6.nlm -c sys:\opt\beginfinite\redline\conf\rlagent.conf -dZ▲
```

If the Agent is started the very first time, you will be asked for Registration Name, Registration Code, Control Center IP address and port. Everything else can be configured through the Control Center web interface.

Control Center Connection Configuration	
Registration Name:	Your Company Name
Registration Code:	012345678901234567
Control Center Address:	127.0.0.1
Control Center Port:	6900

If the Agent was loaded successfully on NetWare, you can see the Agent screen.

```

Redline Agent 3.5.0 (999)                               NetWare Loadable Module

Configuration      : sys:\opt\beginfinite\redline\conf\rlagent.conf
HTTP Monitor       : [Enabled]                          Logfile Monitor   : [Enabled]
FileSys Monitor    : [Enabled]                          Stuck Loops       : 0
GWCheck Monitor    : [Enabled]                          Loops Agent      : 1
Monitored Agents   : 2 (2 Active)                       Uptime           : 0d 0h 0m 2s

Date | Time | Message
11-16-2010 | 14:52:30 | LIBREDLL.NLM Version 3.5.0 (LIBC, Build 999)
11-16-2010 | 14:52:30 | Time Service successfully started.
11-16-2010 | 14:52:30 | Agent Monitor Service successfully started.
11-16-2010 | 14:52:30 | Agent Monitor Loop running ... (timeout is 120 seconds).
11-16-2010 | 14:52:30 | Register Agent RLAgent-REDLINE35 to Control Center.
11-16-2010 | 14:52:30 | Send Agent RLAgent-REDLINE35 (2) Update to Control Center.
11-16-2010 | 14:52:31 | Start _ADMIN copy process.
11-16-2010 | 14:52:31 | Redline Agent is up and running.
11-16-2010 | 14:52:31 | Register Agent REDLINE35 to Control Center.
11-16-2010 | 14:52:31 | Send Agent REDLINE35 (3) Update to Control Center.
11-16-2010 | 14:52:32 | Agent Monitor Loop finished.

(Shift)F6-Loop/Restart F7-Exit F9-RL Agent Info (Shift)F10-GW Agent Info
  
```

Netware Cluster Installation

For High availability it is beneficial to run GroupWise in a Cluster environment. In such a scenario, multiple servers make up a cluster, and every application is running as a resource on the cluster. For more details about NetWare Clusters refer to the Novell Cluster Services documentation.

Control Center

If you want to install the Redline Control Center on a Cluster, create a resource for the Control Center. Make sure that no other POSIX application is running in the same resource, because you cannot run more than one POSIX application in the same address space.

The next step is to install the Control Center as described earlier in this documentation on one of the server nodes, as if this is a single server. Then move the installation to a shared cluster volume. Let's assume MYRL: is a volume on a shared storage device.

- Move the entire SYS:\opt\beginfinite\redline tree to MYRL:\opt\beginfinite\redline, including all subdirectories.
- Create an empty folder on SYS, which will be a placeholder. It is recommended to create a folder SYS:\mnt\posix\myrl. Do not create any subfolders in this new folder. This is necessary because Redline is a POSIX application on NetWare, and SYS is the virtual root on Netware, comparable with / on Linux or UNIX.
- Type EDIT SYS:\etc\pathtab at the system console. If prompted to create a new file, do so. Add the following line to PATHTAB and save it:
/mnt/posix/myrl <space> myrl:\, where <space> is a space character. This step enables POSIX mapping between the /mnt/posix/myrl mount point on SYS and the real Netware volume where Redline was copied to. *Do this on every cluster node.*
- Type EDIT myrl:\opt\beginfinite\redline\bin\rlcc.ncf. Correct the path, which currently points to SYS. Be aware that you need to specify a NetWare style path here; which means you need a path in the form VOLUME:\opt\beginfinite\redline\conf\rlcenter.conf.
- Add the new search path

```
SEARCH ADD MYRL:\opt\beginfinite\redline\bin
```

- Edit the start script of the cluster resource and add the same search path. "Add load address space = rlcc rlcc6 -c myrl:\opt\beginfinite\redline\conf\rlcenter.conf" to your resource script to load the Control Center. *NOTE: if multiple resources exists in the cluster, and it is possible for them to mount to the same node, different address space names must be specified.*
- Add "rlcenter unload" to your stop script for the Control Center resource.
- On NetWare 6.5 and OES you can test if POSIX paths are working, if BASH is installed on your system. type:

```
BASH
cd /mnt/posix/myrl
ls
```

You should see the content of MYRL:\ in the folder sys:\mnt\posix\myrl..

- Edit myrl:\opt\beginfinite\redline\conf\rlcenter.conf and change all path names. add /mnt/posix/myrl to all path names:

```

...
LogFilePath=/mnt/posix/myrl/opt/beginfinite/redline/logs
DataPath=/mnt/posix/myrl/opt/beginfinite/redline/db
ConfigPath=/mnt/posix/myrl/opt/beginfinite/redline/conf
ImportPath=/mnt/posix/myrl/opt/beginfinite/redline/imp
SoftwarePath=/mnt/posix/myrl/opt/beginfinite/redline/software
...
CCTemplatePath=/mnt/posix/myrl/opt/beginfinite/redline/CC-Templates

```

You should now be able to run the Control Center from volume MYRL by typing RLCC. If more information on pathtab and POSIX path names is needed, check the Appendix of this manual.

Make sure you test the failover case. You can do so by moving the Control Center resource from one node to another. A real life way is to use an Abend simulation tool. The Redline Agent can be used to simulate an Abend. Start the Redline agent with the startup parameter -a (or --abend) and hit SHIFT-F4. This will generate a Page Fault Abend, and if everything is configured correct, the Control Center resource should move to another node.

Agent

To monitor your clustered system, you must install the Redline Agent on every resource running a GroupWise agent. To install the Redline Agent on a Cluster, create or locate a resource for the Agent. Make sure that no other POSIX application is running in the same resource, because it isn't possible to run more than one POSIX application in one address space.

The next step is to install the Redline Agent as described earlier in this documentation on one of the server nodes, as if this is a single server. Then move the installation to a shared cluster volume. Let's assume MYRL: is a volume on a shared storage device.

- Move the entire SYS:\opt\beginfinite\redline tree to MYRL:\opt\beginfinite\redline, including all subdirectories.
- Create an empty folder on SYS, which will be a placeholder for the Volume. It is recommended to create a folder SYS:\mnt\posix\myrl. Do not create any subfolders in this new folder. This is necessary because Redline is a POSIX application on NetWare, and SYS is the virtual root on Netware, comparable with / on Linux or UNIX. Complete this step for every node the Redline Agent's resource can failover to.
- Type EDIT SYS:\etc\pathtab at the system console. If prompted to create a new file, do so. Add the following line to PATHTAB and save it:
/mnt/posix/myrl <space> myrl:\, where <space> is a space character. This step enables POSIX mapping between the /mnt/posix/myrl mount point on SYS and the real Netware volume where Redline was copied to. Do this on every cluster node the Redline Agent's resource can failover to.
- Type EDIT myrl:\opt\beginfinite\redline\bin\rlag.ncf . Correct the path, which currently points to SYS. Be aware that you need to specify a NetWare style path here; which means you need a path in the form VOLUME:\opt\beginfinite\redline\conf\rlagent.conf.
- Add the new search path

```
SEARCH ADD MYRL:\opt\beginfinite\redline\bin
```

- Edit the start script of the cluster resource and add the same search path. Add "load address space = rlag rlag6 -c myrl:\opt\beginfinite\redline\conf\rlagent.conf" to your resource script to load the Redline Agent. *NOTE: if multiple resources exists in the cluster, and it is possible for them to mount to the same node, different address space names must be specified.*
- Add "rlagent unload" to your stop script for the Redline Agent resource.
- On NetWare 6.5 and OES you can test if POSIX paths are working, if BASH is installed on your system. type:

```
BASH
cd /mnt/posix/myrl
ls
```

You should see the content of MYRL:\ in the folder sys:\mnt\posix\myrl..

- Edit myrl:\opt\beginfinite\redline\conf\rlagent.conf and change all path names. add /mnt/posix/myrl to all path names:

```
...
LogFilePath=/mnt/posix/myrl/opt/beginfinite/redline/logs
DataPath=/mnt/posix/myrl/opt/beginfinite/redline/db
BinPath=/mnt/posix/myrl/opt/beginfinite/redline/conf
SoftwarePath=/mnt/posix/myrl/opt/beginfinite/redline/software
```

You should now be able to run the Redline Agent from volume MYRL by starting the cluster resource. If more information on pathtab and POSIX path names is needed, check the Appendix of this manual.

Make sure you test the failover case. You can do so by moving the Redline Agent resource from one node to another. A real life way is to use an Abend simulation tool. The Redline Agent can be used to simulate an Abend. Start the Redline agent with the startup parameter -a (or --abend) and hit SHIFT-F4. This will generate a Page Fault Abend, and if everything is configured correct, the Redline Agent resource should move to another node.

IMPORTANT:

If you run the Redline Agent on a Cluster, you should overwrite the Agent Name reported to the Control Center. In the rlagent.conf file, in the [GLOBAL] section, locate the "# Override the Redline Agent with" option and remove the 'Override' section, leaving the 'RedlineAgentName=' section and fill it in. Under the [HOSTS] section, add the 'AgentName=HOST-CLUSTER-X' line. This ensures that the Redline Agent will send information with the same ID regardless from which node data is send. Uncommented lines should include the following in their respective sections:

```
[GLOBAL]
Agent=enabled
RedlineAgentName=Redline-CLUSTER-X

[HOST]
Agent=enabled
AgentName=HOST-CLUSTER-X
```

All GroupWise components monitored on a cluster should be monitored through the virtual cluster IP.

Windows Installation

- Unzip the Redline package onto your Windows desktop.
- From the /redline/windows/ folder run the setup.exe. Click Next.



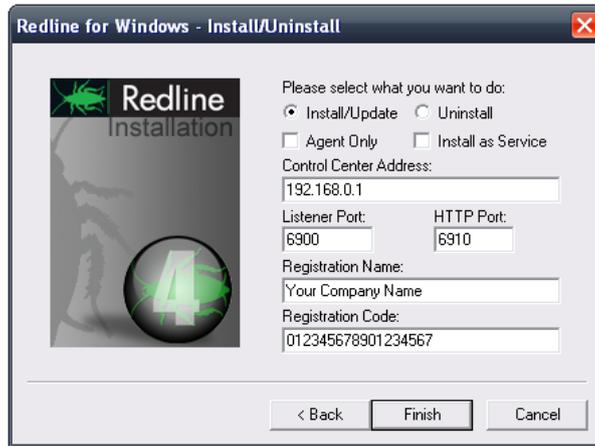
- Accept the license agreement. Click Next.



- 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 components to install / Update and click Finish. Optional: you can select to install Redline as a Windows Service.



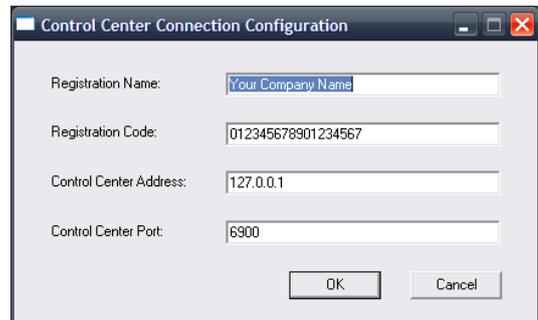
Start Redline on Windows

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

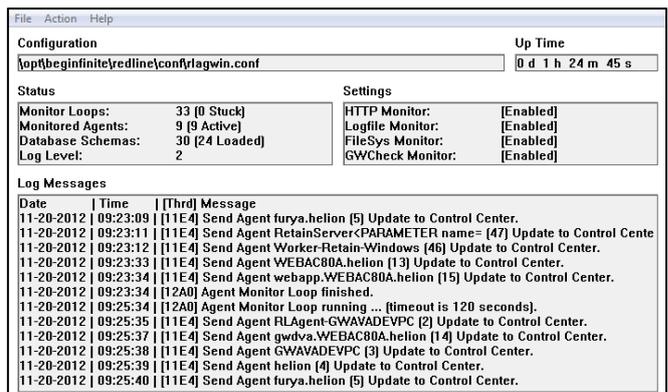
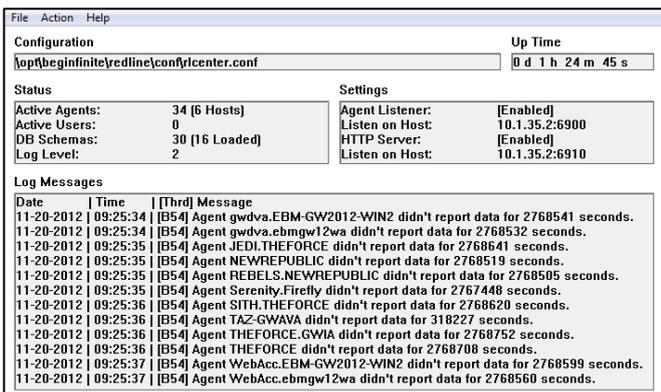


If you installed Redline as a service, the agent is not started. It is important to start the agent manually after installation. To start Redline as a service, start it from the Windows Services interface.

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

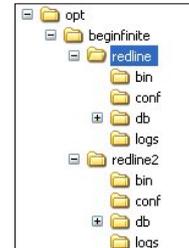


It is recommended to run the agent as a Windows Service. A Service is started without logging in to the server, just by booting the machine. That way the Redline Agent is started every time the server is restarted.

Multiple Redline Agents on Windows

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

- Copy the folder c:\opt\beginfinite\redline to c:\beginfinite\redline2 (or another folder like redline3, redline 4 etc.)
- Open a cmd prompt
- Go to the folder where you've copied your new Redline Agent installation conf folder (c:\opt\beginfinite\redline\conf2)
- Edit rlagwin.conf and adjust the folders for LogFilePath, DataPath, BinPath and SoftwarePath
- Go to the bin folder of your new Redline Agent installation
- Run rlagent install RedlineAgent2 (or any other unique name for this service)



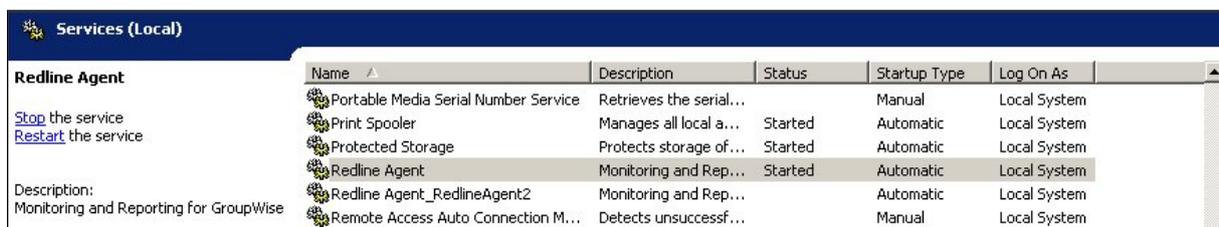
```
C:\>cd c:\opt\beginfinite\redline2\bin
C:\opt\beginfinite\redline2\bin>rlagent install RedlineAgent2
C:\opt\beginfinite\redline2\bin>
```

- Wait a moment until a message appears that the agent has been installed successfully.



- (Optional) In order to uninstall the service, type rlagent uninstall RedlineAgent2 (or whatever name you've given the service).

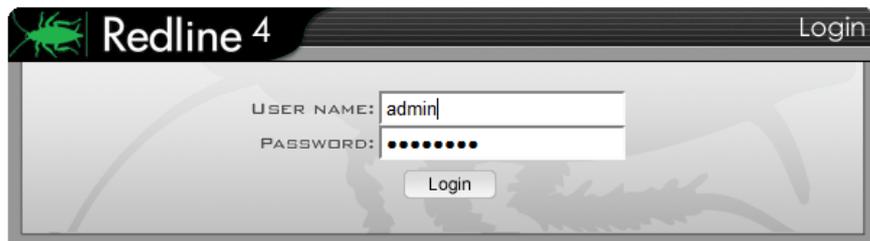
Now you can run the Redline Agent multiple times on your Windows Server:



Access Control Center

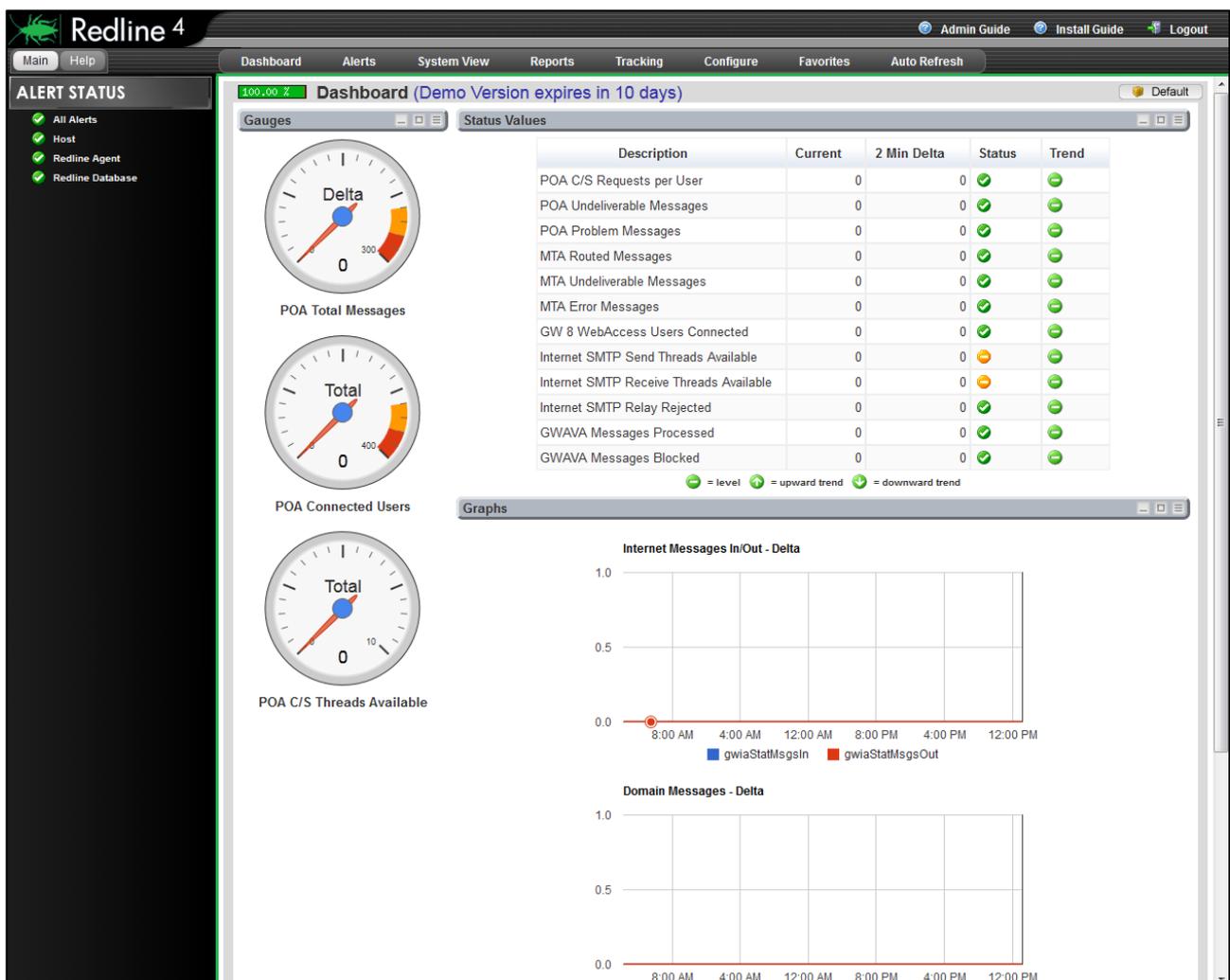
Redline is a full Web Based Application. By default Redline is listening on port 6910. After Installation the default administrator username is admin, and the password is password. To access the Web Interface, type <http://a.b.c.d:6910>

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 Redline itself and all registered GroupWise components.



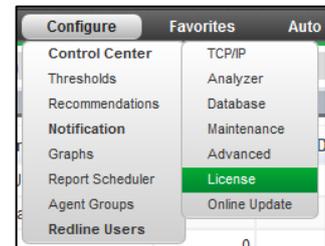
Install License

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 Redline system will become completely inactive after the evaluation expires.

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

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 Redline Agents are updated with this information as well
- Install the license file

A screenshot of the 'Redline Registration / License' web interface. The page has a navigation bar with 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The main content area is titled 'Redline Registration / License' and contains three sections: 'Registration' with input fields for 'Registration Name' (containing 'Your Company Name') and 'Registration Code' (containing '012345678901234567'), an 'OK' button, 'Active License' with a 'License Type' field (containing 'Demo Version expires in 10 days'), a 'Browse...' button, and an 'Install License' button, and 'Installed Licenses' which is a table with columns for 'File', 'Licensed to', 'Product Version', 'Type', 'Valid until', and 'Action'.

The Registration Name and Code must be configured on all Redline 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 Redline Agent and the Redline Control Center use the Registration Name and Registration Code information for two purposes:

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

Update Redline

Redline 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 exactly 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 Redline should work immediately as it has done before. No NCF files on NetWare, thresholds, recommendations, database records, Redline Agent and Redline Control Center configuration files are overwritten. Sometimes new values will be added.

Uninstall Redline

Redline'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 Redline has provided powerful functionality that you cannot find elsewhere.

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

NetWare

- Stop the Redline Agent and Control Center
- Delete the SYS:\opt\Beginfinite\redline tree
- Remove modifications from sys:system\autoexec.ncf

Note: The Windows-based installer can do this automatically. Run SETUP and click through the prompts to select Uninstall at the end.

Windows

- Stop the Redline Agent and Control Center
- Start the Windows Setup.exe and click through the prompts. On the last page select Uninstall. -Uninstalling the Redline 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.

```
gwava@linux-o3in:/root> su  
Password:
```
- uninstall the rpm package with the rpm command

```
rpm -e redline-<version>.rpm
```
- For complete uninstall, delete the /opt/beginfinite/redline directory.

Manually:

- Stop both Redline 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
- Delete the /opt/Beginfinite/redline tree
- Remove /etc/init.d/rlcenter and /etc/init.d/rlagent

- Remove /lib/libredline.so.4.0.0

Configure Redline Agent; Monitor GroupWise

Every Agent must have a unique name to successfully register to the Control Center. If, for some reason, two agents have the same name, the one that registers second is rejected by the Control Center. In that case you must either overwrite the name with another name, or add a prefix or suffix. Having a unique name is important because several Reports, analysis, graphs etc. are based on the agent name.

The GUID is used by Redline to make sure an agent once registered with a unique name will always be assigned to the same name. This can be necessary if the Redline Agent is reinstalled. The GUID's are managed by Redline, and you shouldn't touch or add any GUID anywhere.

Adding monitoring agents to an agent is accomplished through that Agent's page, under the 'manage' tab. (Any agent's page may be accessed simply by selecting the desired agent. Agents are displayed in several locations, agent groups, status overview, redline maps, etc.)

The screenshot shows the Redline 4 web interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'SYSTEM VIEW' sidebar on the left shows 'Host', 'Redline Agent', and 'Redline Database'. The main content area is titled 'Manage' and shows 'Agent Information' for 'Redline Agent: RLAgent-GW2012SLES11SP2'. Below this is a table of 'Monitored Agents' with columns for Type, Description, Unique ID, Agent Name, Status, HTTP IP Address, HTTP IP Port, SSL, and Action. The 'Add or Edit Monitored Agent' form is open, showing a dropdown menu for 'Agent Type' with options like 'GW Post Office Agent', 'GW 2012 DocView Agent', 'GW 2012 WebAccess', 'GW 8 Doc Viewer Agent', 'GW 8 WebAccess Agent', 'GW 8 WebAccess Appl.', 'GW API Gateway', 'GW Async Gateway', 'GW Exchange Gateway', 'GW Internet Agent', 'GW Message Transfer Agent', 'GW Mobile Server 2.x/3.x', 'GW Notes Gateway', 'GWAVA', 'Host', 'NotifyLink Server', 'Novell Messenger Agent', 'Novell Messenger Arch Agent', 'RIM BlackBerry Server', and 'Reload'. The 'Agent Name' field is highlighted in blue.

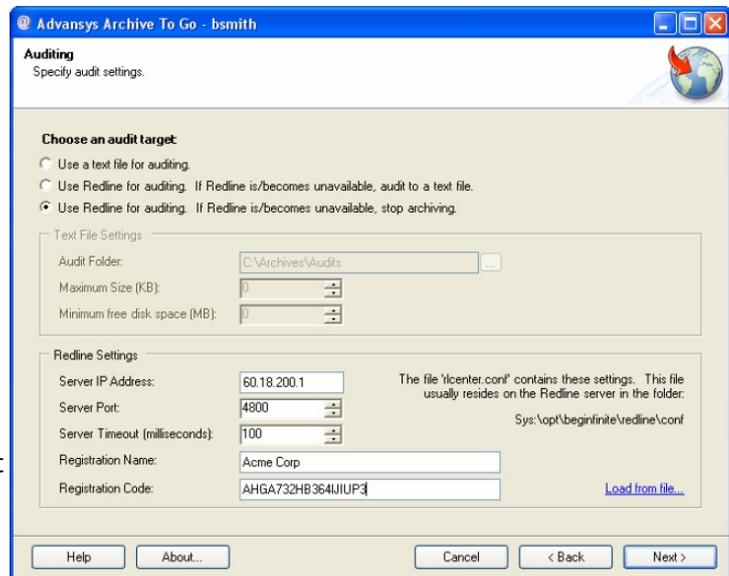
In the agent type dropdown menu, the different agent modules are listed and can be selected from the agent type, and configured.

Advansys Archive2Go

Archive2Go from Advansys is one of the Applications which does not require a Redline Agent. It talks directly to the Control Center. Redline 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 Redline is involved in the auditing process. One is where auditing to Redline is enforced, and Archive2Go doesn't work if Redline is not available, and another option where auditing can fall back to a text file as soon as Redline 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 Redline Control Center Configuration/License tab.

GroupWise API Gateway

The GroupWise API Gateway was introduced in GroupWise 4.1 and has not changed much. Therefore there is no HTTP server to configure; nor is there SNMP support provided. All that is available and required is that you configure the Logging to be on and be verbose, and note the Log Files path on your [Appendix](#) work sheet. By default the configuration file for the API Gateway is named ngwapi.prm. It is recommended to set the log days to 7 and the maximum log file size to 1000Kb.

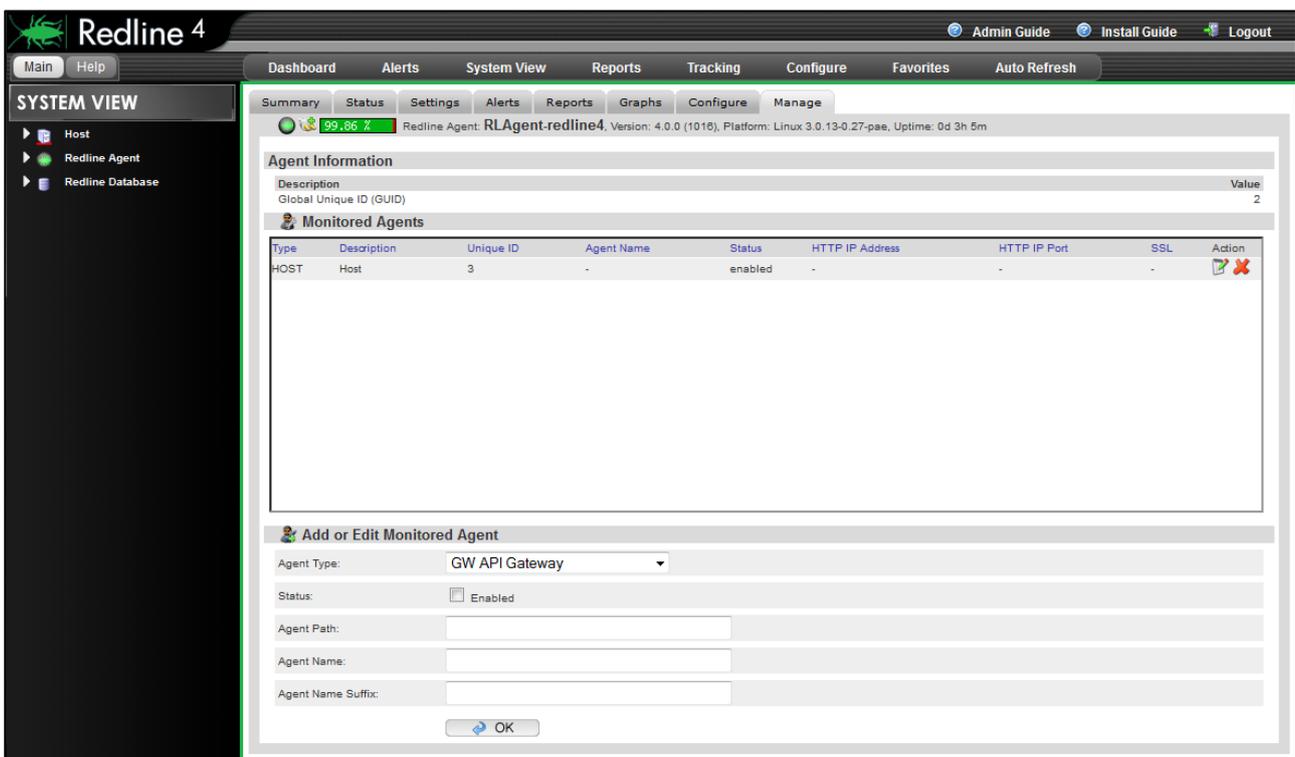
- /loglevel - Verbose
- /logdays -7
- /logmax - 1000

Redline will look for new log file information every 2 minutes. You only need to specify the log file path in Redline. The fields: http username, password, IP address, and port are ignored. The logging files path may be in NetWare, UNC, or POSIX format.

We recommend that NetWare or UNC path format be used. For notes about using POSIX format (/path1/path2/path3), see [Appendix](#)

```
=====
Current File "SYS:\GRPWISE\DOULI\WPGATE\API\NGWAPI.PRM"
=====
;/help
; LOG FILE SWITCHES
; The following switches override default logging values set in Admin
; Override the configured logging level.
; The levels are: Diag, Verbose, Normal, and Off
/loglevel-Verbose
; Path to the gateway's log file directory.
;/log-[Full path to log file directory]
; Number of days that log files are allowed to age.
/logdays-7
; Maximum K bytes that log files are allowed to use.
; The default is set in Admin
/logmax-1000
```

From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the API Gateway. Specify the Path to the API Gateway 000.PRC folder.



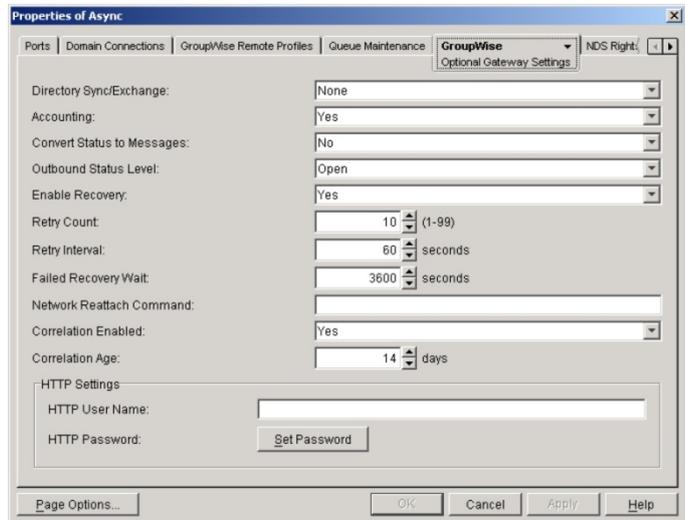
After 2-3 minutes, a message should appear on the Redline Agent that the API agent has been registered to the Control Center and shows up in the Control Center.

GroupWise Async Gateway

The Async Gateway provides a http interface similar to most other GroupWise Agents. You need to enable and configure this interface via ConsoleOne. Specify a username and password for the Async Gateway in the GroupWise/Optional Gateway Settings tab.

Optional you can configure the http interface by editing the agent configuration file, which is `async.cfg` by default and located in the same folder as the `ASYNC` binary file. The following switches need to be added.

- `/http` - Enable HTTP Interface
- `/httpport -port number` - HTTP port to listen on (There is no default port, we suggest 9999)
- `/httpuser -[username]` - Specify the Username for the HTTP interface
- `/httppassword -[password]` - specify the Password for the HTTP interface
- `/loglevel -verbose` – turns on verbose logging

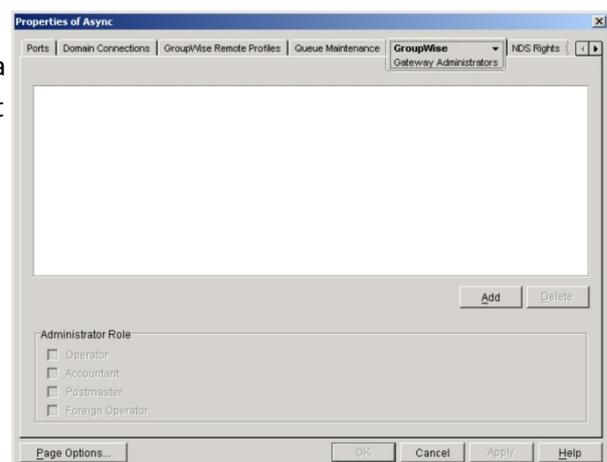


Save the file and restart the agent by unloading and reloading.

Test by opening a web browser by typing <http://ipaddress:httpPort>. For example, if the agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 9999, <http://192.168.2.3:9999>. You should be prompted for the username and password just assigned

- Do not proceed until this is working

If you want to have accounting information for reports and message tracking, enable “Accounting” and specify a gateway accountant. The accounting log files will be sent to this user and can be imported into Redline via SOAP automatically.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Async Gateway. Specify the IP Address, Port, Username and Password.

The screenshot displays the Redline 4 System View interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The left sidebar shows 'SYSTEM VIEW' with a tree view containing 'Host', 'Redline Agent', and 'Redline Database'. The main content area is titled 'Redline Agent: RAgent-redline4' and shows a status of 99.86%. Below this, there is an 'Agent Information' section with a table for 'Monitored Agents'.

Type	Description	Unique ID	Agent Name	Status	HTTP IP Address	HTTP IP Port	SSL	Action
HOST	Host	3	-	enabled	-	-	-	 

Below the table is the 'Add or Edit Monitored Agent' form with the following fields:

- Agent Type: GW Async Gateway
- Status: Enabled
- HTTP Address:
- HTTP Port:
- HTTP Username:
- HTTP Password:
- Use SSL: Yes
- Agent Name:
- Agent Name Suffix:

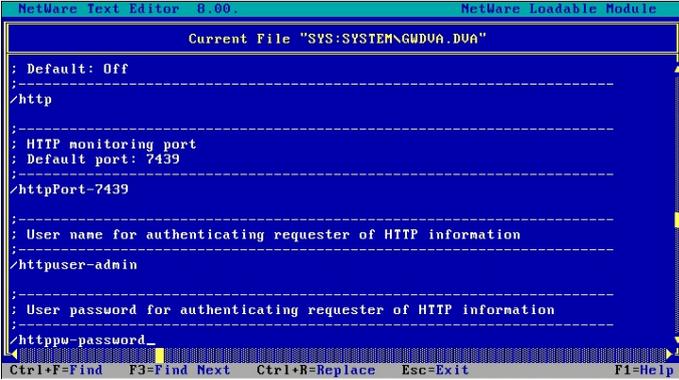
An 'OK' button is located at the bottom of the form.

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

GroupWise Document Viewer Agents (GroupWise 8 and 2012)

The Document Viewer Agent (GWDVA) is used to convert attachments for viewing in the WebAccess client. Redline supports both GroupWise 8 and 2012 viewer agents. There is no ConsoleOne interface for this agent. Instead, open the GWDVA configuration file in a text editor. This file is normally named gwdva.dva and is located in the same directory that the GroupWise WebAccess Internet Agent (GWINTER) is installed.

On NetWare the part in the configuration file looks like this:



```
NetWare Text Editor 8.00 NetWare Loadable Module
Current File "SYS:SYSTEM\GWDVA.DVA"
: Default: Off
:-----
/http
:-----
: HTTP monitoring port
: Default port: 7439
:-----
/httpPort-7439
:-----
: User name for authenticating requester of HTTP information
:-----
/httpuser-admin
:-----
: User password for authenticating requester of HTTP information
:-----
/httppw-password
Ctrl+F=Find F3=Find Next Ctrl+R=Replace Esc=Exit F1=Help
```

Add the following switches manually:

- /http - Enable HTTP Interface
- /httpport -7439 - HTTP port to listen on (7439 recommended)
- /httpuser -[username] - Specify the Username for the HTTP interface
- /httppw -[password] - specify the Password for the HTTP interface
- /loglevel - verbose – turns on verbose logging

Save the file and restart the DVA by unloading and reloading the WebAccess Agent. Test by opening a web browser by typing <http://ipaddress:httpPort>. For example if the GWDVA agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 7439, <http://192.168.2.3:7439>

You should be prompted for the username and password you just assigned

- Do not proceed until this is working

From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Document Viewer Agent. Specify the IP Address, Port, Username and Password.

The screenshot displays the Redline 4 control center interface. At the top, there is a navigation bar with 'Main' and 'Help' buttons, and a menu with 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'System View' section is active, showing a 'Summary' tab with a 99.86% status indicator and agent details: 'Redline Agent: RAgent-redline4, Version: 4.0.0 (1016), Platform: Linux 3.0.13-0.27-pae, Uptime: 0d 3h 5m'. Below this, the 'Agent Information' section shows a 'Global Unique ID (GUID)' of 2. The 'Monitored Agents' section contains a table with one entry:

Type	Description	Unique ID	Agent Name	Status	HTTP IP Address	HTTP IP Port	SSL	Action
HOST	Host	3	-	enabled	-	-	-	

Below the table is the 'Add or Edit Monitored Agent' form, which includes fields for 'Agent Type' (set to 'GW 2012 DocView Agent'), 'Status' (checked 'Enabled'), 'HTTP Address', 'HTTP Port', 'HTTP Username', 'HTTP Password', 'Use SSL' (checked 'Yes'), 'Agent Name', and 'Agent Name Suffix'. An 'OK' button is at the bottom of the form.

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

GroupWise Message Transfer Agent

Begin by writing down the IP address for this component on the installation work sheet.

Open the MTA object in ConsoleOne. Select the GroupWise/Network Address tab.

Ensure that SSL is disabled and that the HTTP port is assigned (the default is 7180). Note this port on the installation worksheet.

Next, go to the GroupWise/Agent Settings tab. A screen similar to the example will be presented:

Assign a HTTP username and password. This should not be the same as a valid eDirectory account. Include this information in the [Appendix](#) work sheet as well.

The MTA already defaults to having SNMP on (unless /nosnmp is in the startup file), but please assign a community name here (other than public or blank) to reduce security risks.

Click OK to save your settings.

Testing

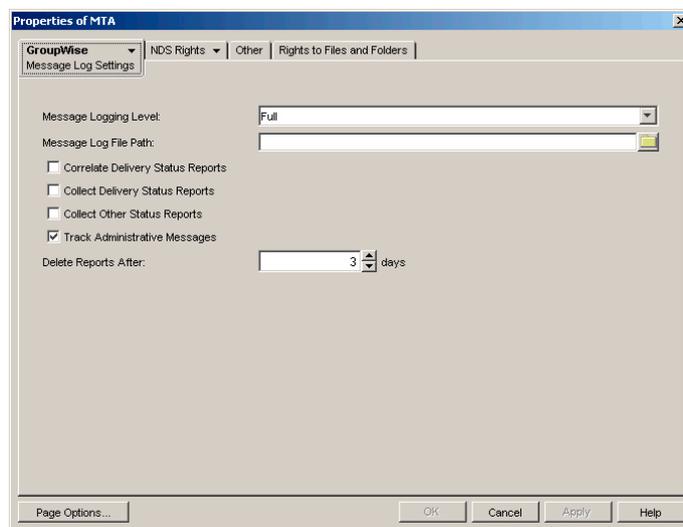
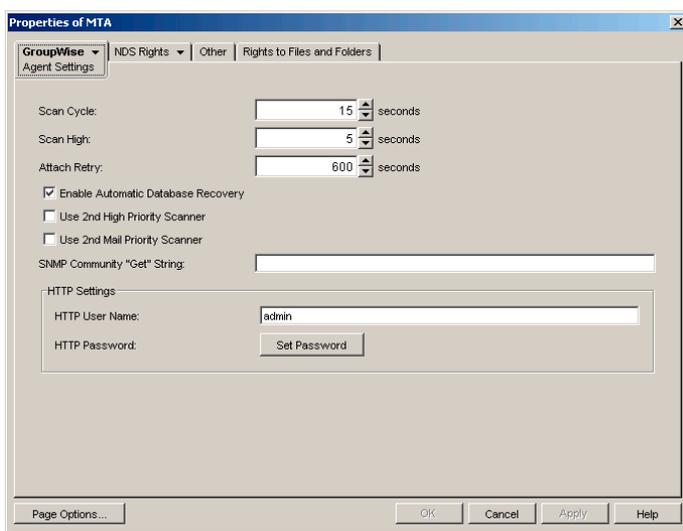
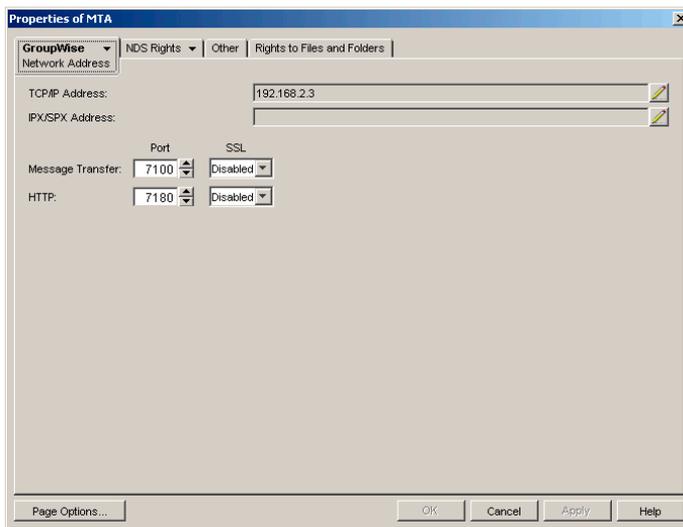
Wait one minute for the GroupWise configuration to propagate. Test your configuration with a web browser by typing: <http://ipaddress:httpPort>

For example: if the MTA were running on a server with an IP address of 192.168.2.3, and an HTTP port of 7180, <http://192.168.2.3:7180>

You should be prompted for the username and password just assigned. If this does not occur, recheck the settings in ConsoleOne, and open the agent's startup file to verify that no startup switches have overridden this configuration. Also, try restarting the agent.

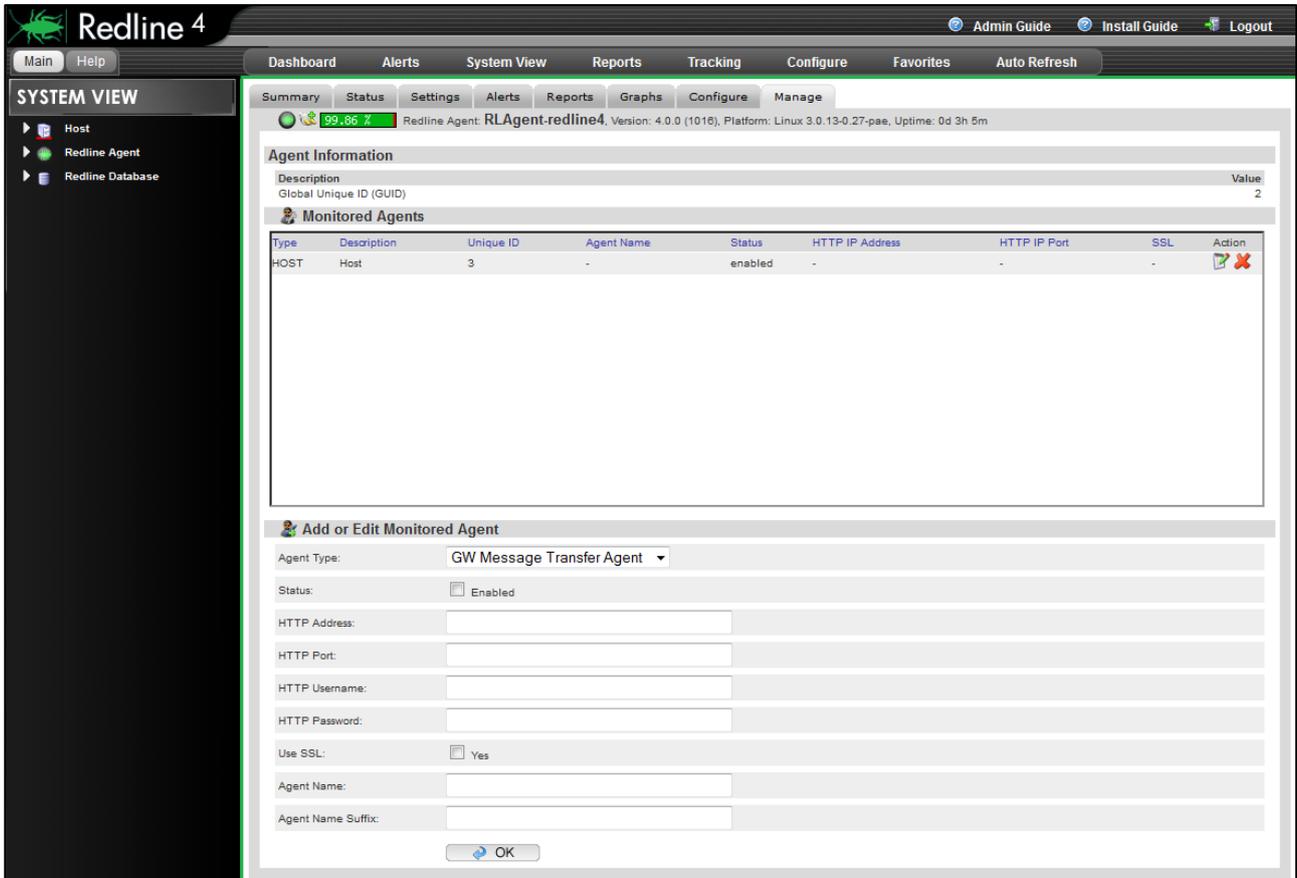
- Do not proceed until this is working

Return to ConsoleOne and reopen the agent. Go to the GroupWise/Log Settings tab to verify logging is on and set to verbose.



If you want to use Message Tracking you need to enable Message Logging for every MTA. This is disabled by default.

From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the MTA Agent. Specify the IP Address, Port, Username and Password.



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

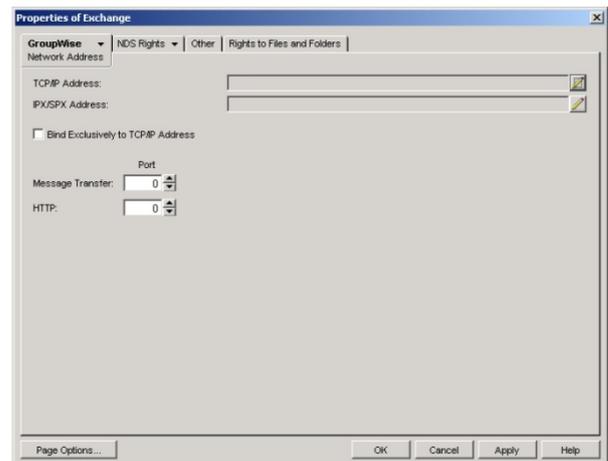
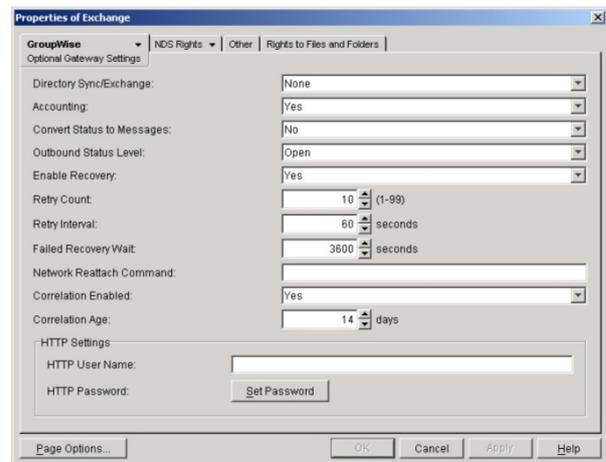
GroupWise Exchange Gateway

The Exchange Gateway provides an http interface similar to most other GroupWise Agents. You need to enable and configure this interface via ConsoleOne. Specify a username and password for the Exchange Gateway in the GroupWise/Optional Gateway Settings tab and specify the http port on the Network Address tab.

Optional you can configure the http interface by editing the agent configuration file, which is exchange.cfg by default and located in the same folder as the Exchange Gateway binary file. The following switches need to be added.

- /http - Enable HTTP Interface
- /httpport -portnumber - HTTP port to listen on (There is no default port, we suggest 9997)
- /httpuser -[username] - Specify the Username for the HTTP interface
- /httppassword -[password] - specify the Password for the HTTP interface
- /loglevel -verbose – turns on verbose logging

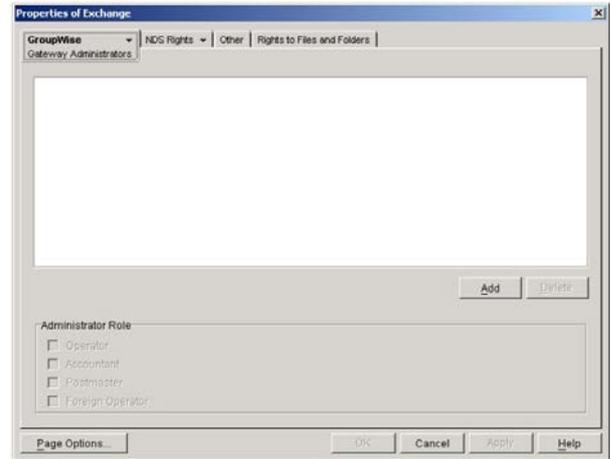
Save the file and restart the agent by unloading and reloading.



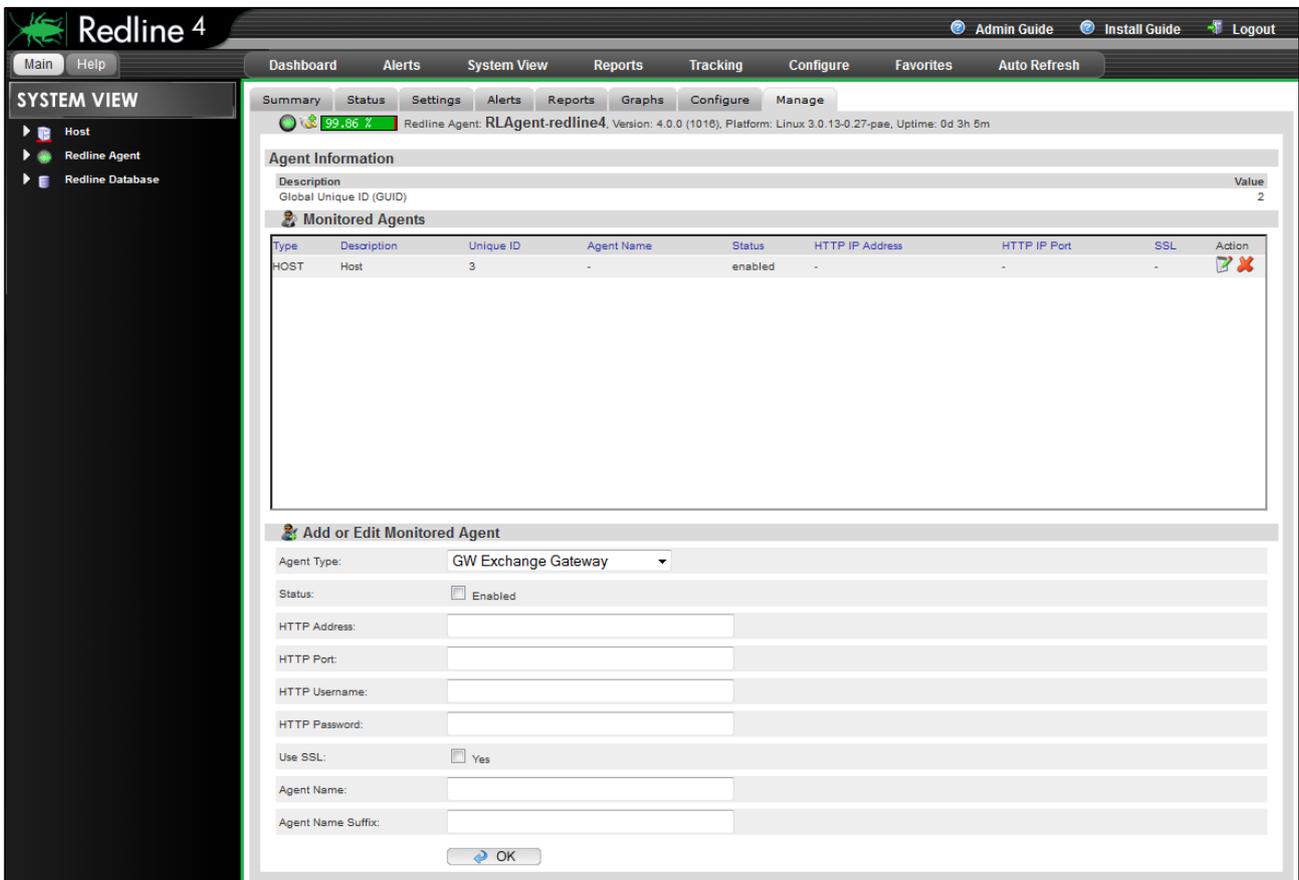
Test by opening a web browser by typing <http://ipaddress:httpPort>. For example, if the agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 9999, <http://192.168.2.3:9999>. You should be prompted for the username and password just assigned

- Do not proceed until this is working

If you want to have accounting information for reports and message tracking, enable “Accounting” and specify a gateway accountant. The accounting log files will be sent to this user and can be imported into Redline via SOAP automatically.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Exchange Gateway. Specify the IP Address, Port, Username and Password.

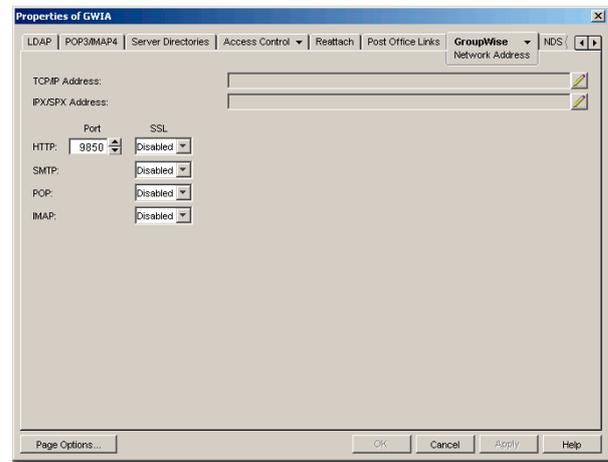


After 2-3 minutes, a message should appear on the Redline Agent that the Exchange Gateway has been registered to the Control Center and shows up in the Control Center.

GroupWise Internet Agent (GWIA)

Begin by writing down the IP address for this component. Record this information on your worksheet. Open the GWIA object in ConsoleOne, and go to the GroupWise/Network Address tab.

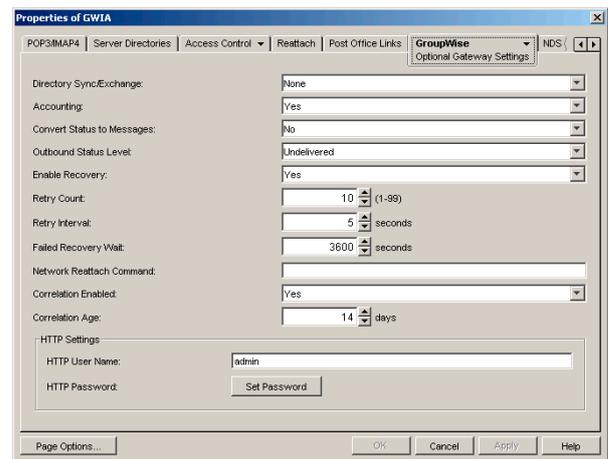
Ensure SSL is disabled and that the HTTP port is assigned (the default is 9850). Note this port for the work sheet as well.



The screenshot shows the 'Properties of GWIA' dialog box with the 'Network Address' tab selected. The 'TCP/IP Address' and 'IPX/SPX Address' fields are empty. The 'Port' is set to 9850. The 'SSL' dropdown is set to 'Disabled'. Other protocols like SMTP, POP, and IMAP are also set to 'Disabled'. Buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help' are visible at the bottom.

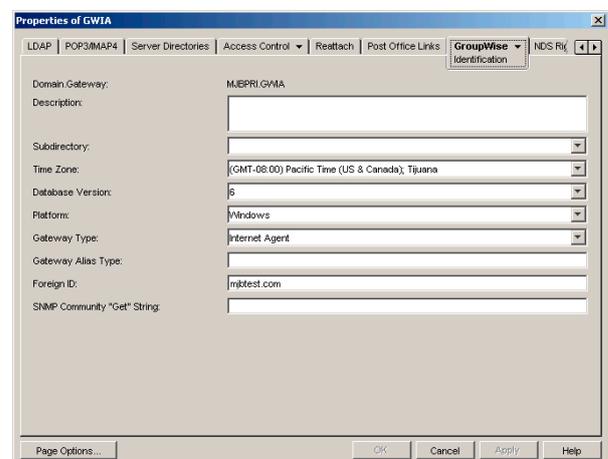
Next, select the GroupWise/Optional Gateway Settings tab.

Assign a HTTP username and password. This should not be the same as a valid eDirectory account. Include this information in the work sheet as well.



The screenshot shows the 'Properties of GWIA' dialog box with the 'Optional Gateway Settings' tab selected. Fields include 'Directory Sync/Exchange' (None), 'Accounting' (Yes), 'Convert Status to Messages' (No), 'Outbound Status Level' (Undelivered), 'Enable Recovery' (Yes), 'Retry Count' (10), 'Retry Interval' (5 seconds), 'Failed Recovery Wait' (3600 seconds), 'Network Reattach Command' (empty), 'Correlation Enabled' (Yes), and 'Correlation Age' (14 days). The 'HTTP Settings' section has 'HTTP User Name' set to 'admin' and a 'Set Password' button. Buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help' are at the bottom.

Select the GroupWise Identification tab. SNMP is automatically enabled for the GWIA, but you should assign a community name here (other than public or blank, which present security risks). Click OK to save your settings. Wait one minute for the GroupWise configuration to propagate. Test in a browser by typing <http://ipaddress:httpPort>



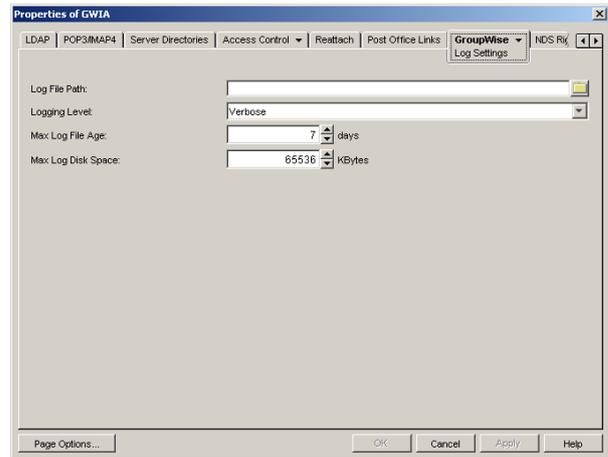
The screenshot shows the 'Properties of GWIA' dialog box with the 'Identification' tab selected. Fields include 'Domain Gateway' (MJEPR1.GWIA), 'Description' (empty), 'Subdirectory' (empty), 'Time Zone' ((GMT-08:00) Pacific Time (US & Canada), Tijuana), 'Database Version' (5), 'Platform' (Windows), 'Gateway Type' (Internet Agent), 'Gateway Alias Type' (empty), 'Foreign ID' (mjbtest.com), and 'SNMP Community "Get" String' (empty). Buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help' are at the bottom.

For example if the GWIA were running on a server with an IP address of 192.168.2.3, and an HTTP port of 9850, <http://192.168.2.3:9850>

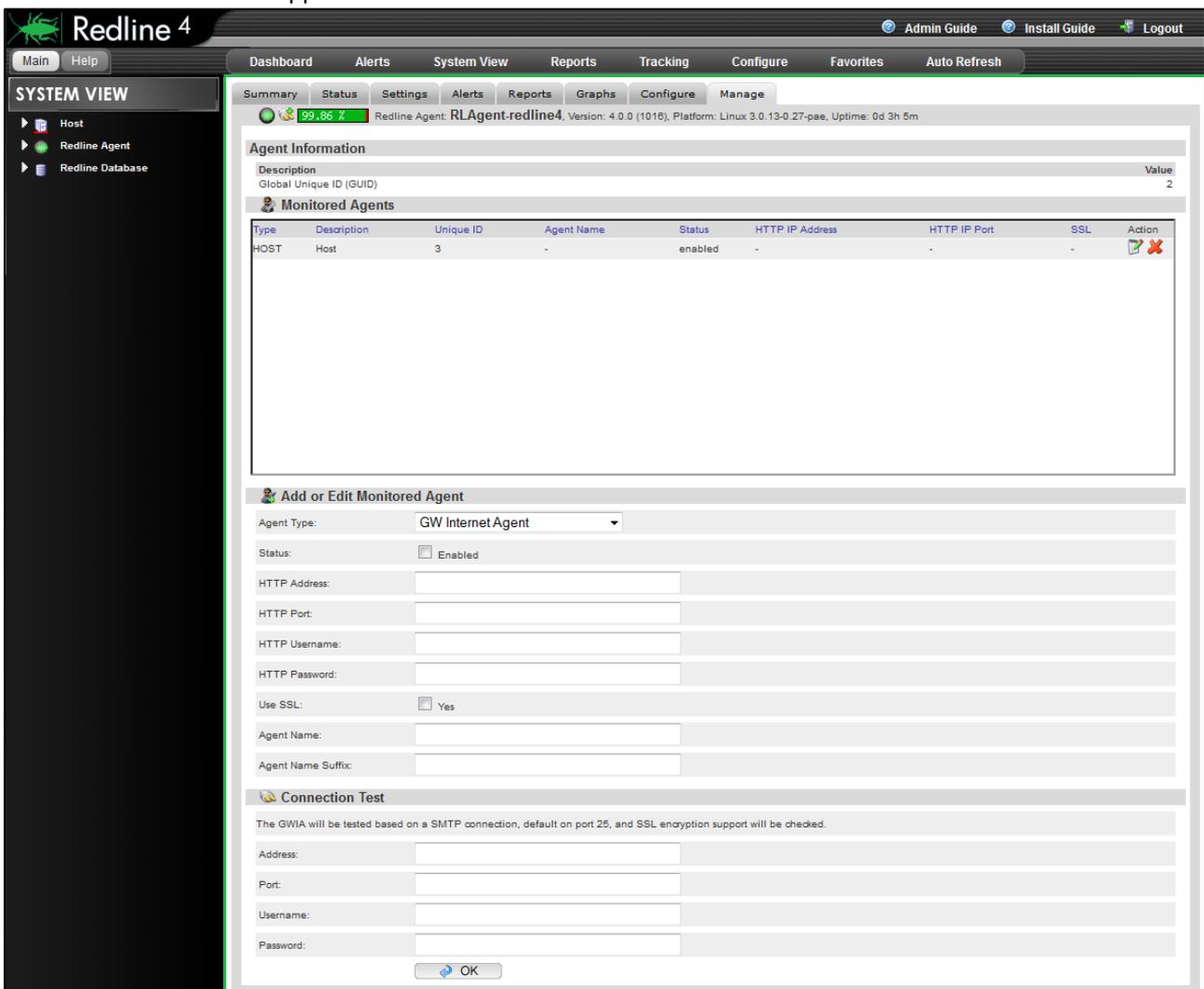
You should be prompted for the username and password just assigned. If this does not occur, recheck the settings in ConsoleOne, and open the agent's startup file to verify that no startup switches have overridden this configuration. Also, try restarting the agent.

- Do not proceed until this is working

Return to ConsoleOne and reopen the agent. Go to the GroupWise/Log Settings tab to verify logging is on and set to verbose.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Internet Agent. Specify the IP Address, Port, Username and Password. Optionally, you can enable a connection test, which will connect to the SMTP port every 2 minutes and tests the gateway for availability and if SSL over SMTP is supported or not.



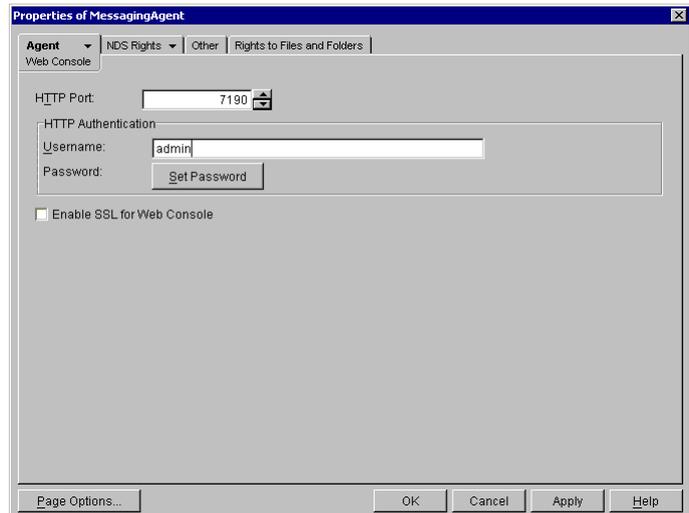
After 2-3 minutes, a message should appear on the Redline Agent that the Internet Agent has been registered to the Control Center and shows up in the Control Center.

Novell Messenger Agent

Begin by including the IP address for this component on the work sheet. Open the Messaging Agent object in ConsoleOne, and go to the Agent/Web Console tab.

Ensure SSL is disabled and that the HTTP port is assigned (the default is 8311). Note this port on the work sheet as well.

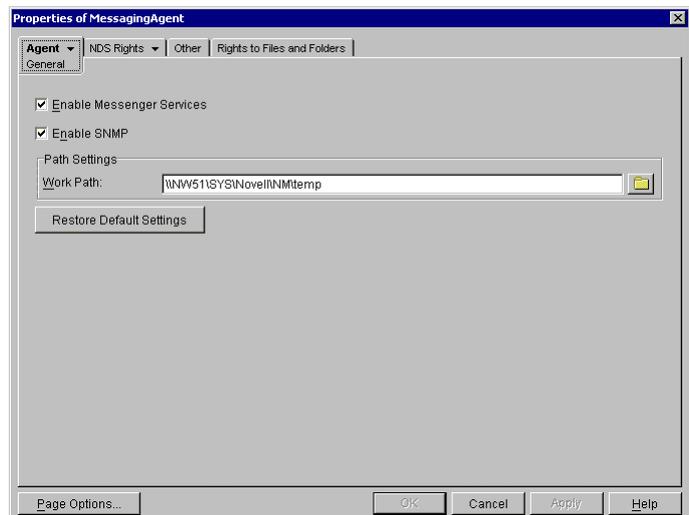
Assign a HTTP username and password. This should not be the same as a valid eDirectory account. Include this information in the work sheet as well.



Next, select the Agent/General tab. Ensure SNMP is enabled.

Click OK to save your settings. Wait one minute for the GroupWise configuration to propagate and then test by opening a web browser by typing <http://ipaddress:httpPort>

For example if the Messenger agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 8311, <http://192.168.2.3:8311>

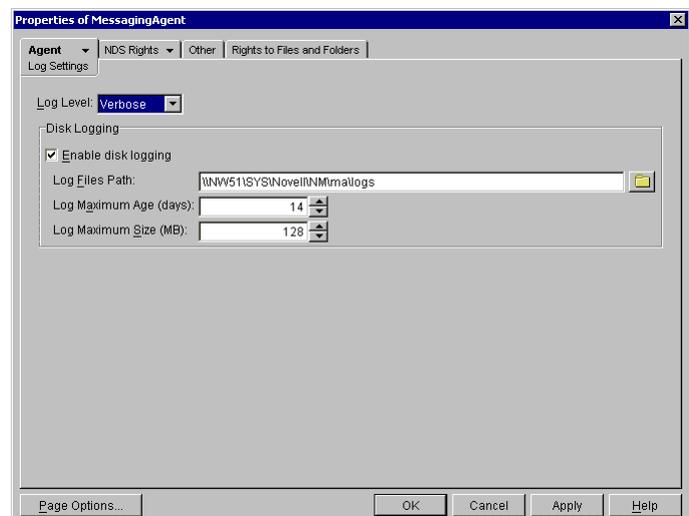


You should be prompted for the username and password just assigned. If you are not, recheck your settings in ConsoleOne, and open the agent's startup file to verify that no startup switches override this configuration. Also, try restarting the agent.

- Do not proceed until this is working

Return to ConsoleOne and reopen the agent.

Go to the Agent/Log Settings tab to verify logging to disk is on and set to verbose.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Messenger Agent. Specify the IP Address, Port, Username and Password.

The screenshot displays the Redline 4 web interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'System View' section is active, showing a sidebar with 'Host', 'Redline Agent', and 'Redline Database'. The main content area is titled 'Agent Information' and shows a 'Monitored Agents' table with one entry: 'HOST' with a Unique ID of 3 and Status 'enabled'. Below the table is a form titled 'Add or Edit Monitored Agent' with fields for Agent Type (Novell Messenger Agent), Status (Enabled), HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL (Yes), Agent Name, and Agent Name Suffix. An 'OK' button is at the bottom of the form.

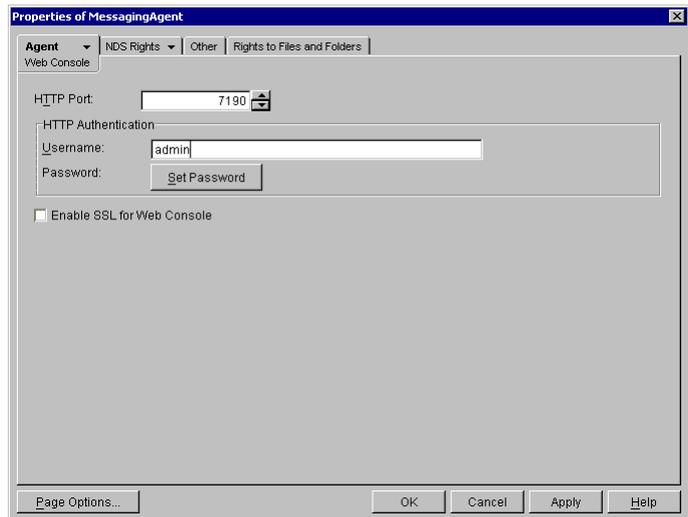
After 2-3 minutes, a message should appear on the Redline Agent that the Messenger Agent has been registered to the Control Center and shows up in the Control Center.

Novell Messenger Archive Agent

The Messenger Archiving Agent is configured almost identically – Open the Archiving Agent object in Console One, and go to the Agent/Web Console tab.

Assign a HTTP username and password. This should not be the same as a valid eDirectory account. Write down this information in the work sheet as well.

Ensure SSL is disabled and that the HTTP port is assigned (the default is 8313). Note this port in the work sheet.

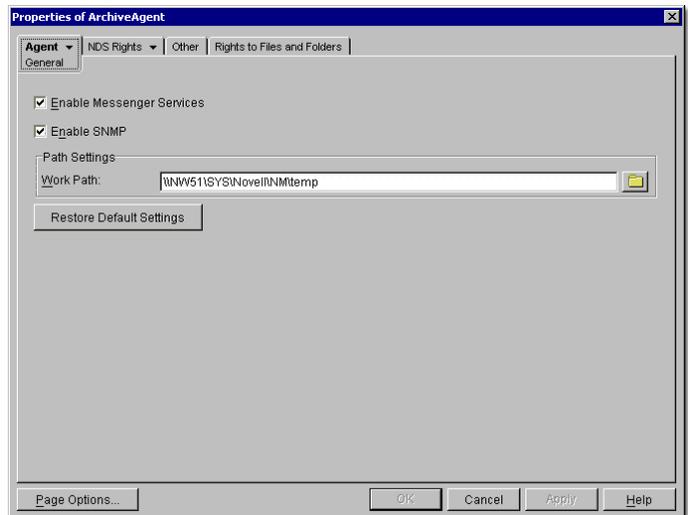


Next, select the Agent/General tab. Ensure SNMP is enabled.

Click OK to save your settings. Wait one minute for the GroupWise configuration to propagate.

Test it in a web browser by typing <http://ipaddress:httpPort>

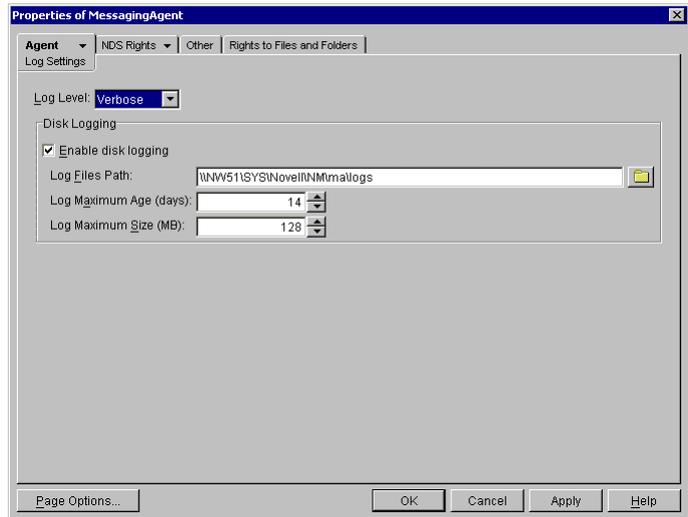
For example if the Archiving agent were running on a server with an IP address of 192.168.2.3 and an HTTP port of 8313: <http://192.168.2.3:8313>



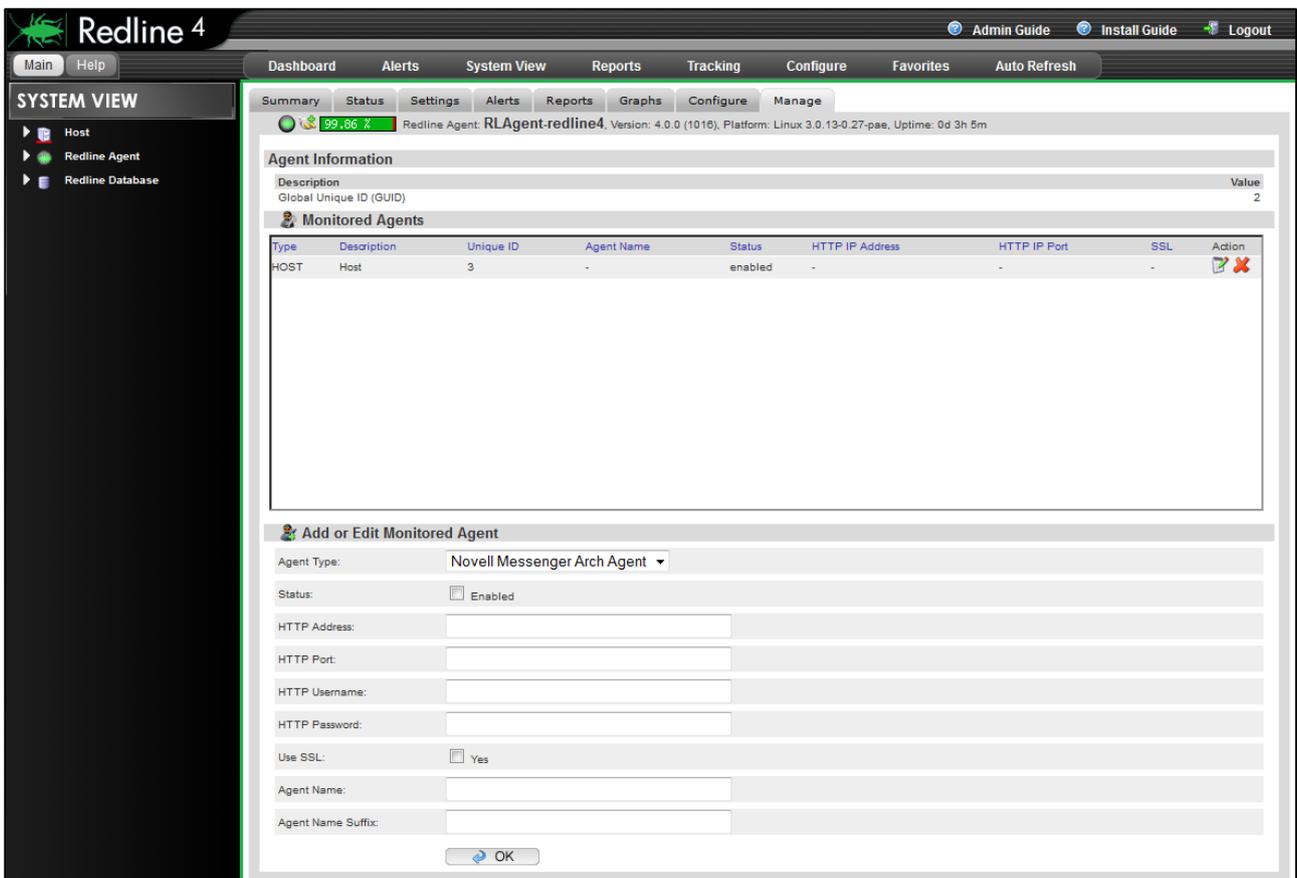
You should be prompted for the username and password just assigned. If you are not, recheck your settings in ConsoleOne, and open the agent's startup file to verify that no startup switches override this configuration. Also, try restarting the agent.

- Do not proceed until this is working

Return to ConsoleOne and reopen each of the agents. Go to the Agent/Log Settings tab to verify logging to disk is on and set to verbose.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Messenger Archive Agent. Specify the IP Address, Port, Username and Password.



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

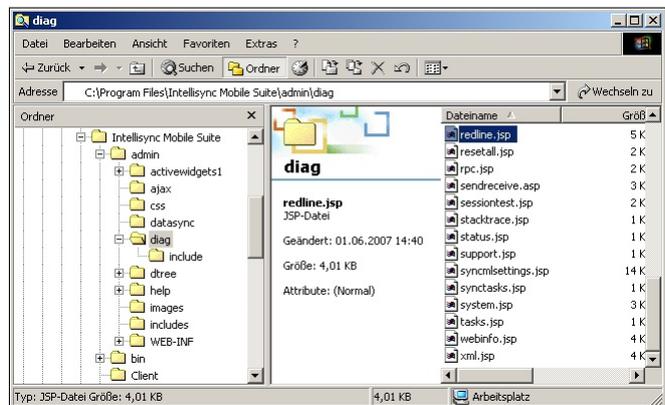
GroupWise Mobile Server

Since Version 7.0.1 Novell ships the GroupWise Mobile Server, which is used to connect mobile devices like PDA's, phones etc to GroupWise.

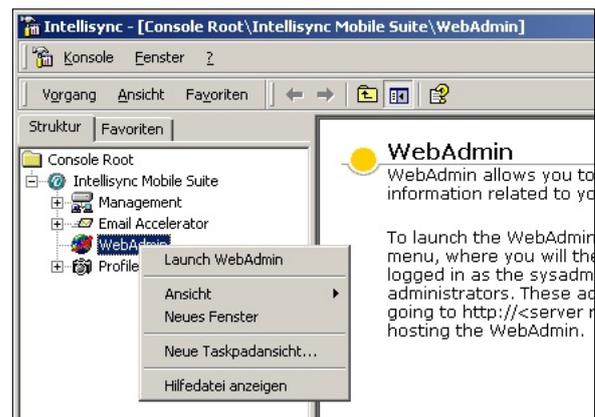
Redline ships with configuration files for GroupWise Mobile Server 2.x/3.x, and the files must be copied into the GroupWise Mobile Server.

If you are running GW Mobile Server 2, copy the file `.../redline/conf/GWMobileServer/redline.jsp` and `.../redline/conf/GWMobileServer/rlaccounts.jsp` to your Mobile Server Program Files/Intellisync Mobile Suite/admin/diag folder.

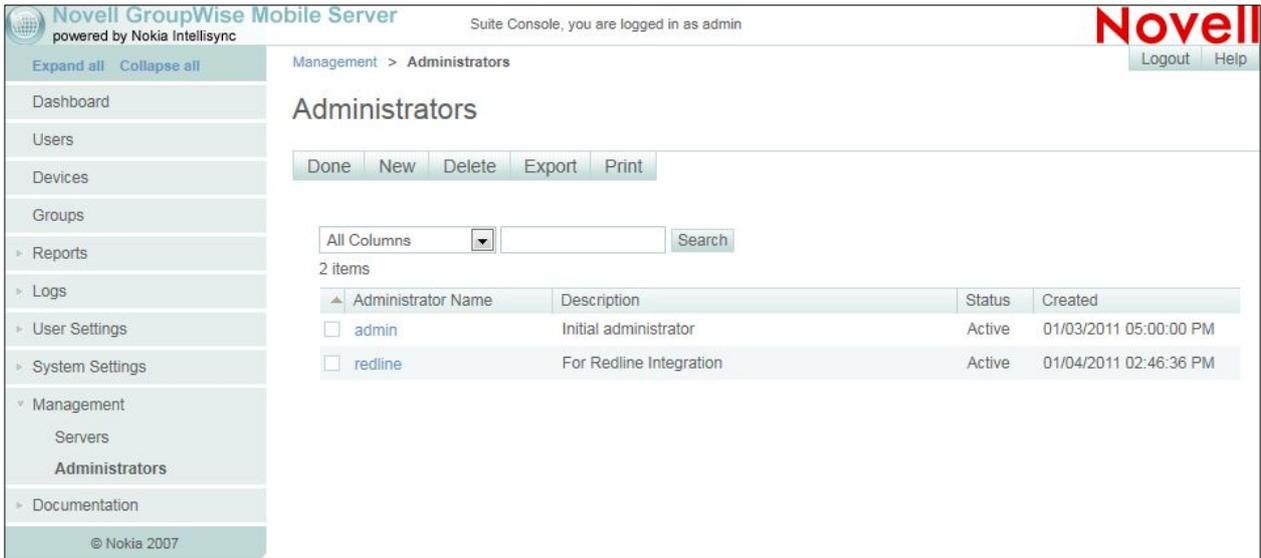
On Linux, the files go in `/opt/ims/www/admin/diag`.



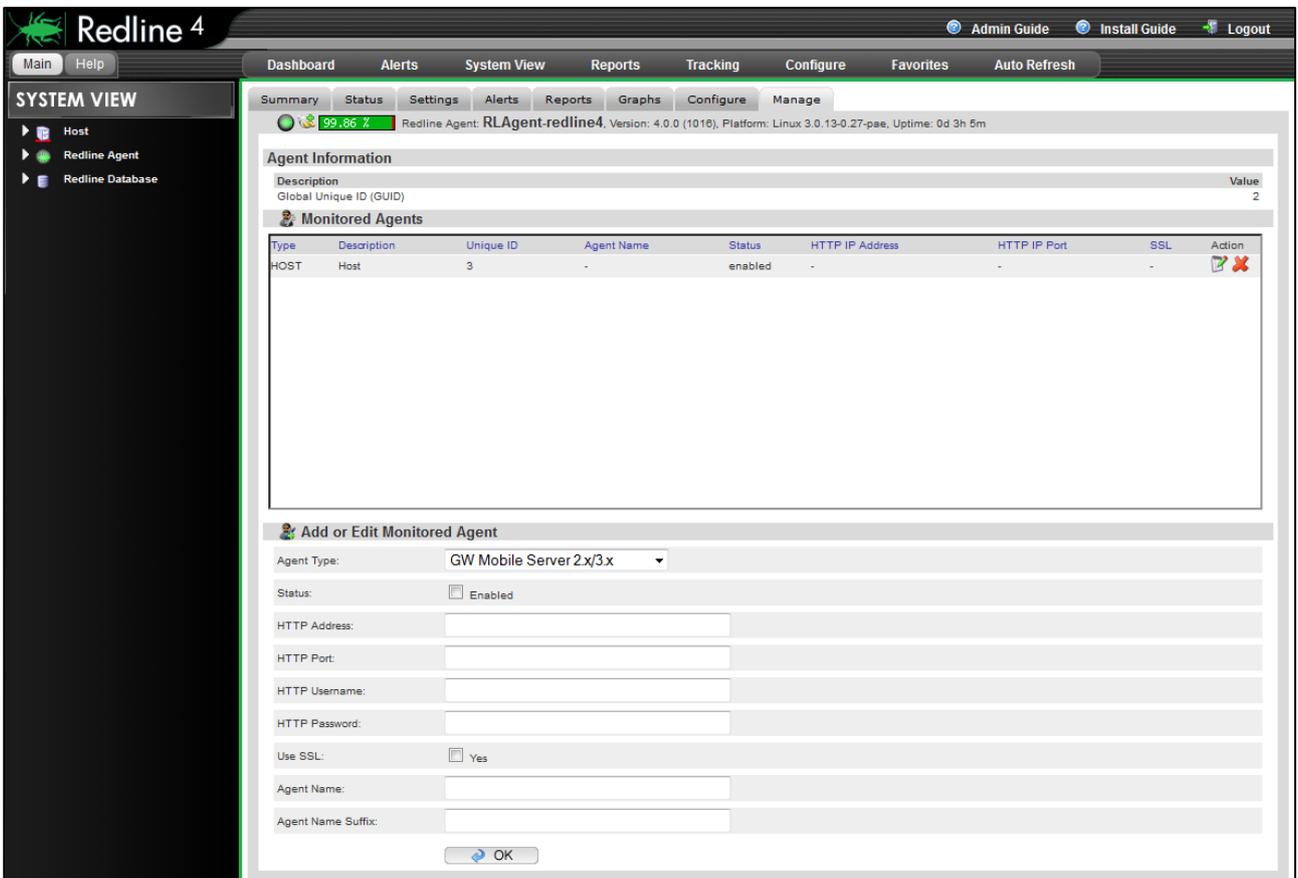
For Redline to access this file it is necessary to create a new administrator account. Start the Intellisync Admin Console, right click on WebAdmin and select Launch WebAdmin.



In WebAdmin, select Administrators and create a new Administrator which will be used in Redline.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Mobile Server. Specify the IP Address, Port, Username and Password. Make sure that you select GW Mobile Server 2x/3x, depending on what Version you are running.



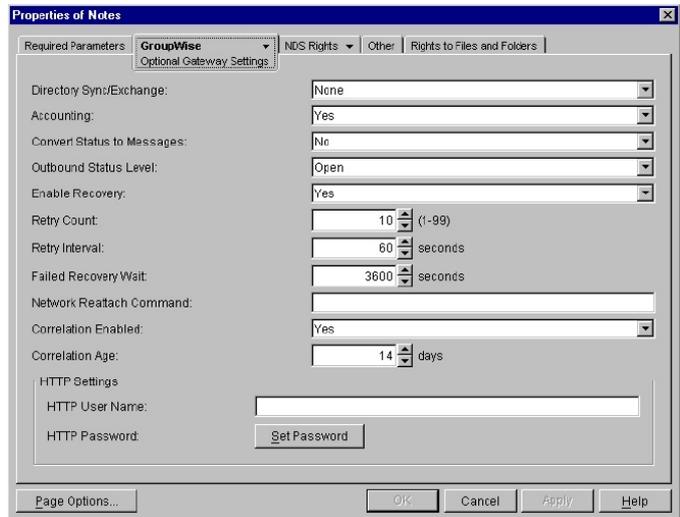
After 2-3 minutes, a message should appear on the Redline Agent that the GW Mobile Server has been registered to the Control Center and shows up in the Control Center.

GroupWise Notes Gateway

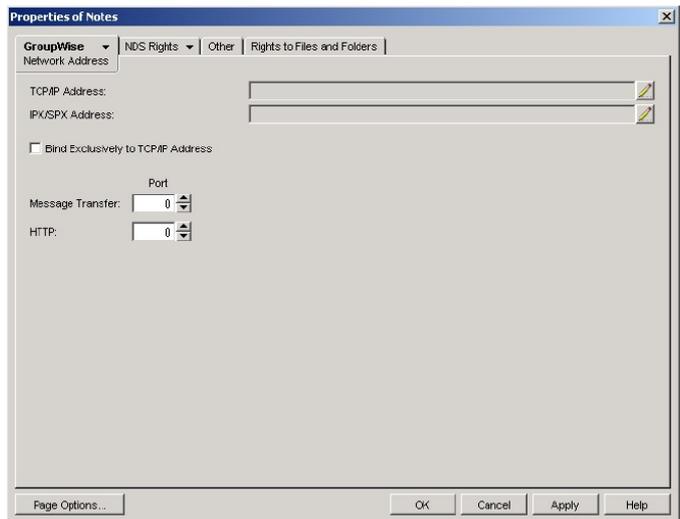
The Notes Gateway provides a http interface similar to most other GroupWise Agents. You need to enable and configure this interface via ConsoleOne. Specify a username and password for the Notes Gateway in the GroupWise/Optional Gateway Settings tab.

Optional you can configure the http interface by editing the agent configuration file, which is notes.cfg by default and located in the same folder as the Notes Gateway binary file. The following switches need to be added.

- /http - Enable HTTP Interface
- /httpport-portnumber - HTTP port to listen on (There is no default port, we suggest 7175)
- /httpuser-[username] - Specify the Username for the HTTP interface
- /httppassword-[password] - specify the Password for the HTTP interface
- /loglevel-verbose – turns on verbose logging



Save the file and restart the agent by unloading and reloading.



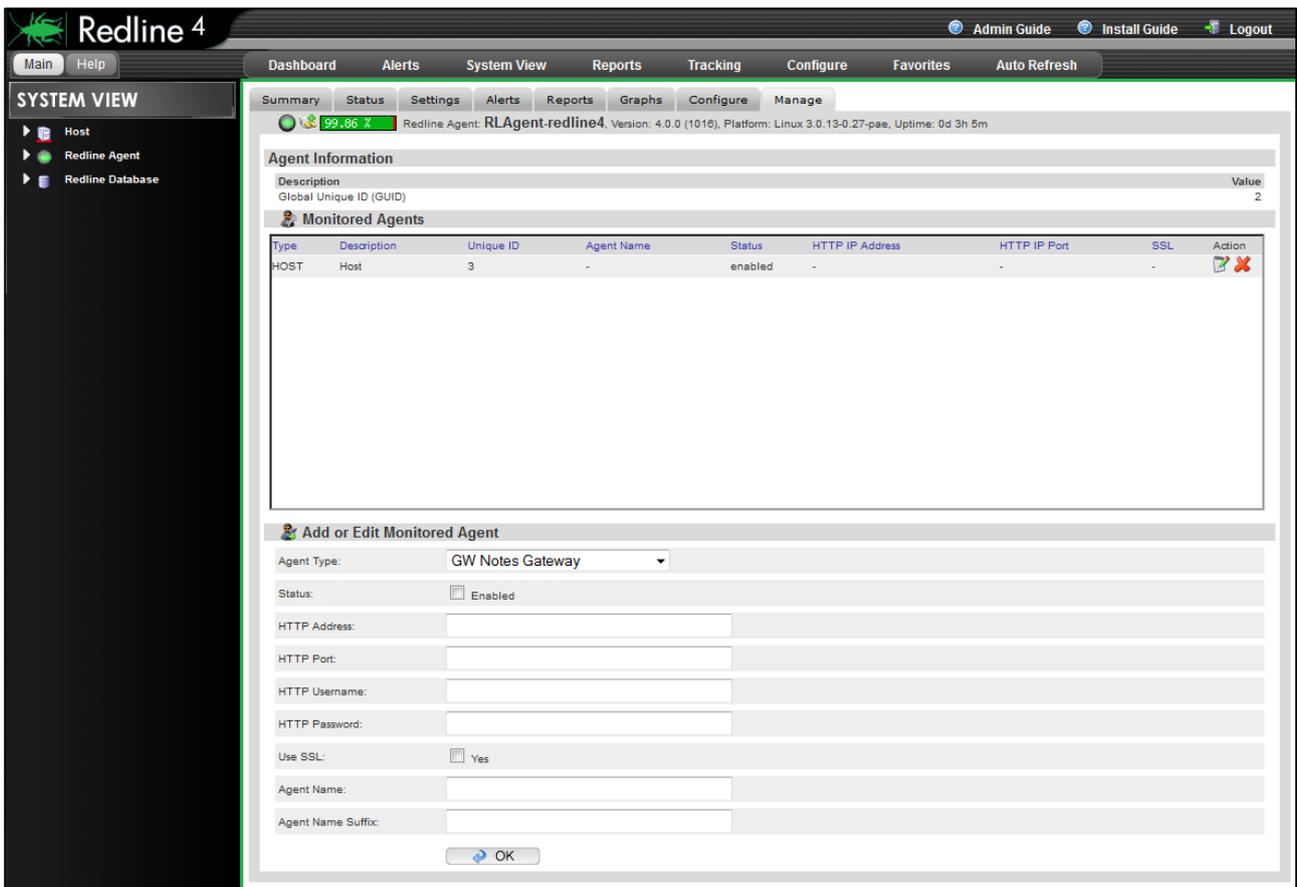
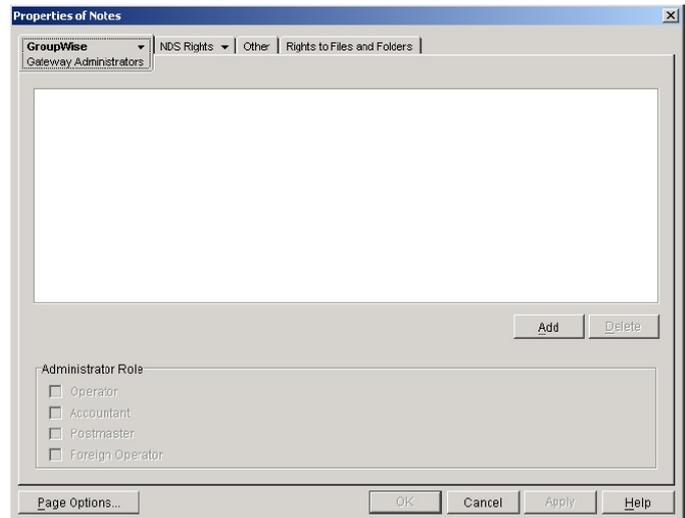
Test by opening a web browser by typing <http://ipaddress:httpPort>. For example, if the agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 9999, <http://192.168.2.3:9999>. You should be prompted for the username and password just assigned

- Do not proceed until this is working

If you want to have accounting information for reports and message tracking, enable “Accounting” and specify a gateway accountant.

The accounting log files will be sent to this user and can be imported into Redline via SOAP automatically.

From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Notes Gateway. Specify the IP Address, Port, Username and Password.



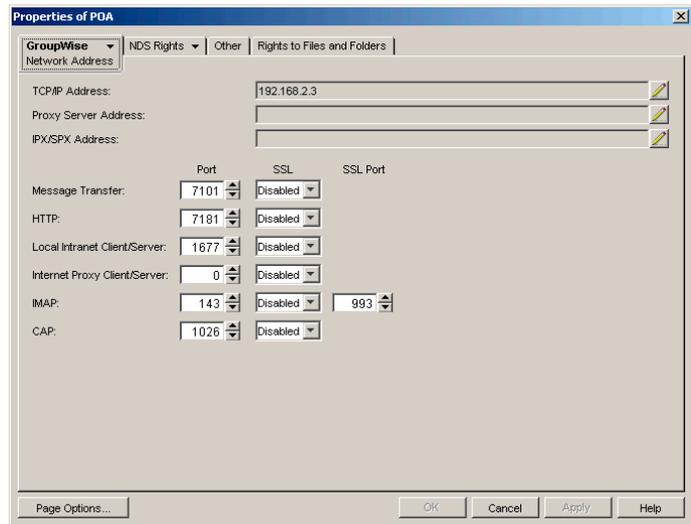
After 2-3 minutes, a message should appear on the Redline Agent that the Notes Gateway has been registered to the Control Center and shows up in the Control Center.

GroupWise Post Office Agent

Begin by writing down the IP address for this component on the work sheet provided in the [Appendix](#).

Open the POA object in ConsoleOne, and go to the GroupWise/Network Address tab.

Ensure SSL is disabled and that the HTTP port is assigned (the default is 7181). Note this port on the work sheet as well.

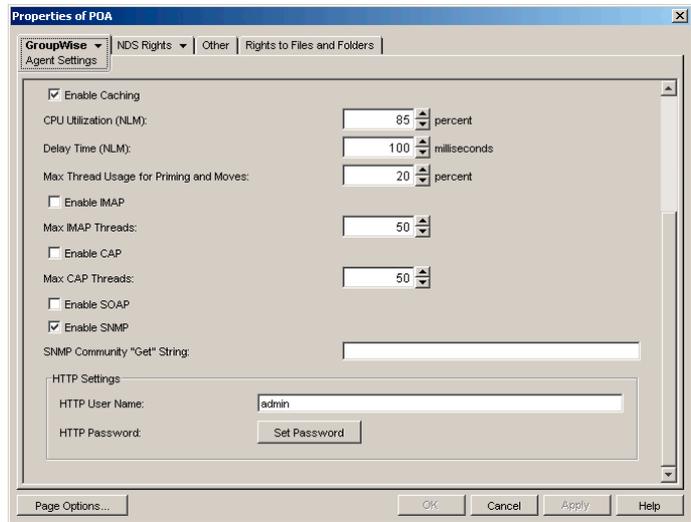


Next, select the GroupWise/Agent Settings tab. Assign an HTTP username and password. This should not be the same as a valid eDirectory account.

Write down this information in the work sheet as well.

Make sure SNMP is turned on. You probably want to assign a community name, other than public or blank (which defaults to public), to reduce the security risk.

Click OK to save your settings.



Testing

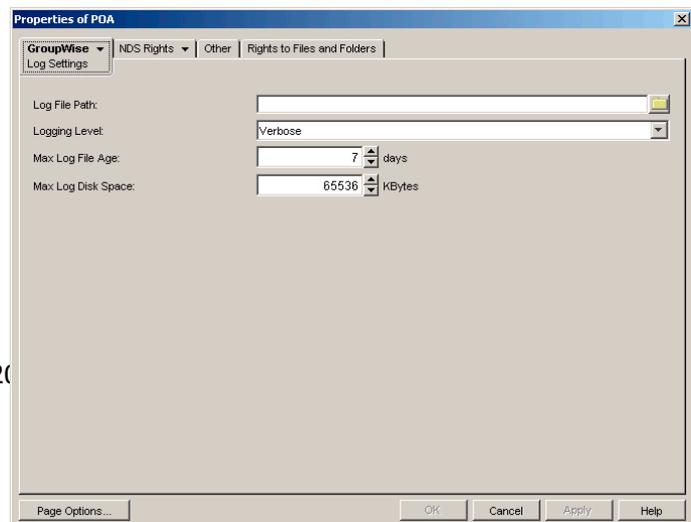
Wait one minute for the GroupWise configuration to propagate. Test in a web browser by typing: <http://ipaddress:httpPort>

For example if the POA were running on a server with an IP address of 192.168.2.3, and an HTTP port of 7181, <http://192.168.2.3:7181>

You should be prompted for the username and password just assigned. If this does not occur, recheck the settings in ConsoleOne, and open the agent's startup file to verify that no startup switches have overridden this configuration. Also, try restarting the agent.

- Do not proceed until this is working

Return to ConsoleOne and reopen the agent. Go to the GroupWise/Log Settings tab, and verify logging is both on and set to verbose. It



is not necessary to specify the Log File Path. GroupWise will use the default path.

Input the information which has been gathered to the worksheet into the agent configuration. The HTTP Address, Port, a username and password are all essential to monitoring the system.

The screenshot displays the Redline 4 web interface. The top navigation bar includes links for Admin Guide, Install Guide, and Logout. The main navigation menu on the left lists Host, Redline Agent, and Redline Database. The main content area is titled 'SYSTEM VIEW' and shows the following sections:

- Agent Information:** A table with columns for Description and Value. The row shows 'Global Unique ID (GUID)' with a value of 2.
- Monitored Agents:** A table with columns for Type, Description, Unique ID, Agent Name, Status, HTTP IP Address, HTTP IP Port, SSL, and Action. The row shows 'HOST' with a Unique ID of 3 and Status 'enabled'.
- Add or Edit Monitored Agent:** A form with fields for Agent Type (set to 'GW Post Office Agent'), Status (checkbox for 'Enabled'), HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL (checkbox for 'Yes'), Agent Name, and Agent Name Suffix.
- Connection Test:** A section with a description: 'The POA will be checked against the SOAP port and a login/logout to the defined account will be done.' It includes fields for Address, Port, Username, and Password, and an 'OK' button.

GWCHECK Scheduled Events in the GroupWise POA

Why are GWCHECK log files important?

GWCHECK log files are an important source of user information in Redline. In order to get this information in the correct way, some settings have to be configured in ConsoleOne. If these settings are not correct, incomplete data is created, or no data at all. Several reports depend on these.

GWCHECK always runs on the POA. If administrators want to have information from GWCHECK, they must configure the GWCHECK reports on every POA from which information is needed.

Redline requires three GWCHECK log files. Their default location is: <PathToYourPostOffice>/wpcsout/chk/

If these files are not generated in this folder, Redline will not be able to read and analyze them. The content of these GWCHECK files are different and provides different kinds of data for the reports. These three log files are:

gwaudit.log - GWCHECK Audit report

- User Name
- Post Office Name
- UserDB file
- Last Active date/time
- Inactive Days
- License Type

gwstats.log - GWCHECK Expire statistics

- User Name
- Post Office Name
- Full Name
- Mailbox Size
- Last DRN
- User MSG file
- Data Records
- Deleted Records
- Setup Records
- Record Bytes

mbstats.log - GWCHECK Mailbox statistics

- User Name
- Post Office Name
- Full Name
- UserDB file
- Last Active date/time
- License Type
- Messages Total
- Messages InBox
- Messages OutBox
- Messages Basket
- # of Mails
- # of Notes
- # of Tasks
- # of Appointments
- # of Phone Messages
- # of Profiles
- # of Attachments
- # of Search folders
- Mailbox Size
- Last DRN
- Data Records
- Record Bytes
- Max. Mailbox Size
- Mailbox Size Threshold

Creating the GWCHECK events

To create the reports, load Console One and open the POA properties. Go to the GroupWise/Scheduled Events tab. Three different jobs must be created, each under a collective entry of Redline Tasks.

If the Redline Tasks option doesn't already exist, click Create, and enter Name, Event Type, and Trigger information exactly as shown below. This instructs the GroupWise POA to generate these three log files once per day at 12:30 AM. We recommend a daily run of these Redline Tasks.

- Note - Until these GWCHECK run, many reports will be not be populated with data.
- Note - Do not use an Interval in GWCHECK - this feature is problematic.

When returning to this screen after configuring the GWCHECK options, ensure the checkbox next to Redline Tasks is enabled.

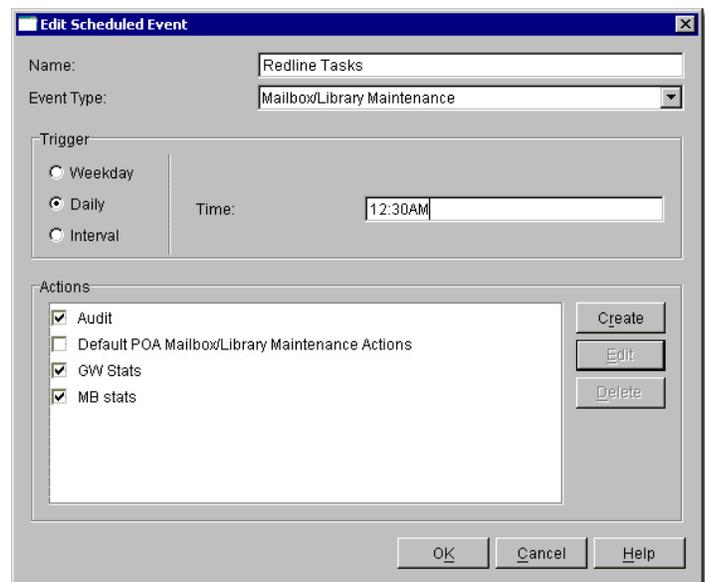
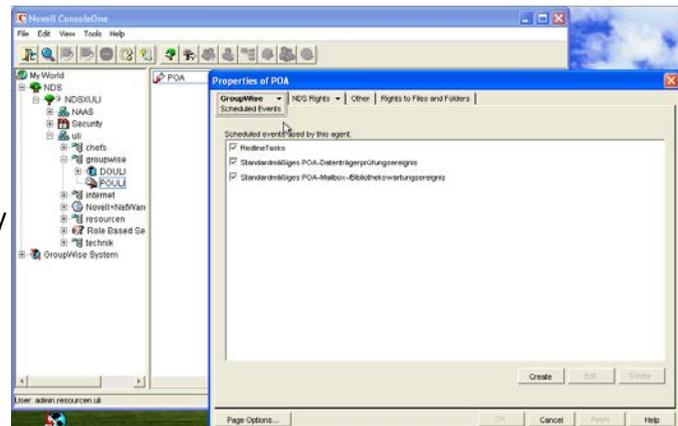
When creating Redline Tasks, a Default Maintenance task may appear in the Actions frame. It should be left unselected.

Individual GWCheck actions – Audit Report, GW Stats, and MB Stats, must also be created. See the next section for specifics.

Note - Remember to make sure all of the GWCHECK actions are enabled (the checkbox is selected) – when first created. These are disabled by default.

Check the Results tab while creating each of the three GWCHECK actions. Make sure that Logfile Results are NOT sent via e-mail to the Administrator. Otherwise the data is not stored to disk, and Redline has no access to it.

- Each GWCHECK action requires verbose logging to be enabled.



Audit Report (GWAUDIT.LOG)

- For the name, type in gwaudit
- Change the Action to Audit Report
- Click the Logging tab and enter gwaudit.log Check the box for Verbose logging
- Click the Results tab and make sure that nothing is checked
- Click OK to confirm your changes or Cancel to leave your settings unchanged

The screenshot shows the 'Scheduled Event Action' dialog box. The 'Name' field contains 'Audit Report'. The 'Action' dropdown menu is set to 'Audit Report'. Below this, there is a section 'Show accounts without activity for previous' with a spinner box set to '60' and the unit 'days'. At the bottom, the 'Logging' tab is selected, showing 'Log File: gwaudit.log' and a checked checkbox for 'Verbose logging'. There are 'OK', 'Cancel', and 'Help' buttons on the right side.

Mailbox Statistics (GWSTATS.LOG)

- For the name, type gwstats
- Change the Action to Mailbox Statistics
- Click the Logging tab and enter gwstats.log Check the box for Verbose logging
- Click the Results tab and make sure that nothing is checked
- Click OK to confirm your changes or Cancel to leave your settings unchanged

The screenshot shows the 'Scheduled Event Action' dialog box. The 'Name' field contains 'GW Stats'. The 'Action' dropdown menu is set to 'Mailbox Statistics'. Under 'Mailbox Statistics', the 'Box limit' is set to '500' items. There are several options for 'Expire Statistics' with spinner boxes: 'Items older than' (60 days), 'Downloaded items older than' (30 days), 'Items larger than' (1000 KB), and 'Reduce mailbox to' (5000 KB). There are also checkboxes for 'Reduce mailbox to limited size', 'Received items', 'Sent items', 'Calendar items', 'Only backed-up items', and 'Only retained items'. At the bottom, the 'Logging' tab is selected, showing 'Log File: gwstats.log' and a checked checkbox for 'Verbose logging'. There are 'OK', 'Cancel', and 'Help' buttons on the right side.

Mailbox analysis (MBSTATS.LOG)

- For the name, type in mbstats
- Change the Action to Mailbox Statistics
- Click the radio button for Expire Statistics
- Click the Logging tab and enter mbstats.log Check the box for Verbose logging
- Click the Results tab and make sure that nothing is checked
- Click OK to confirm your changes or Cancel to leave your settings unchanged

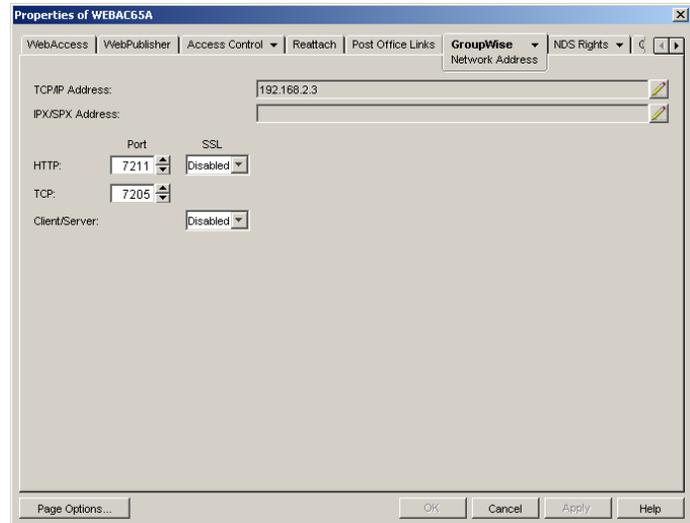
From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the Post Office Agent. Specify the IP Address, Port, Username and Password. In Addition to that it is possible to run a regular SOAP connection test on the Post Office. The Redline agent will try to connect to the SOAP port every 2 minutes, and generates a report if this is not possible.

After 2-3 minutes, a message should appear on the Redline Agent that the POA agent has been registered to the Control Center and the GroupWise Post Office shows up in the Control Center.

GroupWise WebAccess Agent

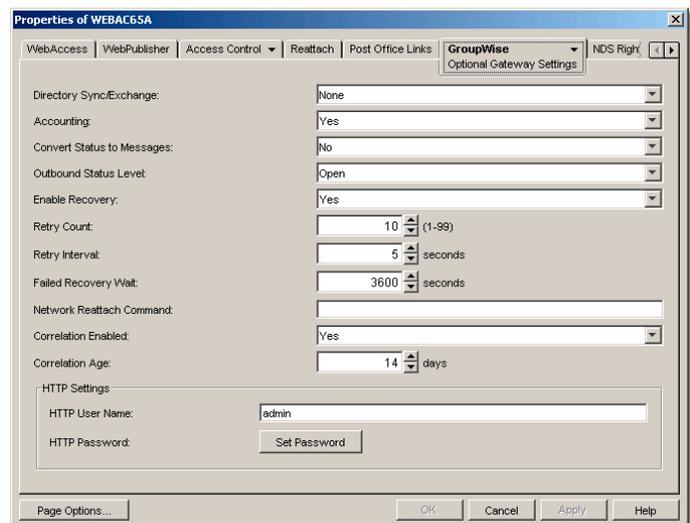
Begin by writing down the IP address for this component. Record this information on your worksheet. Open the WebAccess object in ConsoleOne, and go to the GroupWise/Network Address tab.

Ensure SSL is disabled and that the HTTP port is assigned (the default is 7211). This port should be noted in the work sheet as well.



Next, select the GroupWise/Optional Gateway Settings tab.

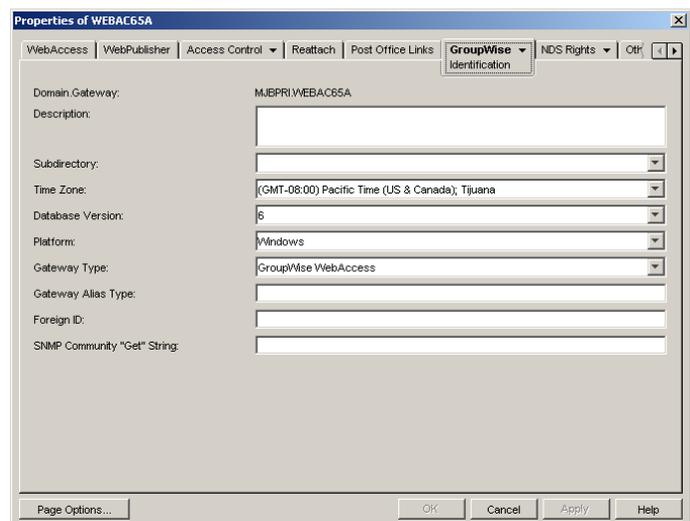
Assign a HTTP username and password. This should not be the same as a valid eDirectory account. Include this information in the work sheet as well.



Select the GroupWise Identification tab. SNMP is automatically enabled for the WebAccess, but you should assign a community name here (other than public or blank, which present security risks).

Click OK to save your settings. Wait one minute for the GroupWise configuration to propagate. Test in a browser by typing

<http://ipaddress:httpPort>

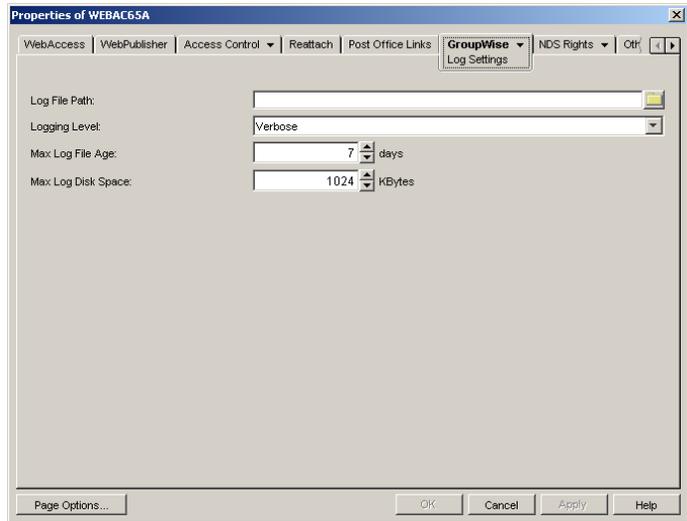


For example if the WebAccess agent were running on a server with an IP address of 192.168.2.3, and an HTTP port of 7211, <http://192.168.2.3:7211>

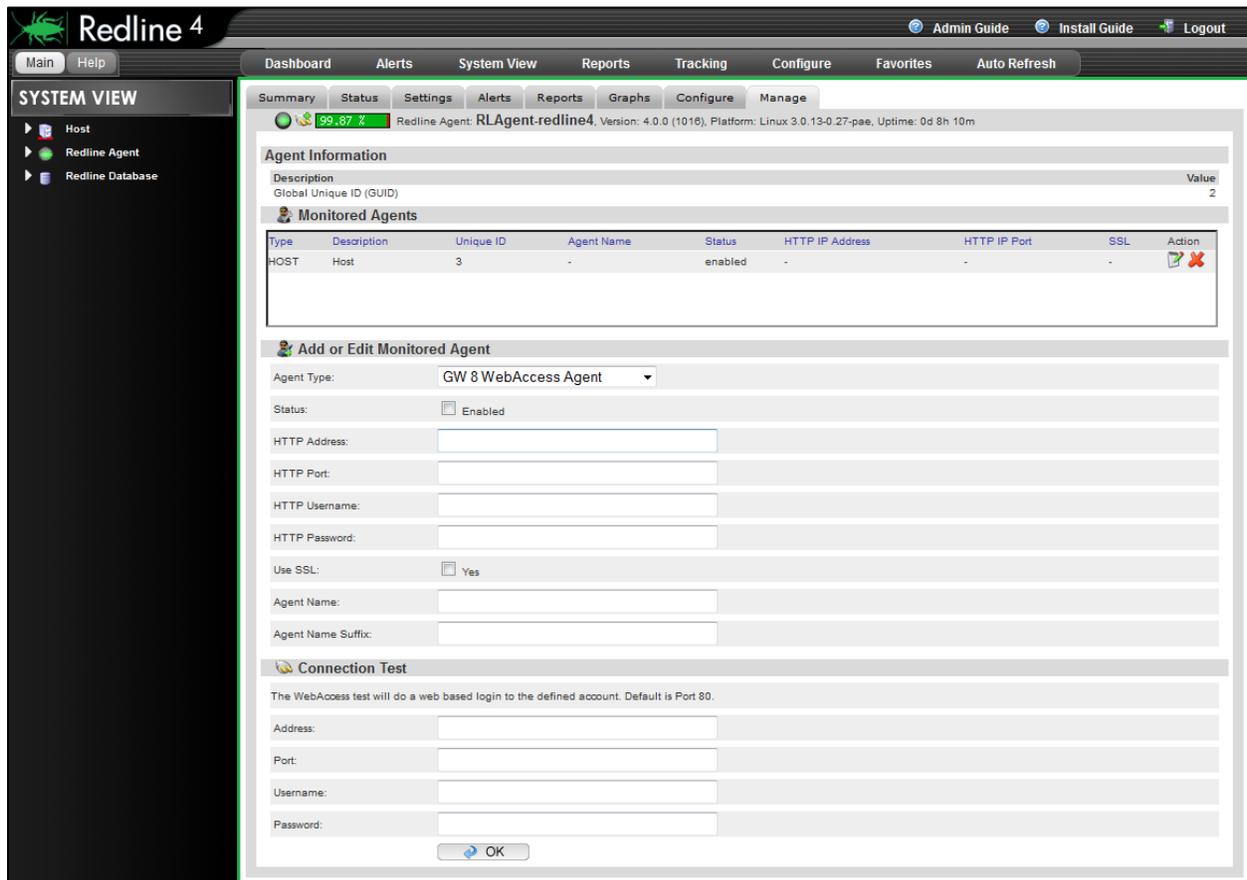
You should be prompted for the username and password just assigned. If this does not occur, recheck the settings in ConsoleOne, and open the agent's startup file to verify that no startup switches have overridden this configuration. Also, try restarting the agent.

- Do not proceed until this is working Return to ConsoleOne and reopen the agent. Go to the GroupWise/Log Settings tab, and verify logging is on and set to verbose.

- Note - Some versions of GroupWise will not write the WebAccess logs to disk unless the startup file (strtweb.ncf) is edited to add /logdiskon as a command line switch.



From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the WebAccess Agent. Specify the IP Address, Port, Username and Password. In Addition to that it is possible to run a regular connection test. The Redline agent will simulate logging in via a browser and try to do a full login every 2 minutes, and reports if this isn't possible.



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

GroupWise WebAccess Application

Beside the WebAccess Agent and the Document Viewer Agent you can monitor the WebAccess Application as well. In order to enable WebAccess Application monitoring, you need to configure the webacc.cfg file. This file is located here:

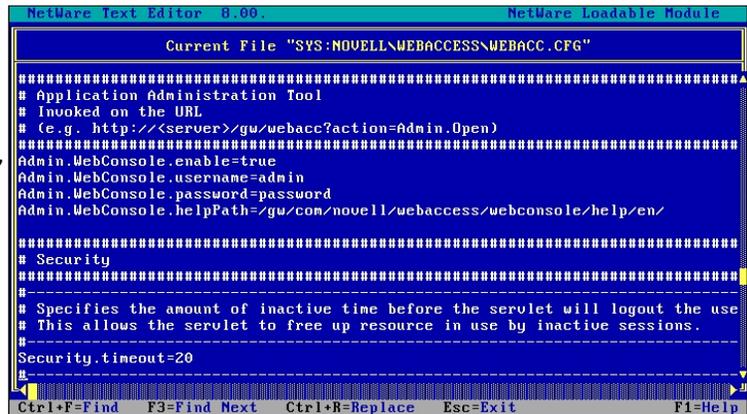
Windows and NetWare: novell\webaccess\
Linux: /opt/novell/groupwise/webaccess/

Enable the http server for the WebAccess Application by editing webacc.cfg. By default, the http interface is disabled.

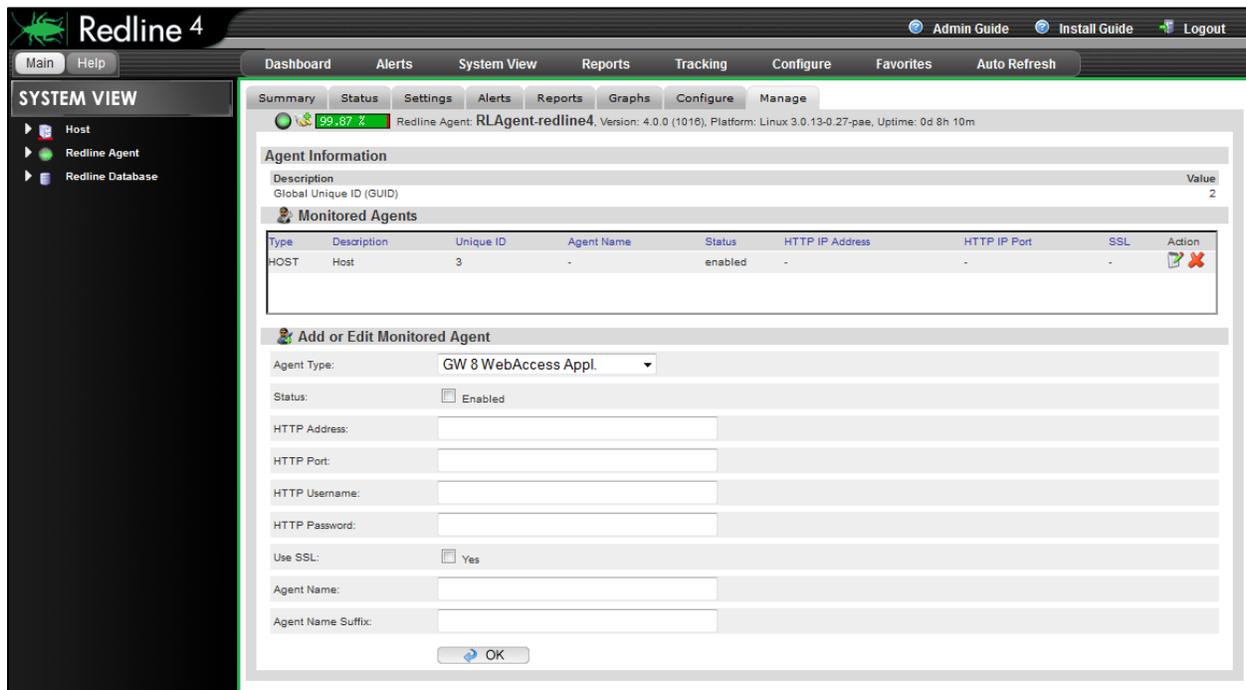
Restart JAVA in order to enable the http interface.

From the Redline Control Center, go to the System View and pick the Redline Agent

which will monitor the WebAccess Application. Specify the IP address, port, username and password.



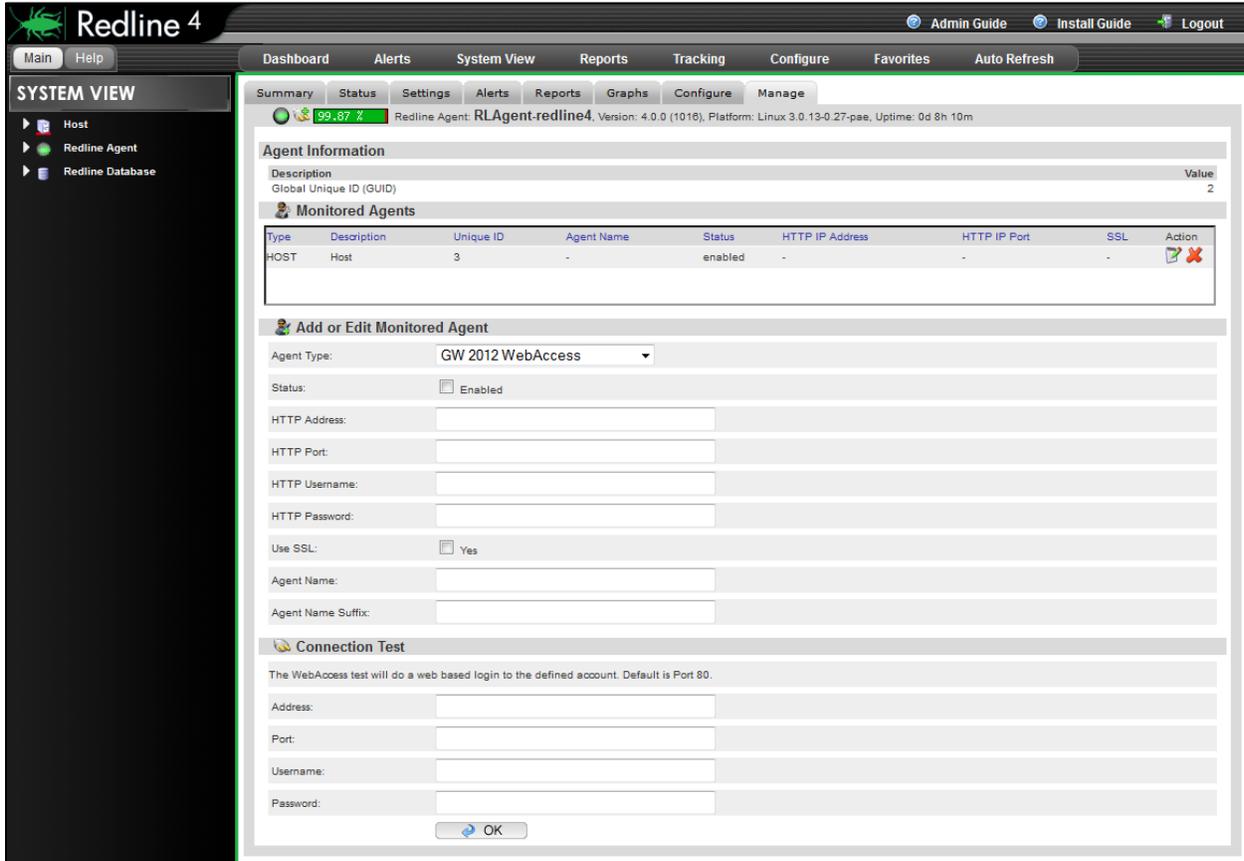
```
NetWare Text Editor 8.00. NetWare Loadable Module
Current File "SYS:NOVELL\WEBACCESS\WEBACC.CFG"
#####
# Application Administration Tool
# Invoked on the URL
# (e.g. http://<server>/gw/webacc?action=Admin.Open)
#####
Admin.WebConsole.enable=true
Admin.WebConsole.username=admin
Admin.WebConsole.password=password
Admin.WebConsole.helpPath=/gw/com/novell/webaccess/webconsole/help/en/
#####
# Security
#####
# Specifies the amount of inactive time before the servlet will logout the use
# This allows the servlet to free up resource in use by inactive sessions.
#####
Security.timeout=20
#####
Ctrl+F=Find F3=Find Next Ctrl+R=Replace Esc=Exit F1=Help
```



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

GroupWise WebAccess 2012

In GroupWise 2012, all WebAccess is monitored by the GW WebAccess 2012 option. Monitoring the GroupWise 2012 agent and application requires the same ConsoleOne settings as required for GroupWise 8.



The screenshot displays the Redline 4 web interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'System View' sidebar on the left shows a tree structure with 'Host', 'Redline Agent', and 'Redline Database'. The main content area is titled 'Redline Agent: RLAgent-redline4, Version: 4.0.0 (1018), Platform: Linux 3.0.13-0.27-pae, Uptime: 0d 8h 10m' and features a '99.87%' status indicator. Below this, the 'Agent Information' section shows a 'Global Unique ID (GUID)' of 2. The 'Monitored Agents' table lists one agent:

Type	Description	Unique ID	Agent Name	Status	HTTP IP Address	HTTP IP Port	SSL	Action
HOST	Host	3	-	enabled	-	-	-	

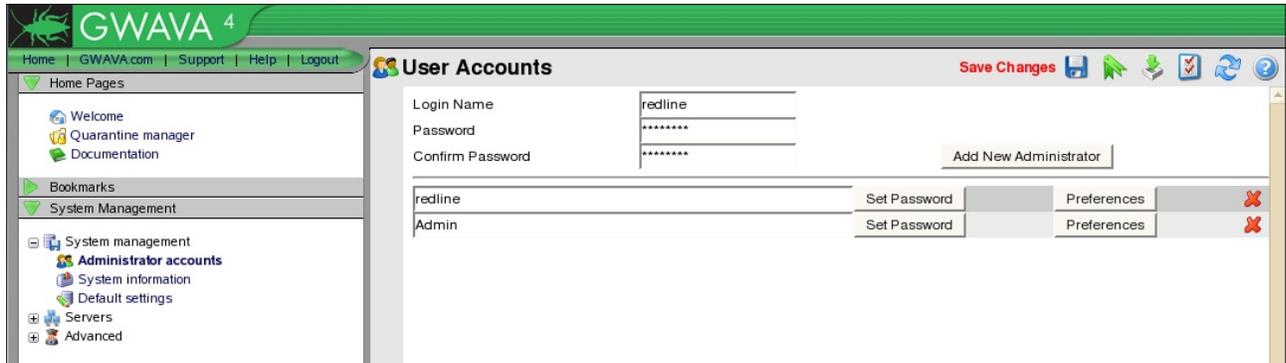
The 'Add or Edit Monitored Agent' form is visible, with the following fields and values:

- Agent Type: GW 2012 WebAccess
- Status: Enabled
- HTTP Address:
- HTTP Port:
- HTTP Username:
- HTTP Password:
- Use SSL: Yes
- Agent Name:
- Agent Name Suffix:

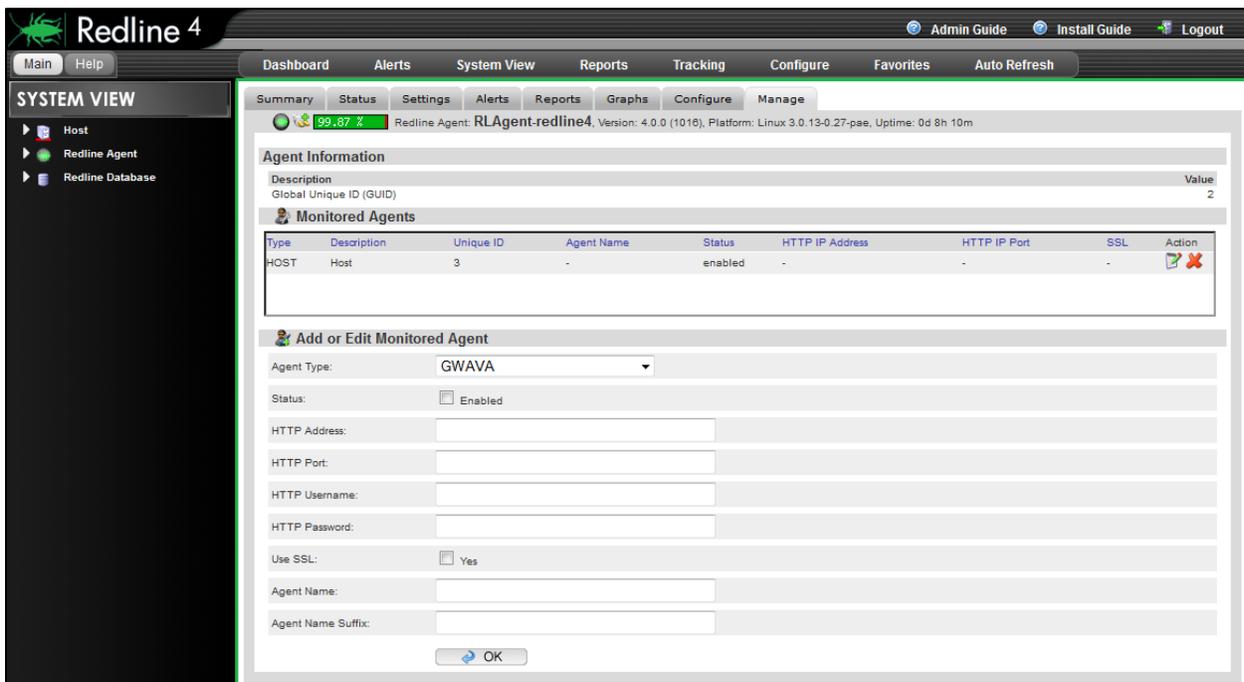
The 'Connection Test' section includes a description: 'The WebAccess test will do a web based login to the defined account. Default is Port 80.' and fields for Address, Port, Username, and Password, with an 'OK' button at the bottom.

GWAVA 4x / 5x / 6x

GWAVA 4 and higher are entirely web based and all that is necessary is to create an administrator account for Redline. Log into the web interface, go to System Management/Administrator accounts and specify the new username and password.



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



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

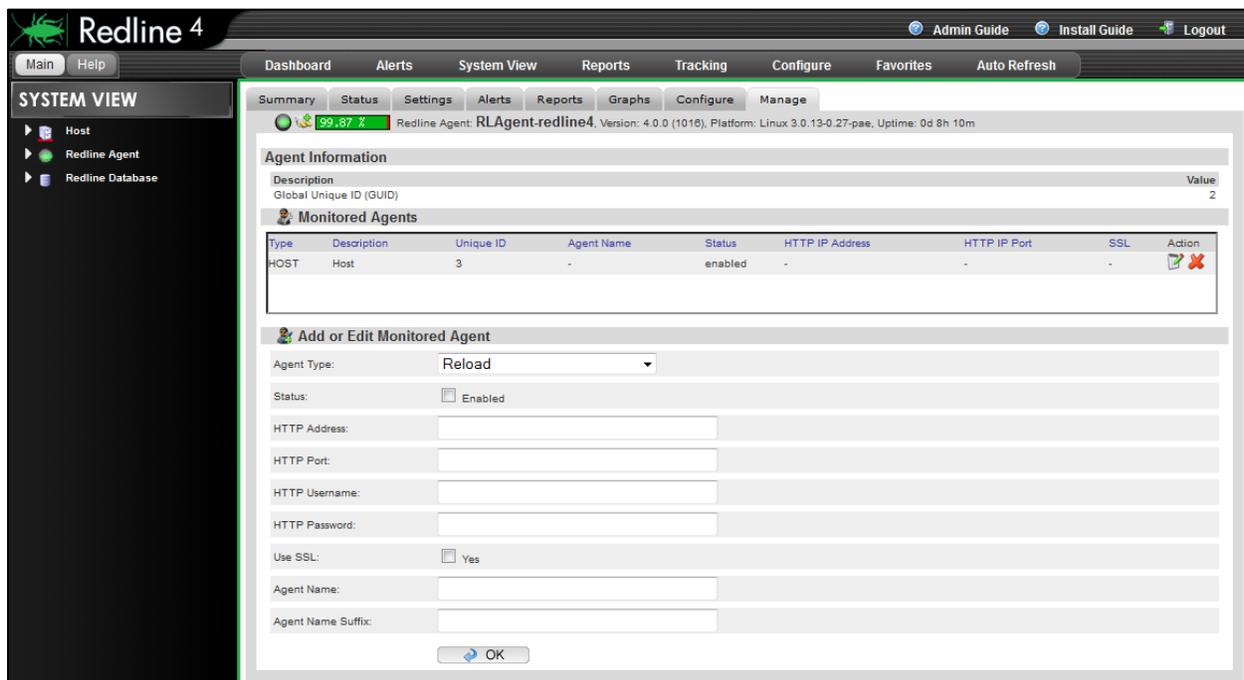
GWAVA Reload

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

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

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

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



The screenshot displays the Redline 4 web interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'SYSTEM VIEW' sidebar on the left shows a tree structure with 'Host', 'Redline Agent', and 'Redline Database'. The main content area is titled 'SYSTEM VIEW' and contains several sections:

- Summary:** Shows a green status indicator with '99.87%' and 'Redline Agent: RLAgent-redline4, Version: 4.0.0 (1016), Platform: Linux 3.0.13-0.27-pae, Uptime: 0d 8h 10m'.
- Agent Information:** A table with columns for Description and Value. The row shows 'Global Unique ID (GUID)' with a value of '2'.
- Monitored Agents:** A table with columns: Type, Description, Unique ID, Agent Name, Status, HTTP IP Address, HTTP IP Port, SSL, and Action. One entry is visible: Type: HOST, Description: Host, Unique ID: 3, Status: enabled, HTTP IP Address: -, HTTP IP Port: -, SSL: -, Action: [Refresh] [Delete].
- Add or Edit Monitored Agent:** A form with the following fields:
 - Agent Type: Reload (dropdown)
 - Status: Enabled
 - HTTP Address: [text input]
 - HTTP Port: [text input]
 - HTTP Username: [text input]
 - HTTP Password: [text input]
 - Use SSL: Yes
 - Agent Name: [text input]
 - Agent Name Suffix: [text input]

An 'OK' button is located at the bottom of the form.

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

GWAVA Retain

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

Because of the fact that 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.

The screenshot displays the Redline 4 web interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'SYSTEM VIEW' section is active, showing a sidebar with 'Host', 'Redline Agent', and 'Redline Database'. The main content area shows 'Agent Information' for 'RLAgent-redline4' with a 99.87% status. Below this is a 'Monitored Agents' table with one entry: 'HOST' with 'Host' description, '3' Unique ID, and 'enabled' status. At the bottom is a form titled 'Add or Edit Monitored Agent' with fields for Agent Type (Retain Server), Status (Enabled), HTTP Address, HTTP Port, HTTP Username, HTTP Password, Use SSL (Yes), Agent Name, and Agent Name Suffix.

After 2-3 minutes, a message should appear on the Redline 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 Redline.

GWAVA Reveal

Reveal is a powerful tool for examining the contents of a live GroupWise system and a Reload System. Authorized administrators may access any mailbox without special rights. To enable auditing security, GWAVA Reveal 1.1 or higher provides an option to produce auditing information and send it to the Redline Control Center automatically.

GWAVA Reveal

Configure auditing

Reveal will not work without proper auditing. This, to enforce existing business and legal policies.

Decide which auditing method to use

- Use Redline for auditing. If Redline becomes unavailable, auto-fallback to textfile auditing.
- Use Redline for auditing. If Redline becomes unavailable, shutdown Reveal.
- Use simple textfile auditing only.

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

Configure Redline auditing settings

Server IP address: 192.168.10.96

Server port: 6900

Server timeout (ms): 300

Registration name: ? X

Registration code: X

Redline

Redline - Complete GroupWise Monitoring and Reporting at your fingertips. More information [here](#)

Configure textfile auditing settings

Auditing directory: \\WW65\sys\tmp

Maximum logfile size (kb): 1024

Minimum free disk space (MB): 50

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

OK Cancel

After Redline is installed, in Reveal, go to Administration/Auditing Settings, and click the Lookup button. Provide the path to RLCENTER.CONF file of the server running the Redline 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 Redline Control Center IP Address and Port, as well the Registration Name and Code for Redline.

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

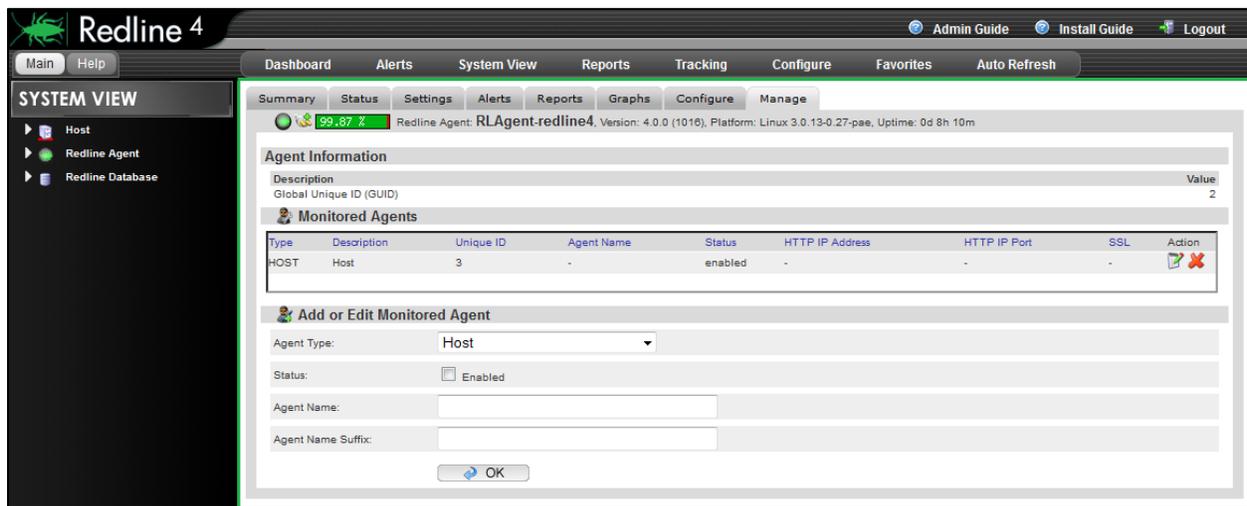
Host Platform

The Host monitoring agent is added automatically on install, though if the monitored agent is ever removed from the Redline system it can be re-added without hassle.

ONLY add the host if it is missing, or has been removed from the system.

Every host platform (Linux, NetWare, and Windows) is important for running applications on top of it. If something is not correct with the host, the application usually can't perform as it potentially would.

CPU speed, disk space, available memory, etc. are all important parameters. Every host where a Redline agent is running on can be monitored. In order to enable host monitoring, you only need to enable this through the Control Center web interface:



The screenshot displays the Redline 4 Control Center web interface. The top navigation bar includes links for Admin Guide, Install Guide, and Logout. The main menu contains Dashboard, Alerts, System View, Reports, Tracking, Configure, Favorites, and Auto Refresh. The left sidebar shows the SYSTEM VIEW with options for Host, Redline Agent, and Redline Database. The main content area is titled 'Agent Information' and shows the status of the Redline Agent (RLAgent-redline4) as '99.87%' with a green indicator. Below this, there is a table for 'Monitored Agents' with one entry: 'HOST' with a Unique ID of 3 and Status 'enabled'. At the bottom, there is a form to 'Add or Edit Monitored Agent' with fields for Agent Type (Host), Status (Enabled), Agent Name, and Agent Name Suffix, and an OK button.

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

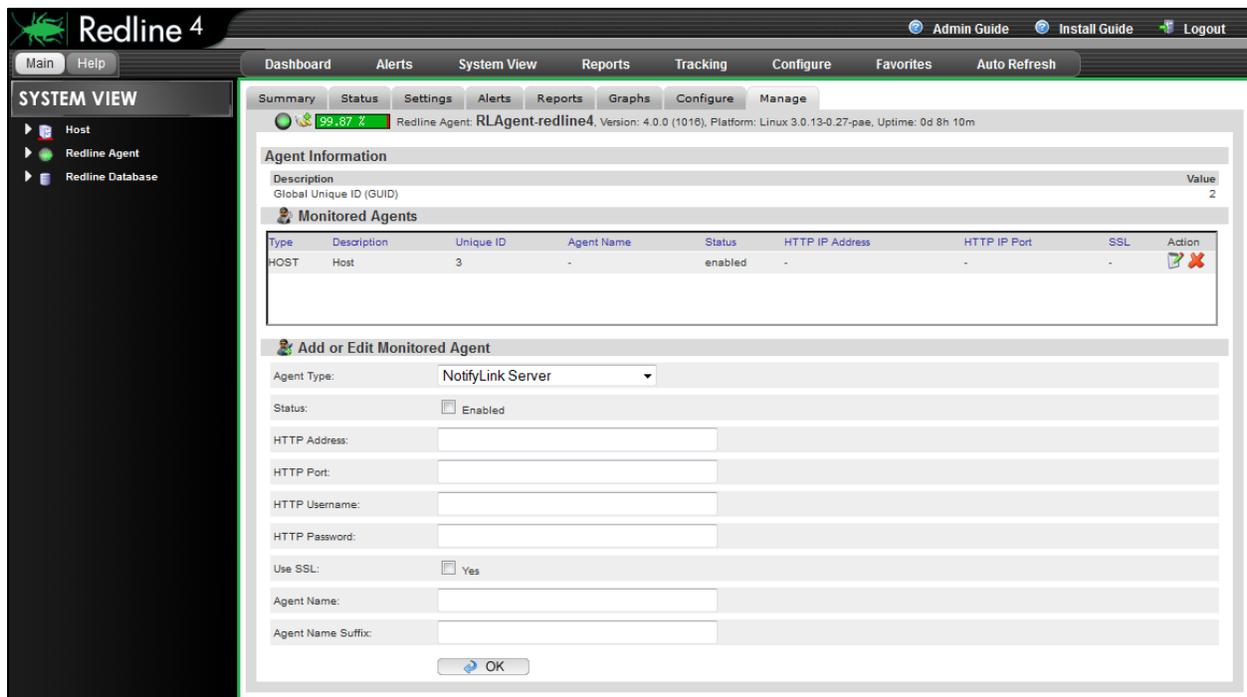
NotifyLink 4

NotifyLink 4 is supported in all NotifyLink builds from September 2005 onwards. The NotifyLink Enterprise Server for GroupWise requires three components to be installed - the SQL Database, the Web Server and the Messaging Server. The system and server requirements vary depending on the components being installed, and whether or not they are on a single or multiple servers. Obviously, the installation and configuration of NotifyLink systems are beyond the scope of this manual; however, in general, the components that must be installed with a NotifyLink Enterprise Server are:

- Messaging Engine
- Database
- Web Interface
- Device Client

Please consult the NotifyLink 4 documentation for further details.

From the Redline Control Center, go to the System View and pick the Redline Agent which will monitor the NotifyLink Agent. Specify IP address, port, username and password of your NotifyLink server.



The screenshot shows the Redline 4 control center interface. The top navigation bar includes 'Main', 'Help', 'Dashboard', 'Alerts', 'System View', 'Reports', 'Tracking', 'Configure', 'Favorites', and 'Auto Refresh'. The 'SYSTEM VIEW' sidebar on the left shows a tree structure with 'Host', 'Redline Agent', and 'Redline Database'. The main content area displays the configuration for a 'Redline Agent: RLAgent-redline4'. The 'Agent Information' section shows a 'Global Unique ID (GUID)' of 2. Below this is a table of 'Monitored Agents' with one entry: 'HOST' with a 'Unique ID' of 3 and 'Status' of 'enabled'. At the bottom, the 'Add or Edit Monitored Agent' form is visible, with 'Agent Type' set to 'NotifyLink Server' and 'Status' set to 'Enabled'. The form includes fields for 'HTTP Address', 'HTTP Port', 'HTTP Username', 'HTTP Password', 'Use SSL' (checked), 'Agent Name', and 'Agent Name Suffix'. An 'OK' button is at the bottom of the form.

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

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.

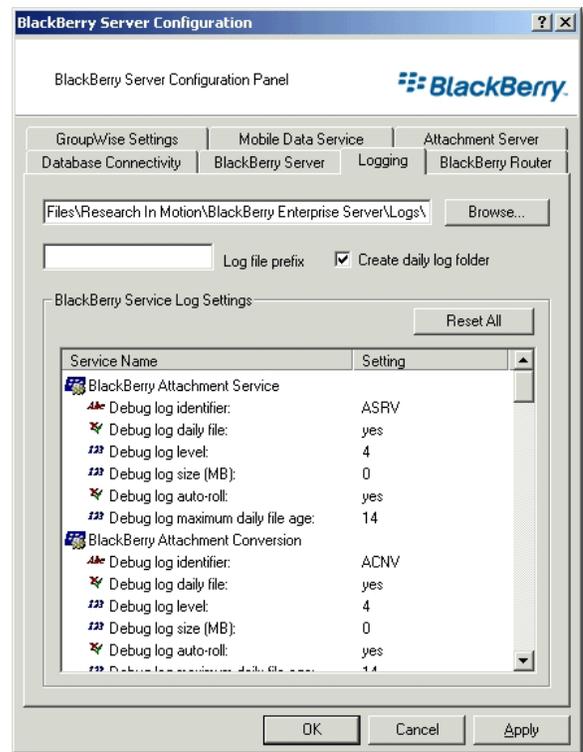
Configuring Blackberry Enterprise Server

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 Redline.

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

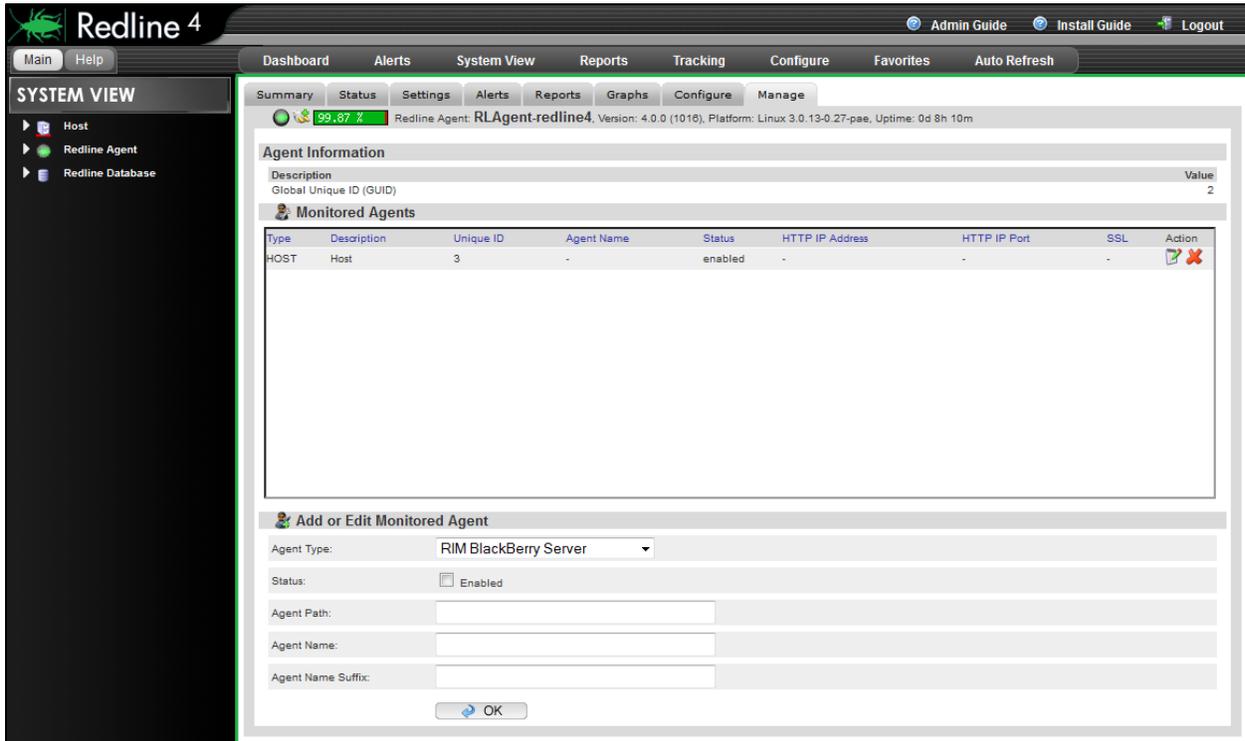
Scroll through the BlackBerry Service Log Settings and set the various services as follows:

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



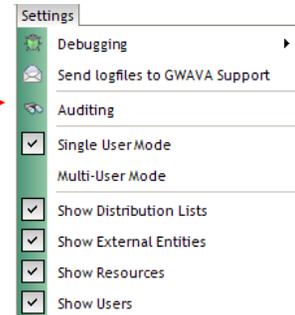
After 2-3 minutes, a message should appear on the Redline Agent that the Blackberry Enterprise server has been registered to the Control Center and shows up in the Control Center.

Vertigo

Redline monitoring in Vertigo is accomplished without any Redline agent. Vertigo reports and connects directly to Redline. All configuration required for Vertigo monitoring is contained inside Vertigo.

To configure Vertigo to connect to Redline:

- Start Vertigo 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 Redline for Auditing. If unavailable, auto fall-back to text auditing.
 2. Use Redline for Auditing. If unavailable, shutdown Vertigo.



- Enter the IP address or host name of the Redline 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 Redline. (The registration code and name is used by the Control Center to communicate with agents.)

Configure Auditing
GWAVA Vertigo can store an audit trail in in order to enforce existing business and legal polides.

Decide which auditing method to use

Use Redline for auditing. If unavailable, auto-fallback to textfile auditing.
 Use Redline for auditing. If unavailable, shutdown Vertigo.
 Use simple textfile auditing only. If unavailable, shutdown Vertigo
 No Auditing

Configure Redline auditing settings

Server DNS name or IP address: 10.1.9.25
Server port: 6900
Server timeout (ms): 300

Registration details:
Registration name: Company Name
Registration code: 12345

Configure textfile auditing settings

Auditing directory: C:\Program Files\GWAVA\Vertigo
Maximum logfile size (MB): 10
Minimum free disk space (MB): 1000

Ok Cancel

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 rlicenter.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, Vertigo will register and appear in Redline automatically.

Appendix

POSIX, UNC, and NetWare Paths

There are four common file path formats that Redline uses.

- UNC (Universal Naming Convention) is used commonly on Windows and occasionally on NetWare. An Example of UNC is [\\servername\volumename\path](#)
- Mapped Drive format is used exclusively on Windows. An example is `driveletter:\path1\path2`
- NetWare path format is used exclusively on NetWare. An Example is `volumename:\path1\path2`, or `server/volume:\path1\path2`
- POSIX is used on Linux, but also is used on NetWare by Redline. A POSIX example is `/path1/path2`

Although Redline gathers the majority of its information via HTTP (and thus is file system independent), there are several circumstances when file paths must be specified (and hence the specific format used is important):

- The RLAGENT and RLCENTER configuration files specify directory paths for internal Redline directories such as the Database or Reports locations.
- The RLAGENT file may contain PATH specifications for integrated components such as BES, Guinevere, and the API Gateway that do not have HTTP servers.
- Behind the scenes, Redline gathers log file information from many agents. These log files must be located in an accessible location.

On Linux and Windows systems, the rules are fairly straightforward:

- For Linux boxes, all paths must be POSIX format. UNC, mapped drive, or NetWare paths will not function. When first installed, all your paths will be in POSIX, and you must keep them that way.
- For Windows, you may use either mapped drive or UNC format. POSIX, NetWare paths will not function correctly. When first installed, all your paths will be in mapped drive format, and you may alter them between mapped drive and UNC as desired.

On NetWare the situation is a bit more complicated. As long as Redline is installed in its default location, and all of the component agents are on the SYS volume, all should work perfectly. Otherwise:

- Regarding issue 1, if you actually need to change these paths (and in normal operation, even when moving Redline to another volume, this is not needed), POSIX format is required. See below for the POSIX and NetWare path discussion
- Regarding issue 2: POSIX, NetWare, and UNC paths are all accepted in the PATH section. Hence, it is recommended that you use NetWare or UNC paths, and avoid the POSIX path issues described below
- Regarding issue 3: Redline will automatically deal with NetWare Log File paths read from the HTTP server and convert them to POSIX format internally, creating mount points as needed (under `sys:\mnt\posix\volumename`). So, no extra configuration is normally needed. If you really want to understand more about mount points, read on.

NetWare and POSIX Path Conversion

Consider a standard Netware server, named MJBSERVER, with 2 volumes, SYS and DATA1. Now let's take the example of GroupWise being installed on this server, first on the SYS volume and then the DATA1 volume. For simplicity, we'll assume the GroupWise agents are all installed under a directory right off the root of the volume named GRPWISE.

Start with the GRPWISE directory on SYS, the Netware path is volume:\path, so in this case it is the straightforward SYS:\GRPWISE. POSIX format is /path1/path2. In this case it is simply /grpwise. The only change is to eliminate the volume name and changed to forward slashes.

Other examples of path conversions on SYS would be SYS:\system vs. /system, or SYS:\novell\webacc vs. /novell/webacc. It may be clear that an issue will arise shortly: namely that POSIX paths don't include volume names.

Let us move the GroupWise system to the volume DATA1

The NetWare path will still be straightforward. It will be DATA1:\grpwise. But what is the POSIX path? The way that Novell solved this problem was to allow users and programs to provide a "mapping" between POSIX paths and Netware volumes. More specifically, there is a file (which doesn't exist by default) in SYS:\ETC called PATHTAB which contains entries such as: POSIXPath<space>NetwarePath

You may specify as many as you wish, using any text editor you please. So the first thing an administrator might do is create an entry like this: /mygw<space>DATA:\

One might then expect that I could use /mygw/grpwise to refer in POSIX format to DATA1:\grpwise. Similarly if another directory was off the root of DATA1 called EXAMPLE. I could refer to in NetWare format as DATA1:\example and in POSIX as /mygw/example

There is one complication, that isn't so obvious: NetWare is really using a "mount point" to represent the NetWare volume. The "mount point" must always exist on SYS, and can be more or less arbitrarily named (but shouldn't collide with other directories on SYS)

This is a roundabout way of saying that whatever POSIX path specified in PATHTAB must have a corresponding directory structure on SYS. Let's take another step-by-step example.

- Create a POSIX path, and I have a directory named ANOTHEREXAMPLE off my GOOGLE volume. The NetWare path would be GOOGLE:\ANOTHEREXAMPLE

- Open `SYS:\etc\pathtab`, and add a mount point. Remember that I can name it how I want. In this case I'm going to decide that I want a POSIX path of `/mnt/myothervol/anotherexample` in the end.
- Add: `/mnt/myothervol<space>GOOGLE:\`
- I'll save `PATHTAB`, and then I will create off `SYS` the following: `SYS:\mnt`, `SYS:\mnt\othervol`. Their contents do not matter. A POSIX compliant program should now be able to use `/mnt/myothervol/example` and be redirected to `GOOGLE:\anotherexample`.

How is this relevant to Redline?

- If you must change the internal configuration paths of Redline, they must be valid POSIX paths, constructed as above. If you have integrations that use the `PATH` entry in `RLAGENT.CONF`, and for some reason WANT to use POSIX, you can, but you must follow these guidelines.
- Redline handles the issue of log files transparently. All it does is create mount points named `sys:\mnt\posix\volume name` and create a `PATHTAB` entry for you. This is done behind the scenes, so normally you don't need to worry about it.

Installation Worksheet

Print this sheet. Fill out the fields for each GroupWise agent that must be monitored

Sheet Number

ServerName _____
NOS Agent Type _____
HTTPAddress _____
HTTPPort _____
HTTPUserName _____
HTTPPassword _____
Logging _____
Message Logging _____
GWCHECK _____

ServerName _____
NOS Agent Type _____
HTTPAddress _____
HTTPPort _____
HTTPUserName _____
HTTPPassword _____
Logging _____
Message Logging _____
GWCHECK _____

Server Name - File Server Name
HTTPAddress - IP Address
HTTPPassword - Password for agent's HTTP server
GWCHECK - Yes or No, valid only for POA

NOS - Windows, Linux, Netware
HTTPPort - TCP Port of agent's HTTP server
Logging - Turned Logging on, set to Verbose. Enter Yes or No
Agent Type - MTA, POA, GWIA, WebAccess, Messenger, Messenger Archive, API Gateway
HTTPUserName - Username for accessing agent's HTTP server
Message Logging - Yes or No, valid only for MTA
The RLAGENT configuration file needs this information for each component.