GWAVA

Administrator's Guide

GWAVA 6.5

November 2017

Table of Contents

Preface

About This Guide

This Micro Focus GWAVA Administrator's Guide helps you integrate this software into your existing email system.

Audience

This manual is intended for IT administrators in their use of GWAVA or anyone wanting to learn more about GWAVA. It includes installation instructions and feature descriptions.

Technical Support

If you have a technical support question, please consult the Micro Focus Technical Support at http://support.gwava.com

Sales

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

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

Copyright Notice

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

Legal Notices

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

Major New Changes

GWAVA has changed a few core ways that scanners are implemented in the system. This was completed to facilitate multi-tenant systems, or systems containing more than one active domain, which require different settings.

To enact this new ability, several changes were necessary. The scanner is no longer associated with any interface, domain, or server. GWAVA uses 'policies' to manage to manage different scanning configurations. Policies enable more comprehensive control over scanning from a broad scope down to a granular, user by user, level. See the Policy Manager section for details.

GWAVA also includes a new image analyzer which can scan and flag offending images. As with other configurations, the image analyzer offers the same actions for mail in the GWAVA system: block, quarantine, notify, and flag. The image analyzer is an additional service to the GWAVA scanning system and requires an additional license. See a GWAVA sales representative for details.

GWAVA has changed the way it installs. GWAVA has a native installer supporting both 32-bit and 64-bit installations for Windows. For Linux, GWAVA is provided in an RPM which installs the system automatically with the appropriate version.

GWAVA's New Web interface.

GWAVA has included a new Web Interface which allows the GWAVA system to connect to an ICAP enabled proxy to filter web traffic. The Web Interface can filter, or block based on URL as well as specified keywords found on web pages. User access may also be restricted through user authentication.

Installation Guide

Minimum System Requirements

Supported Operating Systems: (with appropriate Java installed)
Linux

- Novell Open Enterprise Server 2.x (Linux)
- SUSE Linux Enterprise Server 10.x
- SUSE Linux Enterprise Server 11.x

Windows

- Windows 2003 Server
- Windows 2008 Server
- Microsoft Visual C++ (Required for Windows installer)

Hardware Recommendations:

Hardware recommendations are made according to approximate system load, and are dependent on OS and configuration type. General configuration settings are assumed. All RAM recommendations are for existing, unused ram, not total system RAM. (If connection dropping is used on an SMTP scanner, the expected performance rises significantly.)

3,000 Messages per hour

- Modern Multi-core 2.4 GHz Processor
- 1.5 GB Free RAM
- 40 GB Hard Drive space

10,000 Messages per hour

- Modern Xeon / Opteron Class 3 GHz Processor
- 4 GB Free RAM

100 GB Hard Drive space

Supported GroupWise Versions (For GroupWise integration)

- GroupWise 7.0 SP 3
- GroupWise 8.0 SP 2
- GroupWise 2012, 2014, 2014R2

Supported Databases

- Internal Database: SQLite
- External Supported Database: Postgres 9.1.3

Installation

Linux

GWAVA provides a native RPM installer for Linux. The rpm installer wraps together all pertinent information into a very painless installation experience.

Download the GWAVA-i586.rpm file to the desired server and run the installer either through the GUI with 'install software' or with the rpm command.

```
rpm –ivh gwava-<version number>.rpm
```

The installation will set GWAVA to run automatically, use no proxy, and update virus definitions within an hour after installation.

The GWAVA installer does not open any ports in the system firewall. To access GWAVA Management, port 49282 must be open.

The default commands for stopping and starting GWAVA on Linux are:

```
rcgwavaman start
rcgwavaman stop
```

GWAVA is installed, but must be activated.

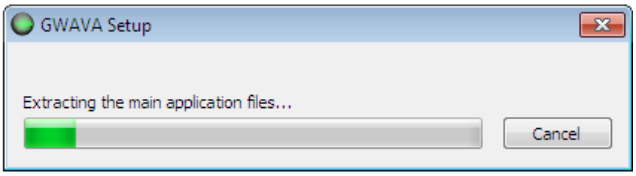
To continue, make sure that the GWAVA service is running and then open a browser and navigate to the setup and server activation:

```
http://<server_ip>:49282
```

Windows Installation

To install GWAVA on Windows, locate or download the installation file to the desired server and execute the installer.

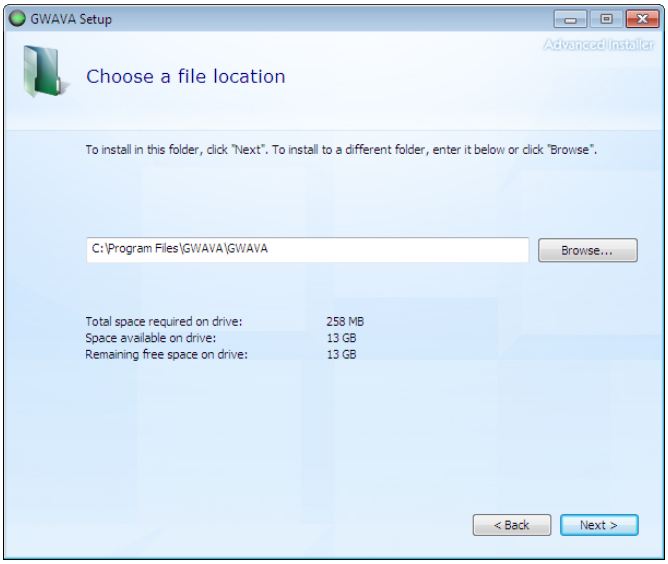
The installer will extract all files necessary and begin the installation wizard.



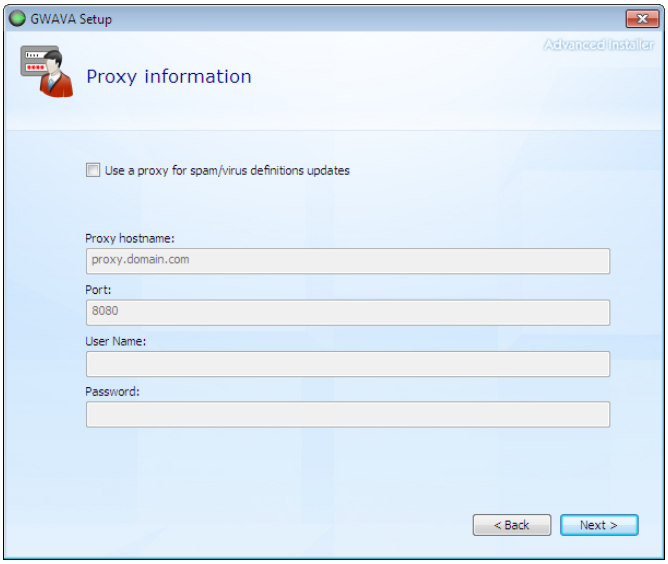
When the installer begins, click 'Next' to continue.

Agree to the license terms and select ‘next’ to continue.

GWAVA installs to the default location shown, if a different location is desired, specify the new location and select ‘Next’ to continue.

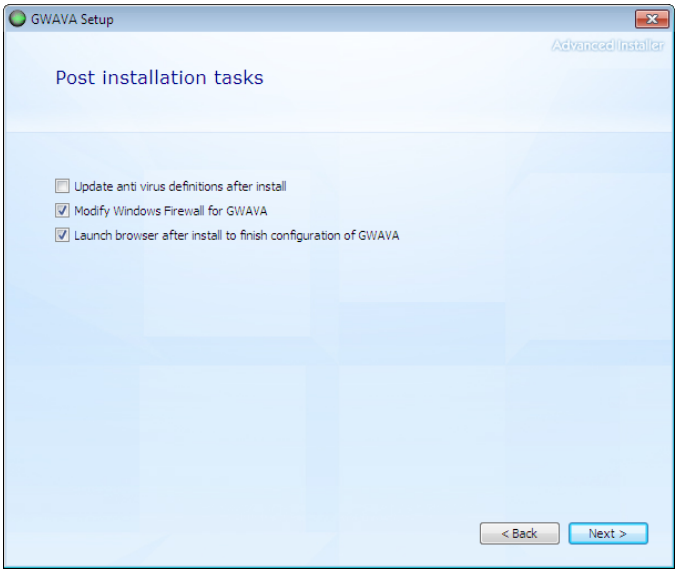


If a Proxy is utilized or desired to be used in the system, enable the proxy setting and input the relevant information.



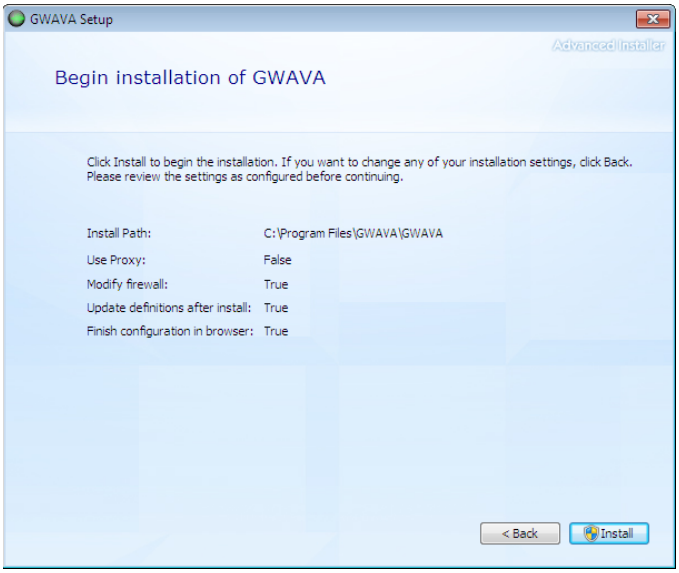
If your Proxy uses a username and password, the information must be provided for GWAVA to function correctly.

All post installation tasks options are offered. Select the appropriate desired tasks and click 'Next' to continue.

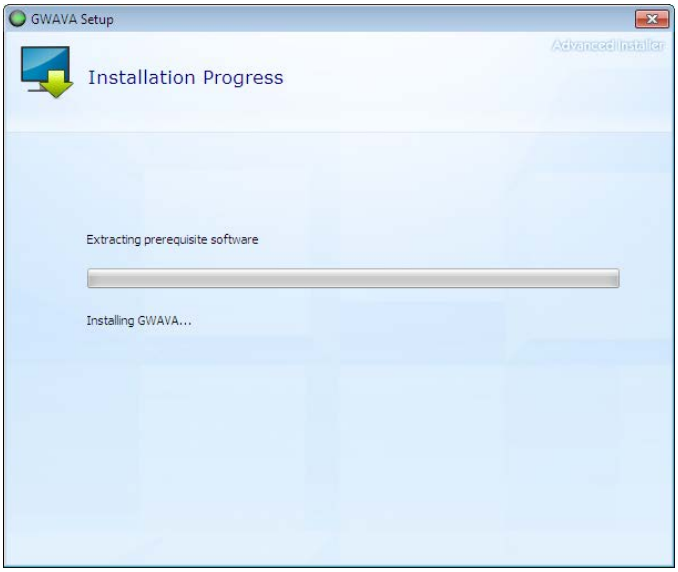


To access the GWAVA Management page, port 49282 must be opened in the firewall.

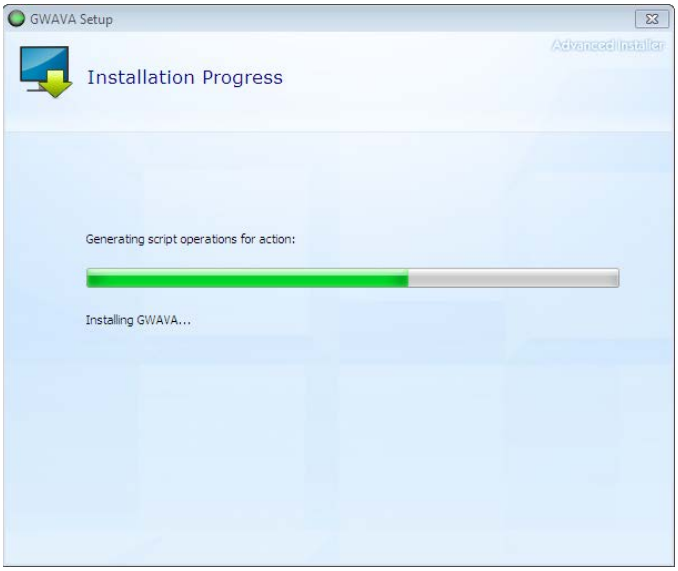
Once all the necessary information has been collected, they are displayed for review. If the settings are correct, select ‘Install’ to continue.



The GWAVA installer will check for Microsoft Visual C++ runtime, and if it is missing, the GWAVA installer will initiate the download and install for it.



After C++ is installed and the required prerequisite software is installed, the GWAVA installer will be resumed.



When the installer finishes installing GWAVA, click ‘close’ to exit the wizard.

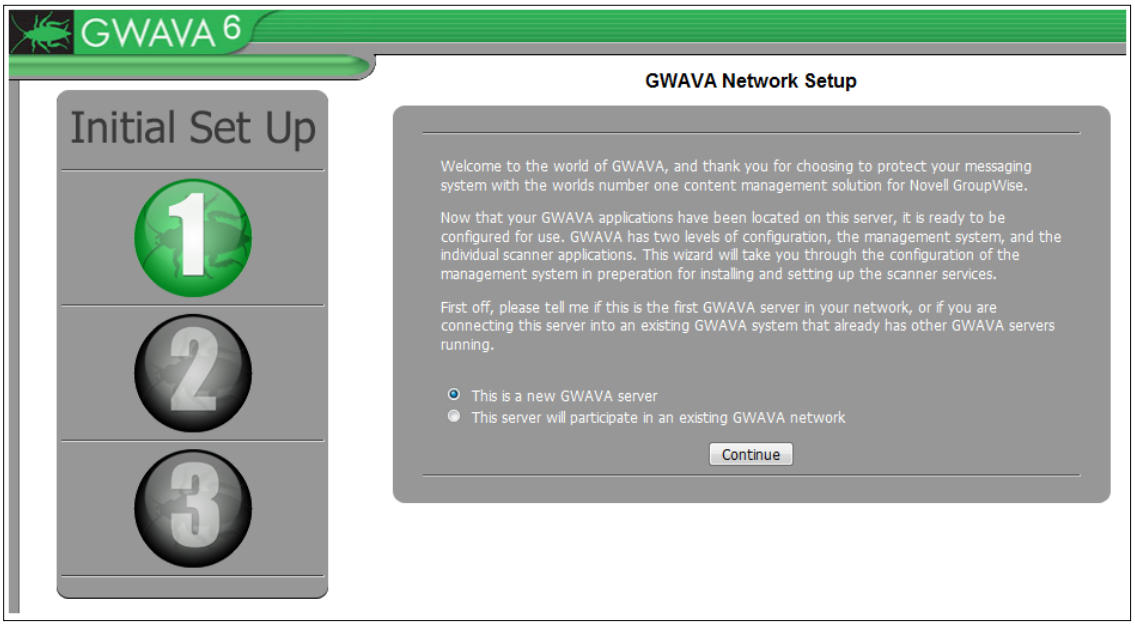
On Windows, by default the GWAVA server is run as a system service.

The GWAVA system is now installed, running, and is waiting for Server Activation.

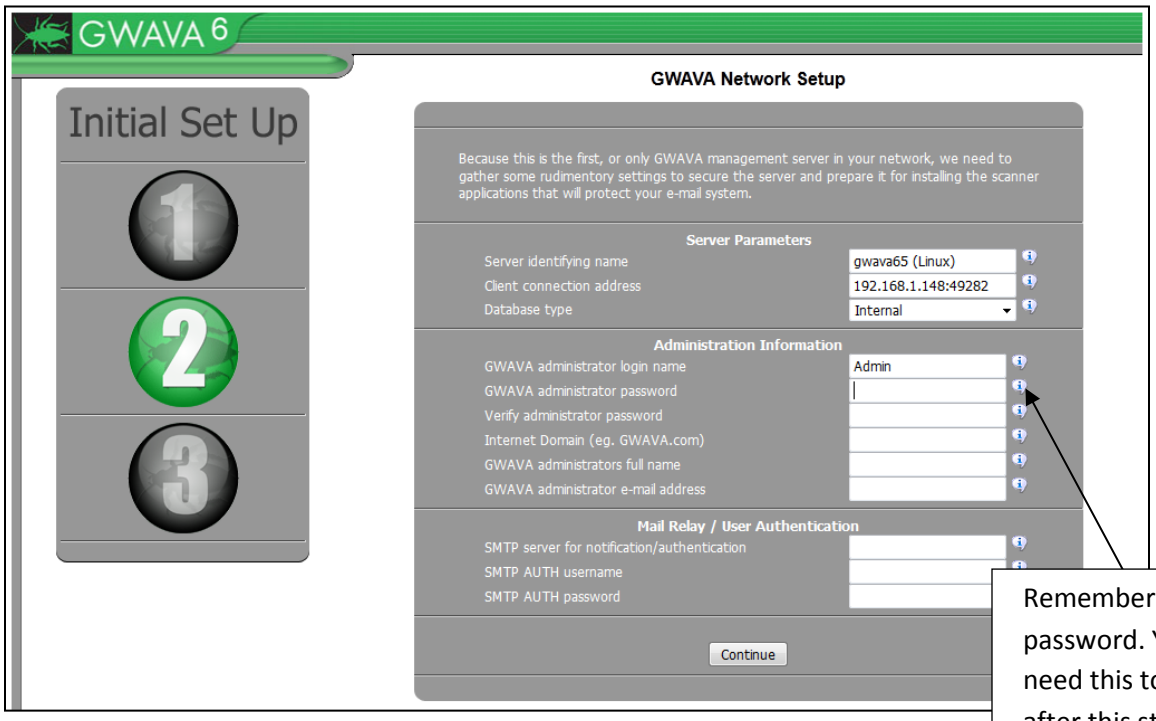
GWAVA Server Activation

From your workstation, enter the URL `http://<your_server _ip>:49282`. For example: `http://192.168.10.60:49282`, then click 'Go' or press ENTER.

Choose the default, '**this is a new GWAVA server'** and click '**Continue'**



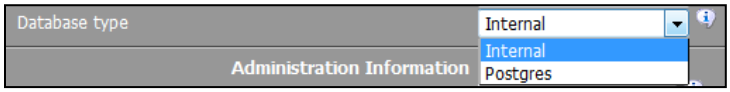
Enter the requested information for your environment.



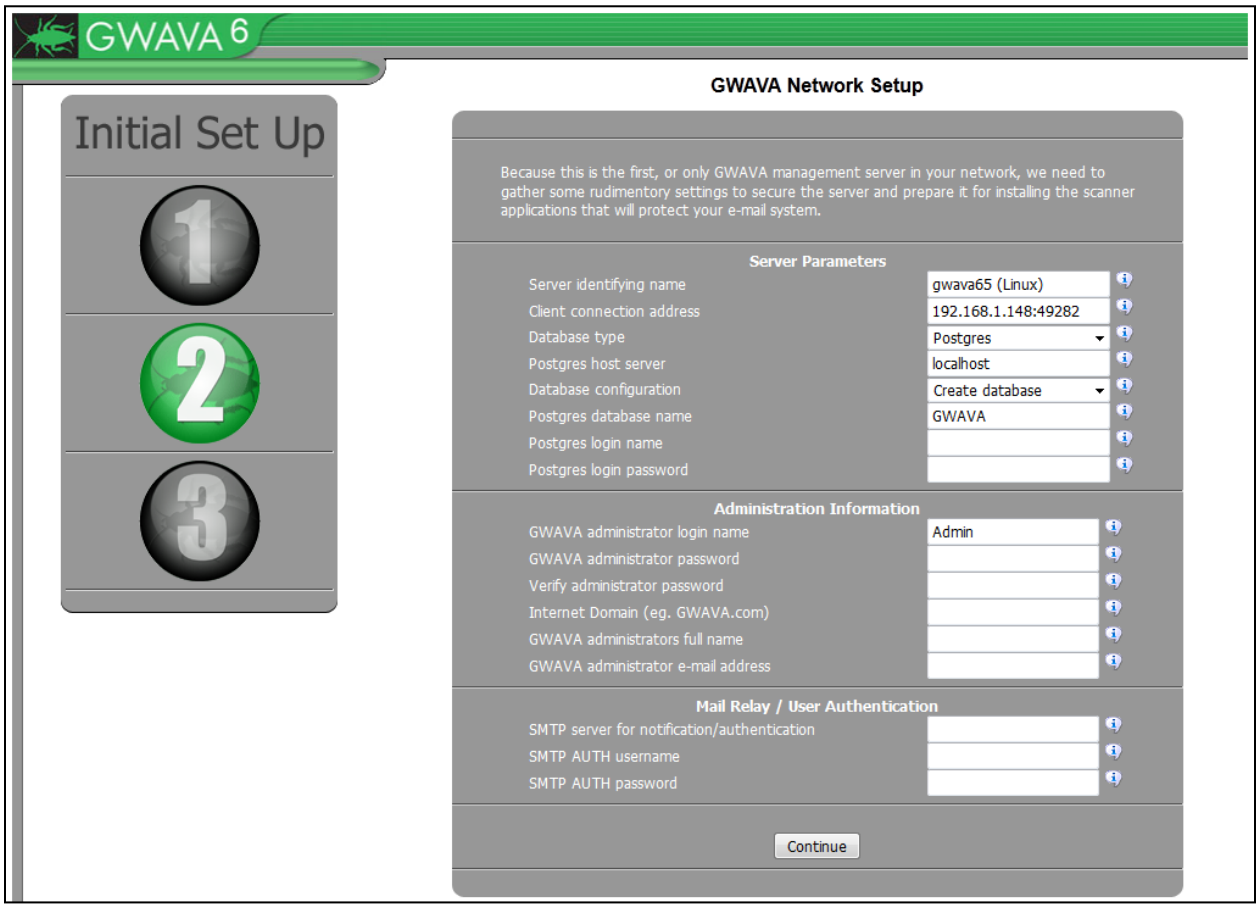
Remember this password. You will need this to login after this step is complete.

GWAVA comes with an internal database, SQLite, which is sufficient, and which requires no tuning or separate installation, and if the internal database is selected, no further database configuration is required.

However, for those who desire an external and more robust database engine, GWAVA also supports Postgres db. (Postgres 9.1.3)



Installation, setup, tuning, and maintenance of the Postgres database is the responsibility of the administrator.

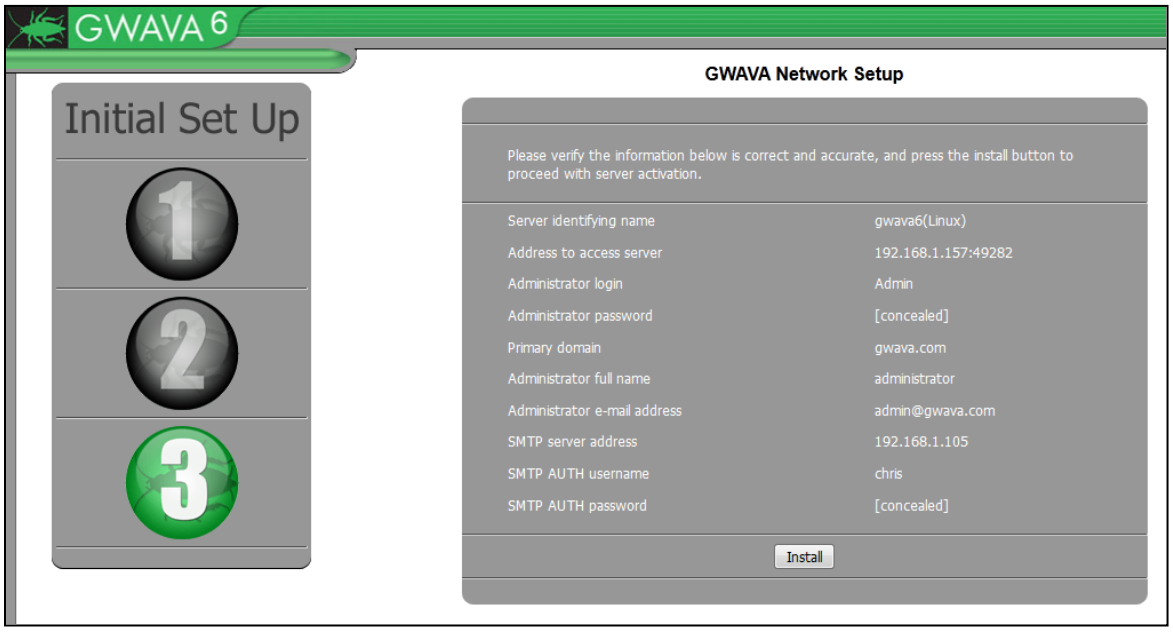


GWAVA requires the basic connection information for Postgres: IP address or DNS name and database name. The account login name and password for Postgres must be an account with database creation rights – or if connecting to an existing database, the username and password with full rights to that database.

Specify whether GWAVA will create the database automatically or whether GWAVA is to connect to an existing database. Because GWAVA can create a database with everything required, it is recommended to allow GWAVA to create the database.

When configuration has been completed, select ‘Continue’.

Confirm that the information is accurate and click ‘Install’.



After the server has been activated, the following screen should appear. You should see a login prompt to the web interface in the future.

Now that the server is activated, we can proceed with creating the desired scanners and scanner configuration. See the Administration guide for all configuration and scanner creation instructions.

To connect to the GWAVA Management Console in the future, open any browser that has access to the server and type the URL `http://<server_ip>:49282`

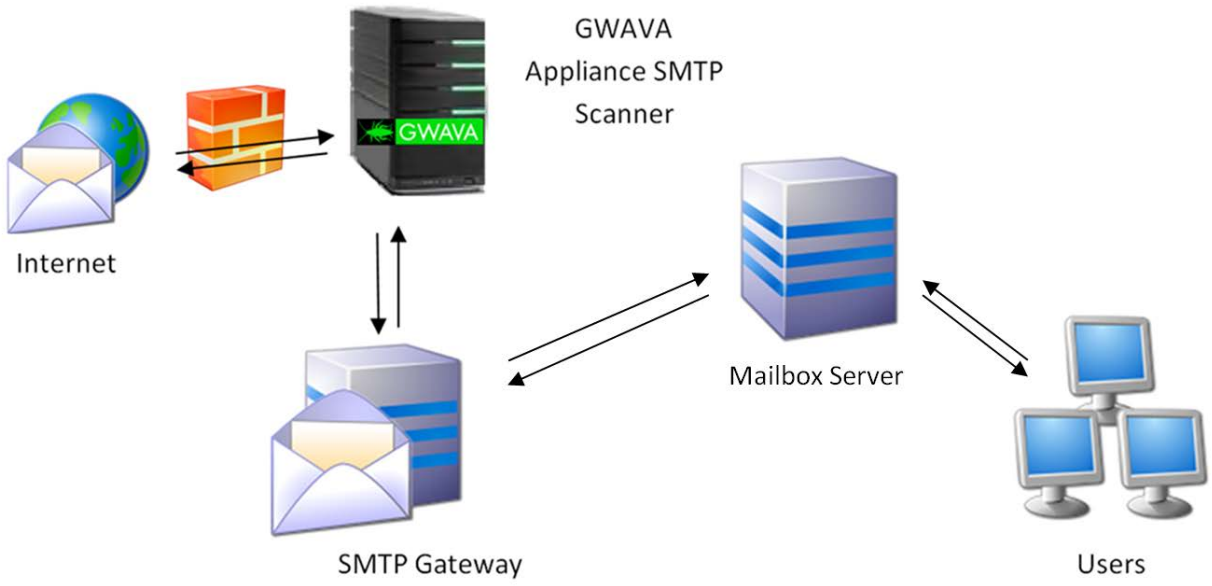
Log into your GWAVA Management Console to begin server configuration.

Appliance Installation Guide

Overview

The GWAVA Appliance is a complete software package for implementing the GWAVA system and is designed to replace an existing GWAVA server with a standalone GWAVA system running an SMTP scanner for any mail system. The GWAVA Appliance is ideal for a virtual machine environment.

The GWAVA Appliance is designed to run the SMTP scanner for any email system in the market. The SMTP scanner, and GWAVA Appliance, are completely independent of, and can be implemented in any system. The SMTP scanner acts as a proxy for the SMTP Gateway of your mail system.



The SMTP scanner and GWAVA appliance are meant to be placed in front of the current Gateway for the mail system. Incoming email sent to your domain will first go to the GWAVA appliance, which scans then sends clean email to the Gateway. Mail sent from your domain will pass through the normal system, but the SMTP Gateway will send the mail to the GWAVA appliance, which sends the email to the internet.

Ports

If the GWAVA appliance is set behind a firewall, or multiple firewalls, the following ports should be open for mail flow and GWAVA functions or services:

Inbound and general traffic

- 53 – UDP (DNS lookups)
- 25 – TCP Inbound (Used for Mail)

The following are optional but should be open to allow access the GWAVA appliance from outside the network:

- 49285 – TCP Inbound (QMS message release service)
- 49282 – TCP Inbound (GWAVA Management Console)
- 22 – TCP (SSH access. This can be a security concern, but may be necessary to enable for support access.)

Outbound traffic

- 80 – TCP Outbound (Updates services for Antivirus, Signature Engine, and GWAVA system.)
- 21 – FTP Outbound (OS updates)
- 25 – TCP Outbound (Only if scanning outbound mail)
- 123 – TCP Outbound (Network Time Protocol (NTP))

Minimum System Requirements

For a system which processes ~2,000 messages per hour:

- 2.4 GHz Pentium 4 or equivalent processor
- 1 GB RAM
- 36 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

For a system which processes ~4,000 Messages per hour:

- 3.2 GHz Pentium 4 or equivalent processor
- 1.5 GB RAM
- 40 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

For a system which processes ~8,000 messages per hour:

- 3.6 GHz Pentium 4 or equivalent processor
- 2 GB RAM
- 60 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

Installation

To install the GWAVA appliance, download the ISO and burn the image to a blank CD using your preferred CD burning program.

Insert the GWAVA Appliance CD into the CD or DVD drive of the target system and boot from the Appliance CD. On boot, you will be presented with the following menu.

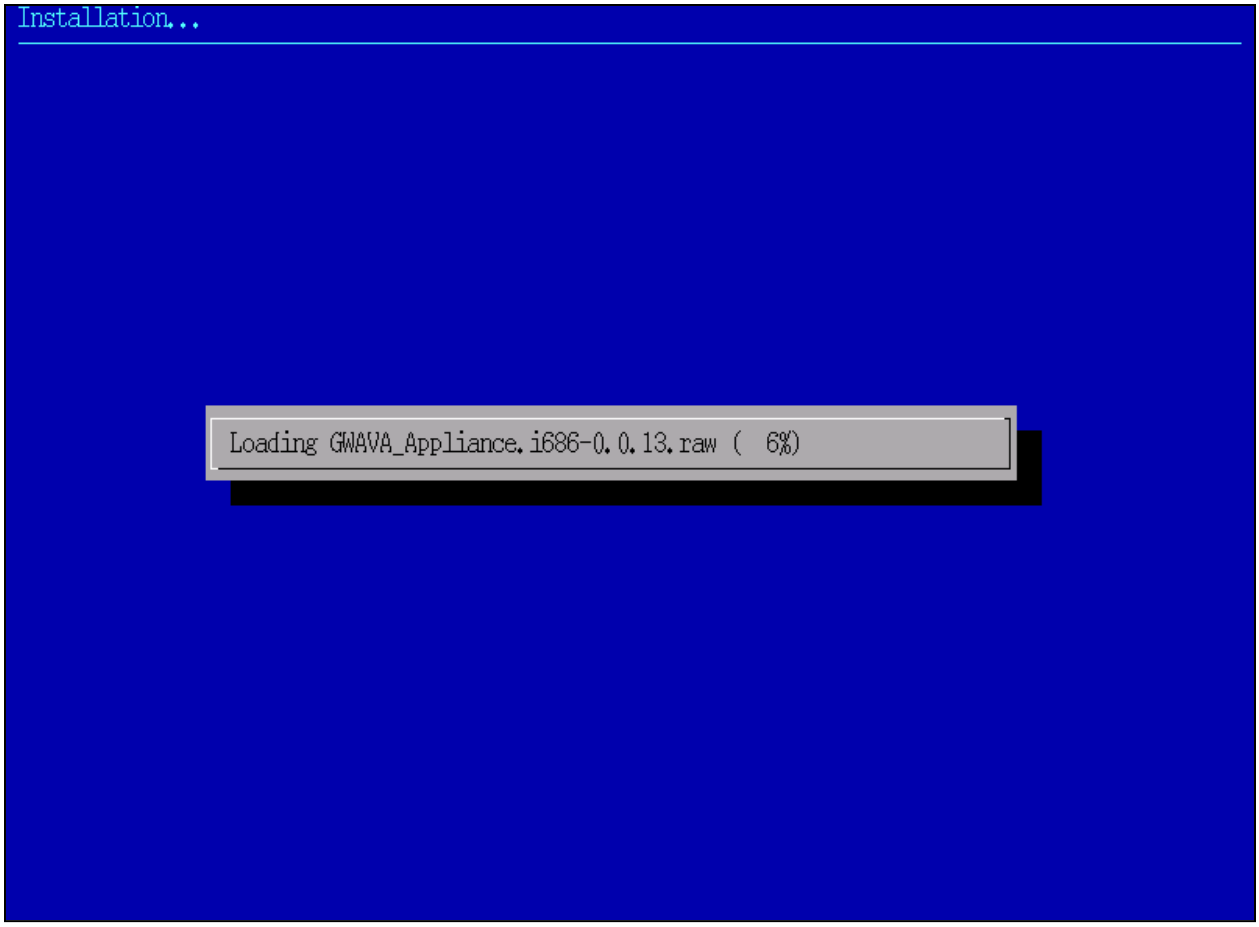
To install the Appliance, choose the install option.

Allow the system to completely boot from the Appliance CD, and the installation will automatically start.

You will be warned that running the installation will delete all data currently on the system. **This is the last chance you have to avoid formatting the drive in this system.**

If you have several hard disks in the system, GWAVA will ask which disk is the install destination.

As soon as you select 'Yes', the installation will begin.



The setup does not require any user input until after the system is initialized.

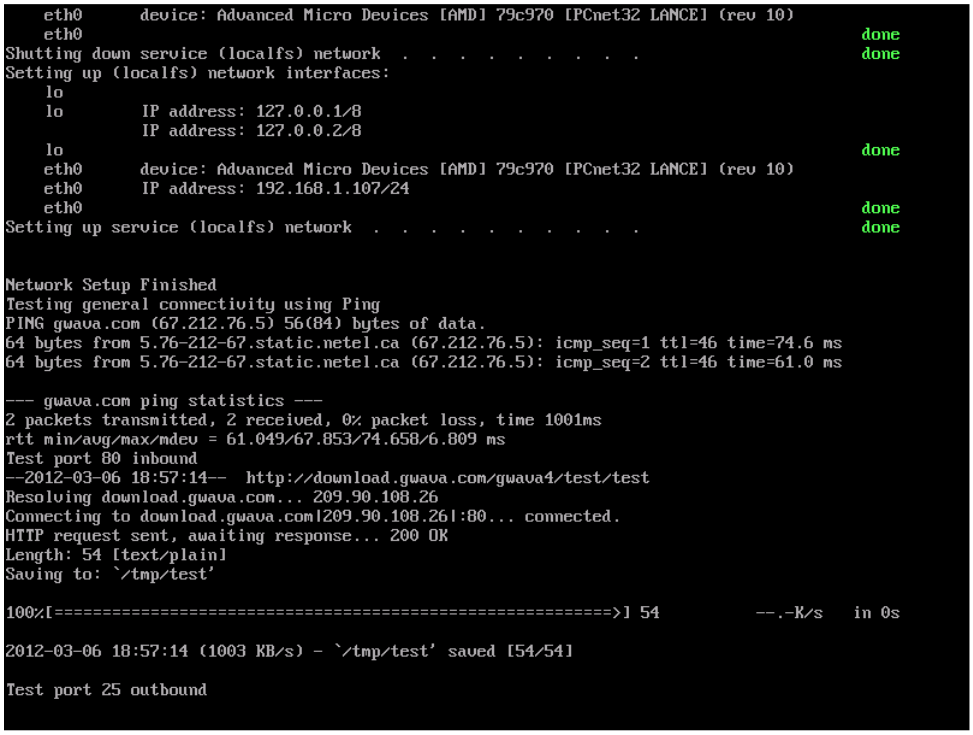
Once the installation has completed, you will be asked to provide connection and security information for your new system.

To complete the setup, all pertinent network information must be provided for your system. The defaults detected in parentheses will be set if you simply hit 'enter'. To change the setting, enter the appropriate value.

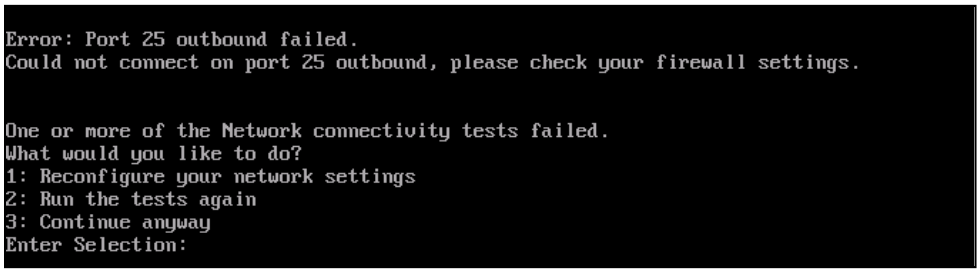
Ensure that you have the IP address configured correctly, this is the only interface to set or change the network settings.

After the settings have been entered, you are asked to verify that the following information is correct. Review the information and hit 'y' or 'n' and 'enter' to either re-enter the information or to continue.

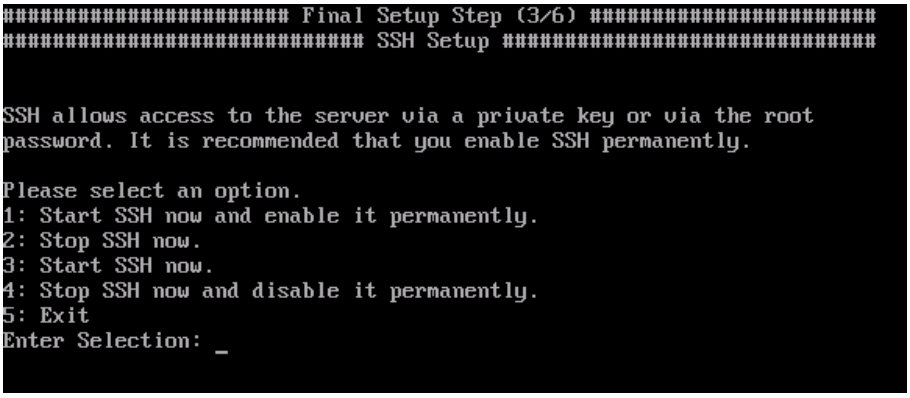
After you have set the network settings, they will be tested for connectivity.



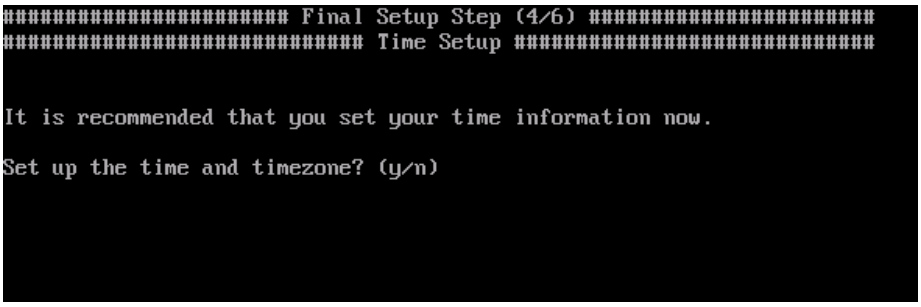
If there are problems, a chance to resolve the problem or move on will be offered.



SSH allows remote console administration on port 22. This can be turned on and off later through the GWAVA appliance control web interface. When you permanently enable or disable the service, it is removed from the runlevel and will be enabled or disabled on system startup until the setting is changed.



Next, is the time setup for the server. It is strongly recommended to setup the time on your system.



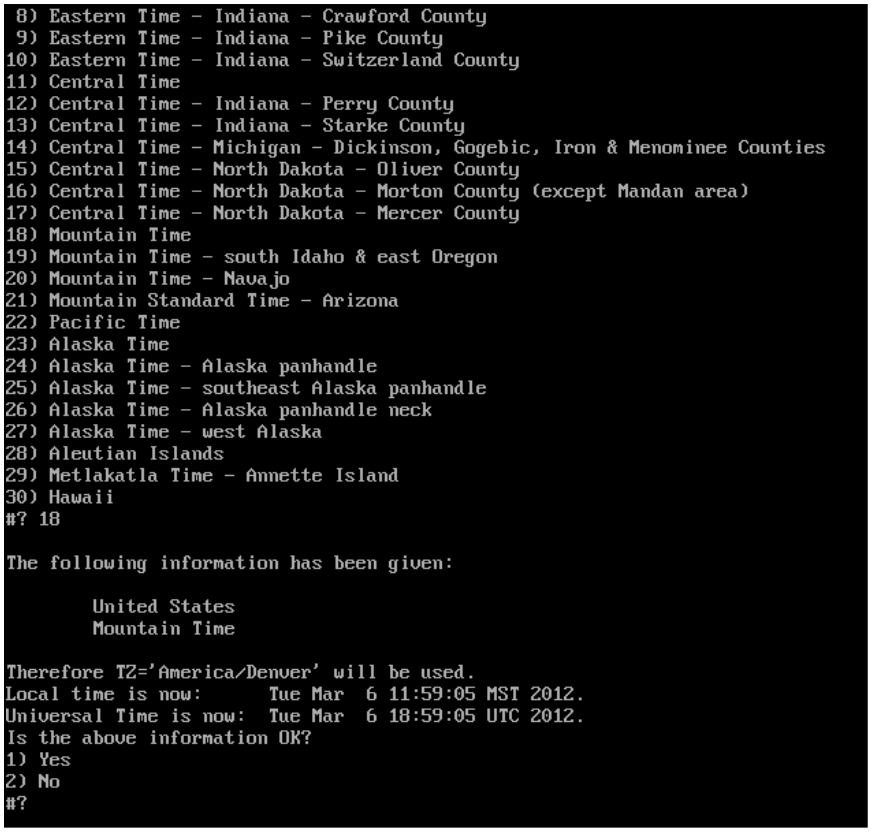
Pick your location. The wizard will narrow the terms to display a manageable list of time zones for you to select from.

```
######################### Final Setup Step (4/6) ##########################
################################ Time Setup ################################


It is recommended that you set your time information now.

Set up the time and timezone? (y/n)y
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 2
```

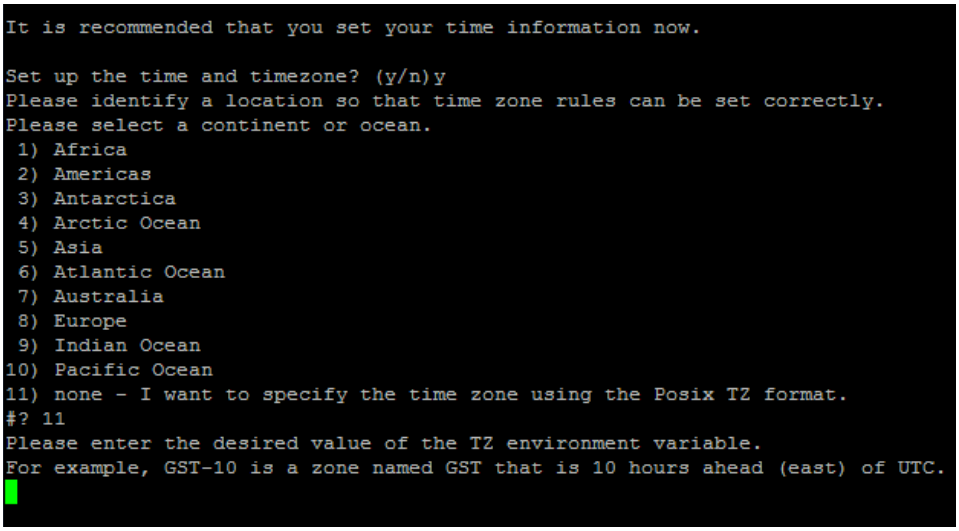
Select your resident country.

```
Please select a country.
 1) Anguilla                    28) Haiti
 2) Antigua & Barbuda           29) Honduras
 3) Argentina                   30) Jamaica
 4) Aruba                       31) Martinique
 5) Bahamas                     32) Mexico
 6) Barbados                    33) Montserrat
 7) Belize                      34) Nicaragua
 8) Bolivia                     35) Panama
 9) Bonaire Sint Eustatius & Saba  36) Paraguay
10) Brazil                      37) Peru
11) Canada                      38) Puerto Rico
12) Cayman Islands              39) Sint Maarten
13) Chile                       40) St Barthelemy
14) Colombia                    41) St Kitts & Nevis
15) Costa Rica                  42) St Lucia
16) Cuba                        43) St Martin (French part)
17) Curacao                     44) St Pierre & Miquelon
18) Dominica                    45) St Vincent
19) Dominican Republic          46) Suriname
20) Ecuador                     47) Trinidad & Tobago
21) El Salvador                 48) Turks & Caicos Is
22) French Guiana               49) United States
23) Greenland                   50) Uruguay
24) Grenada                     51) Venezuela
25) Guadeloupe                  52) Virgin Islands (UK)
26) Guatemala                   53) Virgin Islands (US)
27) Guyana
```

Select the appropriate time zone and confirm the selection or decline it to return to the beginning of the time zone wizard.



If you opt to specify a custom time zone, or do not find your time zone listed, you may choose the custom option: 'none'.



The time zone must be specified in Time Zone Environment Variable. Syntax: `<time zone name> <hours ahead of UTC>`. The time zone may be any name you like, as long as it conforms to Posix Time Zone format. The time zone name does not matter, but the hour variable sets the time for the system.

For example, for the Mountain Standard Time zone, U.S. and Canada use: `MST-6`

```
Please enter the desired value of the TZ environment variable.
For example, GST-10 is a zone named GST that is 10 hours ahead (east) of UTC.
GST-6
awk: cmd. line:4: warning: escape sequence `\.' treated as plain `.'

The following information has been given:

        TZ='GST-6'

Therefore TZ='GST-6' will be used.
Local time is now:      Wed Jul  1 23:50:39 GST 2009.
Universal Time is now:  Wed Jul  1 17:50:39 UTC 2009.
Is the above information OK?
1) Yes
2) No
#?
```

After your custom time zone has been created, the information must be verified.

```
Setting the time using NTP

Specify custom time server? (y/n)y
Time server (example: time.nist.gov):
```

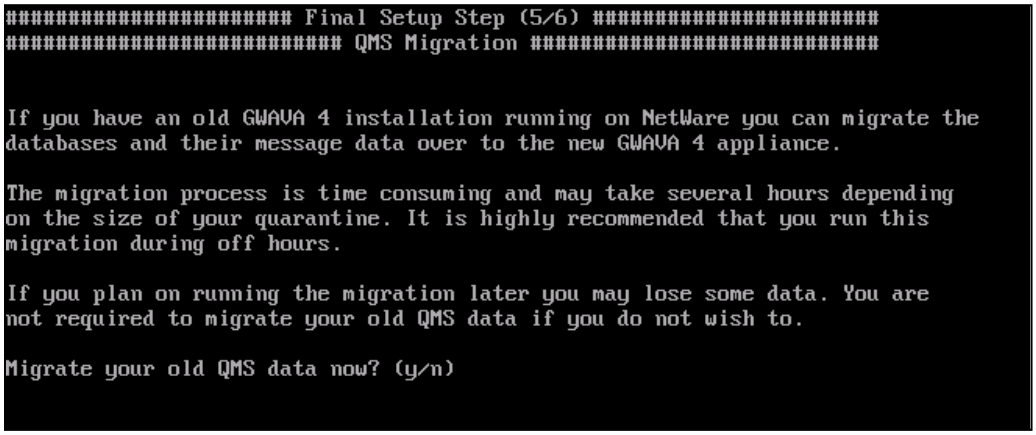
A custom Network Time server may also be specified. If a custom time server is used, provide the DNS name or IP address of the NTP server. Default, (time.nist.gov), is shown.

```
Setting the time using NTP

Specify custom time server? (y/n)y
Time server (example: time.nist.gov): time.nist.gov
Server: time.nist.gov
 1 Jul 17:51:34 ntpdate[3525]: adjust time server 192.43.244.18 offset 0.080447
sec

Time is now set to Wed Jul  1 17:51:34 UTC 2009
Try to get initial date and time via NTP from  time.nist.gov          done
Starting network time protocol daemon (NTPD)cp: cannot stat `/etc/localtime': No
 such file or directory
                                                                      done

Time and timezone setup complete
gwava-iso:/opt/beginfinite/gwava/scripts #
```

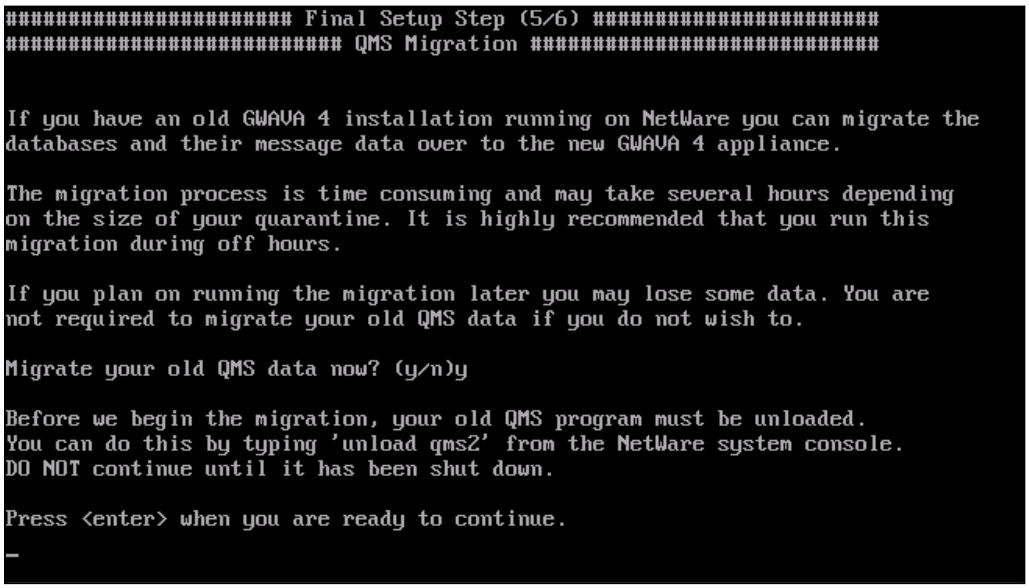
After the time server is specified, the system attempts to connect and sync the time.

Confirm the time settings for your system to continue.

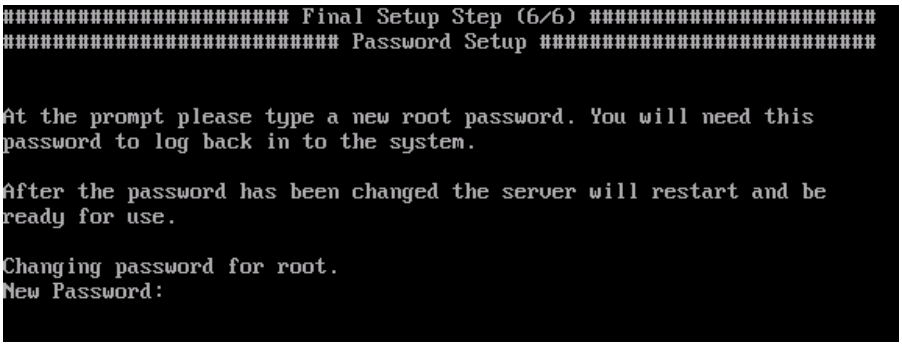
If you want to migrate an existing NetWare GWAVA Quarantine to the GWAVA Appliance, select 'yes' here. The wizard uses NCPMount to pull the information over the network connection from the existing QMS to the Appliance.



NOTE: You will be required to shut down the QMS system on the NetWare machine to complete the operation. This process can take several hours and should only be performed after-hours. If you wish to migrate QMS, this is the time to do so. Though you may invoke the command later, you will have data loss unless the migration is completed during setup.



For the final step, you are asked to set the root password for the system. This is the administrator password which will be required to log in to the system via ssh or through the console. DO NOT LOSE THIS PASSWORD.



The Appliance is designed to provide all the necessary functions for GWAVA inside the GWAVA web administration, thereby removing all need for console level administration. While normal operation of the GWAVA Appliance removes all need for console level administration, the root password may be required for support.

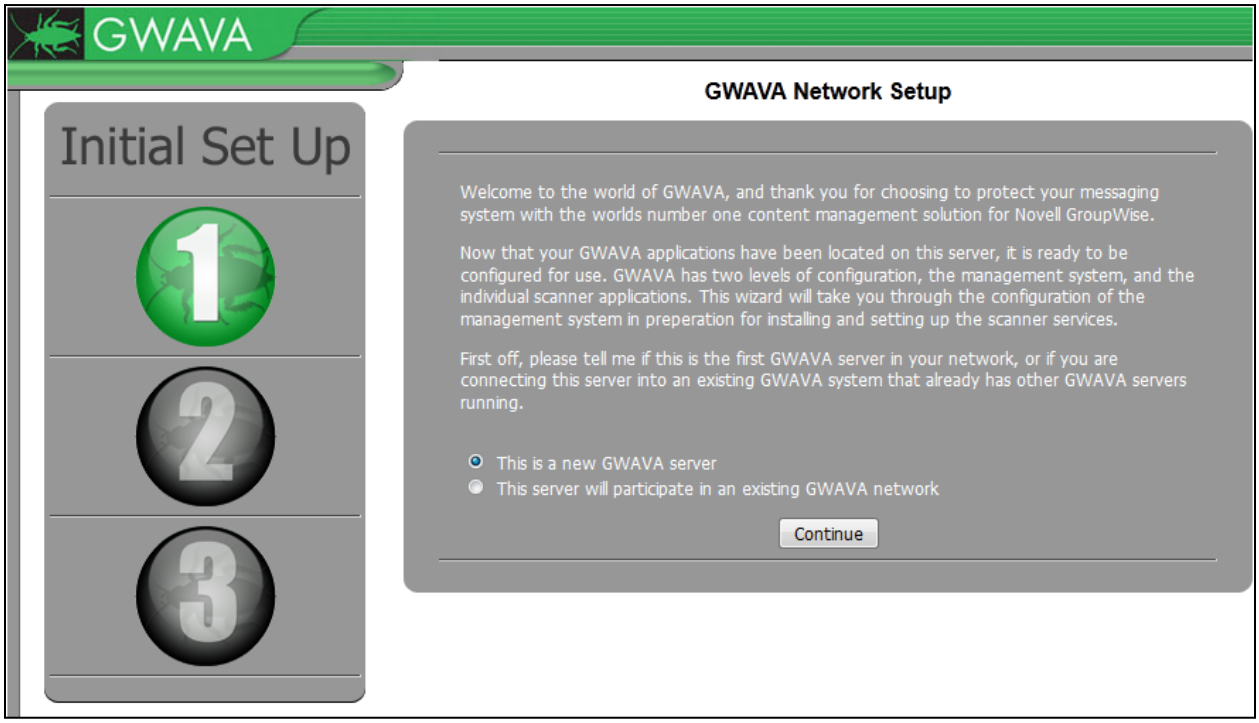
GWAVA appliance setup is now complete. All that remains is activating the GWAVA server and creating a scanner of your choice. (If this server was installed to a virtual machine, install all tools and aids.)

Server Activation

To activate your server, open a browser and enter the IP address or DNS name of the Appliance, with port 49282.

`http://<your_server_ip>:49282`

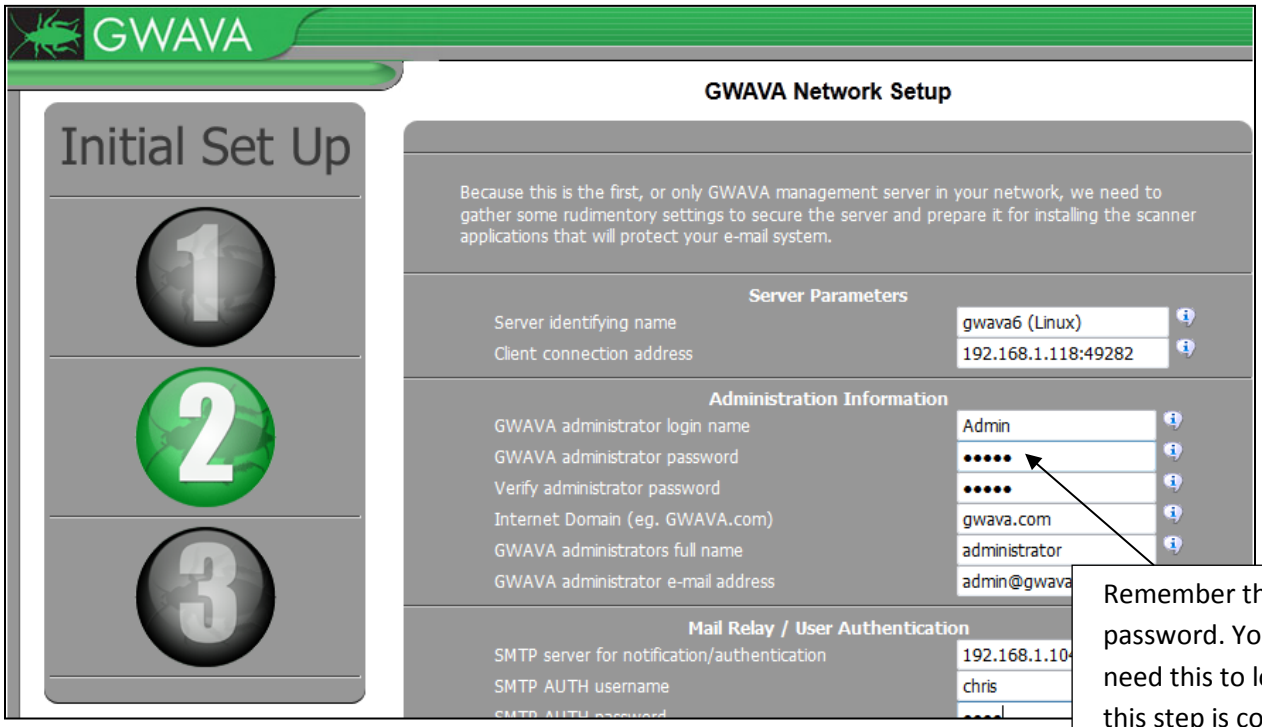
This is the connection address for the GWAVA management console. When you first connect to the system, you should be taken to the setup page, shown below.



The GWAVA Appliance is designed to replace existing GWAVA servers, and as such it is recommended to setup the Appliance as a new GWAVA server.

Select '**Continue**'.

The following information is required.



The server name should match the host name you set for the server. The connection address is the address that GWAVA will use to serve the management console. Both the Server parameters should be left as default.

The Administrator login name and password are required to connect to, and administer the GWAVA management console. **DO NOT LOSE THIS PASSWORD!**

The Internet domain is the domain that the GWAVA server will filter mail for. This should be your company domain. (For example, GWAVA.com)

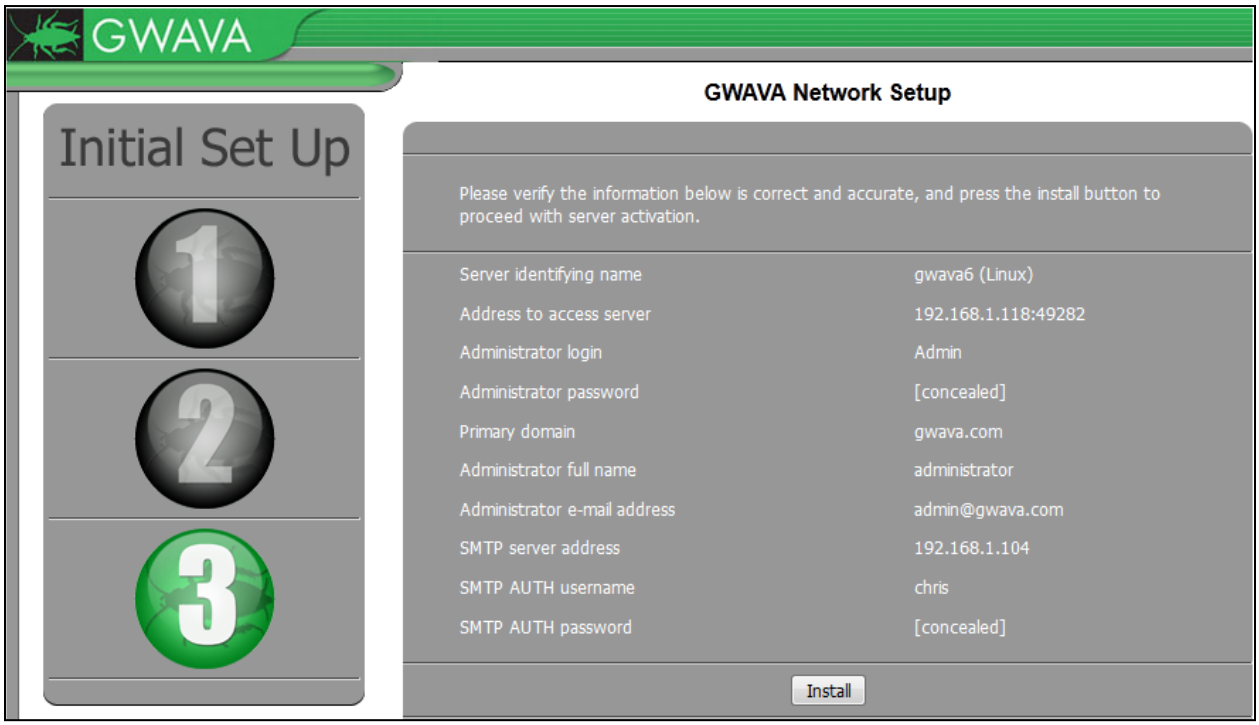
The administrator name and email address are the name and address which will appear on GWAVA notifications and digests. Any responses to these messages will be sent to the Administrator's e-mail address.

The SMTP server address should be the address of your SMTP gateway. If you are using an SMTP scanner, this will be the address which GWAVA will forward the incoming mail to. GWAVA also uses this address for QMS authentication and access.

The SMTP authorization name and password are not required for notifications, but are recommended. For GroupWise systems, this can be any username and password, and does not have to be an administrator. (For example, Username: bob, Password: c751h)

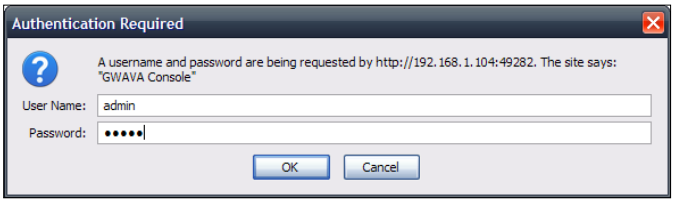
After you have provided the information, select '**Continue**'.

You will be asked for confirmation. Clicking '**Install**' will activate the GWAVA server, and you will be required to login using the admin name and password you provided earlier. Click '**back**' on your browser if you need to make any changes.



When you click '**Install**', wait for the activation process to complete. You should be redirected to the management login screen after the install completes.

Click on '**Enter Management Console'** and provide the administrator username and password to login.



Please see the main guide for scanner creation and system configuration.

How GWAVA works

GWAVA is an anti-malware and content management solution which provides complete protection for your mail system through a real-time interface. The Signature scanning engine in GWAVA allows for instant protection and regular spam definition updates with virtually no false-positives. The Signature scanner recognizes spam due to a managed definition base which can also recognize most viruses before the mail reaches the virus scanner, adding an extra layer of protection.

GWAVA can fit its scanner to any mail system through a SMTP interface to protect the mail system from attack and wasted bandwidth. In addition, GWAVA is able to implement its scanner in the following GroupWise agent interfaces:

- GWIA interface
- MTA interface
- POA interface
- WASP (WebAccess) interface
- Vibe interface

How the different Interfaces work

The different scanning interfaces offered by GWAVA all utilize the same scanning engine in the base of the GWAVA system, but each interface is configured separately to integrate to the different components they are named for. These different scanning interfaces are briefly explained below.

SMTP Interface

The SMTP interface allows incoming and, or, outgoing mail to be intercepted, scanned, and filtered completely independent of the mail system. This setup has the distinct advantage of relieving the mail system of unnecessary and unwanted traffic, leaving the mail system resources open to function with greater performance and security.

The SMTP interface adds a scanning layer between any mail system's SMTP agent and the internet. Outbound mail is forwarded through the GWAVA SMTP, (like a proxy), which can scan the mail and then send messages to the internet. Incoming mail is first received by the SMTP interface which then sends the filtered mail to the SMTP agent. This interface allows GWAVA to act independently of your mail system. If used behind a firewall, see the appendix on suggested open ports.

Web Interface

The Web interface is a scanner applied to the web traffic passing through an ICAP enabled proxy. When enabled and connected to an active ICAP proxy, the Web Interface can filter web traffic, scan pages for keywords and block offending pages, require user authentication and deny access to specified users, and block specific URLs. This interface adds a layer of control and limits or defines access to the internet through the network. Because this interface scans web pages instead of messages, many settings do not apply to this scanner, and configuring mail filters for this interface is not recommended. For instance,

utilizing anti-spam scanning on the web interface will slow down the system and effectively block everything. See the applicable sections for configuration settings.

GWIA Interface

The GroupWise Internet Agent interface, or GWIA interface, intercepts the mail flowing through the GWIA folder structure, scans the mail, then passes clean mail back to the GWIA for normal mail processes. The point of interception comes directly after the GWIA receives the mail from the internet source, or right before the connected GWIA sends the mail across the internet. The GWIA interface does not directly receive mail or send mail, and has no connection to the internet whatsoever. GWAVA's GWIA interface instructs the GWIA to place mail it has received into a holding folder structure, called the 3rd folder, where the mail waits to be scanned by GWAVA. Once the mail has been scanned and sorted, GWAVA places the clean message files into the proper folder, where the GWIA then moves the incoming mail to the MTA and the outgoing mail to the internet destination, as part of its normal process. Clean messages are passed through the system as normal, with no alterations to the file.

Because the GWIA interface is integrated in the base folder structure, and not in the actual processes of the GWIA agent itself, there is no start or stop order for GWAVA or the GWIA. If a GWIA interface has been created and installed correctly, then if GWAVA is not running while the GWIA is attempting normal operation, then mail received from the internet, and mail waiting to be sent to the internet, will queue up in the holding folders created for the interface. Once GWAVA is started, the queued mail will be processed and sent to the internet or the MTA as normal.

MTA Interface

The Message Transfer Agent interface integrates into the process of the actual GroupWise agent, adding the anti-malware scanner into the normal processes of the MTA. GWAVA utilizes the GWMTAVS virus scanning API provided by Novell. To utilize this API, GWAVA invokes the virus scanning switches in the MTA startup file, calling first GWMTAVS, which then loads the GWAVA MTA interface. Each file passing through the MTA is handed to the GWMTAVS and then the GWAVA MTA interface, which scans the message, reporting to the GroupWise MTA if the message should be blocked or is clean, and can be passed through to the rest of the system. Clean messages are passed through the system as normal, with no alterations to the file.

Because of the nature of the API and the loading process, there is an order to starting and stopping the GroupWise MTA and GWAVA with a MTA interface. Because it is called during start and not controlled by the MTA on shutdown, the GWAVA interface is the first started, and the last stopped in order to prevent the GroupWise MTA from failing to start or stop. The order to start a GroupWise MTA with an attached GWAVA MTA interface is, first to start GWAVA, and then start the MTA. To shut down the MTA and GWAVA, first stop the MTA, then shutdown GWAVA.

Due to environmental variables, the MTA interface will not function on Windows GroupWise systems.

POA Interface

The Post Office Agent interface is the only interface in the GWAVA suite which does not implement a real-time scanner. Because there is no API or process that allows the Post Office to be scanned in real time, GWAVA has created a scheduled interface which can periodically sweep the Post Office for malware and unwanted or unapproved messages and files.

Utilizing a trusted application key generated by the system administrator, the POA interface enters and scans each user's post office and messages individually. The POA interface can be set on a reoccurring schedule or set to run as a single use job, and has the ability to exclusively target or exclude specific user mailboxes as desired for security or policy. Clean messages and files are left completely unaltered. The POA interface requires the POA to be running in order to operate, but has no start or stop order associated with the operation.

Vibe Interface

GWAVA can implement a scanning interface into the Novel Vibe system to scan correspondence and work flow. All input text and transferred files can be scanned through the Tomcat servlet. Essentially, all text messaging, emails, threaded conversation, sent files, and attachments can be scanned by GWAVA.

Files and messages which are caught by the interface will be blocked, deleted, or quarantined according to the settings and configuration of the interface. Notification and released messages and mail will be sent through the email system, allowing the Vibe interface to be effortlessly moderated, protected, and controlled according to company policy.

WASP Interface

The GroupWise WebAccess interface integrates into the WebAccess system by hooking into the WebAccess servlet, working between the message composition interface of WebAccess and the WebAccess agent. This allows WASP2 to scan all messages for viruses and any defined content before they are sent to the GroupWise server. If a problem is found, the message will not be sent, and the user is notified of the problem.

The WASP interface scans the message as soon as the user clicks 'send' in the WebAccess interface. In case of a problem, the notification that WASP sends to the user will inform them which part has the targeted problem, so they may correct the blocked item and send their message.

WASP scanning interfaces can be operated remotely to the Web Access server if desired, though there must be a quick and reliable network connection between the WebAccess machine and the machine running GWAVA.

Choosing an interface for your system

The most recommended scanning interface for any mail system is the SMTP interface, which has the highest performance and least intrusion while providing several services that are not available to the GWIA, MTA, and POA interfaces. However, the SMTP interface may not be the best fit for your system.

Determine what protection and service needs you have for your GroupWise system in order to determine which interface would fit best. The POA interface will only protect the Post Offices on a scheduled basis, and should never be relied on for full protection of your system. The MTA interface will provide protection between domains and different post offices as well as external mail, but the MTA interface also has a specific start and stop process, connects directly into the GroupWise Agent structure, and cannot provide the service which appends a specific signature to the end of each message sent.

The GWIA interface sorts all mail passing through the GWIA, which protects the GroupWise system from all external mail threats. The GWIA interface provides almost all options available, (except connection dropping), including the signature service, and does so without connecting directly into the GroupWise agent structure or requiring a start and stop procedure. If the client computers connected to the GroupWise system are equipped with virus protection software of their own, there is little advantage to choosing an agent interface other than the GWIA or SMTP interface.

The SMTP interface is designed to provide protection for any email system in the market. The simplest way to implement the SMTP interface is to use it in conjunction with the GWAVA Appliance, which completely separates the GWAVA system from any mail structure.

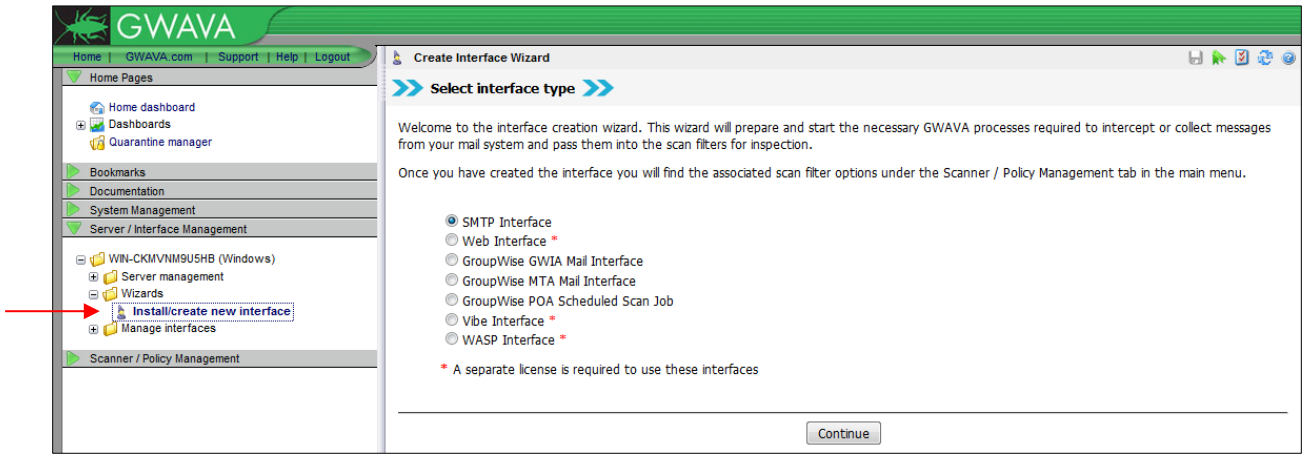
The SMTP interface acts as a proxy for the SMTP Gateway of your mail system.

The SMTP interface and GWAVA appliance are meant to be placed in front of the current GWIA or SMTP Gateways for the mail system. Incoming email sent to your domain will first go to the GWAVA appliance, which scans the messages and then sends clean email to the GWIA or SMTP Gateway. Mail sent from your domain can also pass through the SMTP interface and the GWAVA appliance, which sends the email to the internet.

Contact the sales representative for your area if you wish to implement the GWAVA Appliance and SMTP interface.

Creating an Interface

Installing an interface is the next step in creating a functioning GWAVA system, followed by domain configuration, (covered in the SMTP Interface wizard section), and licensing. If the GWAVA server is to be used in a trial period, the interface will be automatically placed into bypass mode as soon as the trial period is over unless a license has been applied.



The Interface creation wizards, (found under Server/Interface Management | Wizards | Install/create new interface), walk through the steps and information required to install the different interfaces for your system. Select the desired interface and follow the instructions to install.

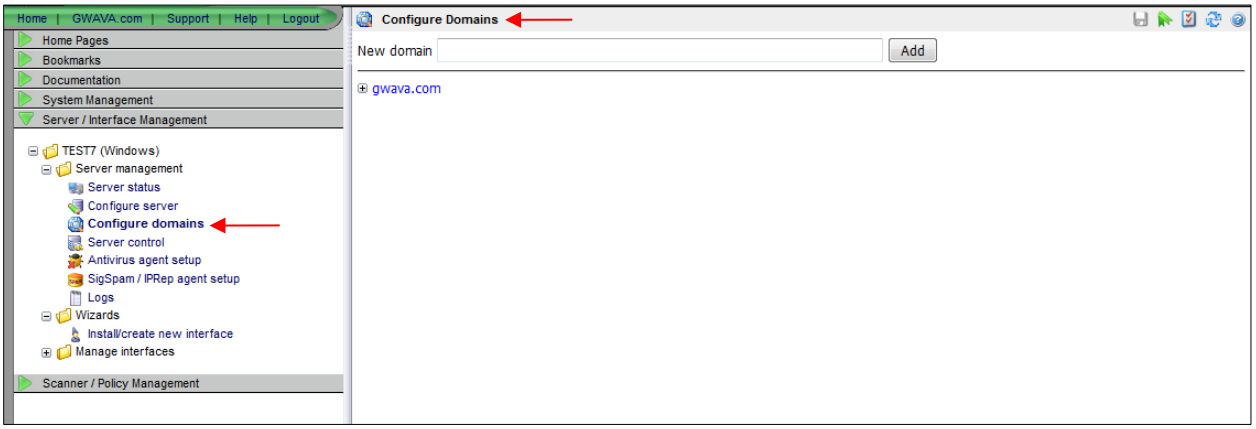
SMTP Interface

The SMTP interface is the most recent option to the GWAVA system, and allows the incoming and, or, outgoing mail to be intercepted, scanned, and filtered independent of the mail system. This setup has the distinct advantage of relieving the mail system of unnecessary and unwanted traffic, leaving mail system resources open to function with greater performance and security.

The SMTP interfaces adds a layer between the GWIA, or any other mail system's SMTP sending agent, and the internet. Sending mail is forwarded through an SMTP proxy, which then sends the filtered, clean mail to the original recipient. Incoming mail is scanned via the SMTP interface, which then sends the filtered and clean mail to your mail system, unaltered. These interfaces allow GWAVA to act independently of your mail system.

The SMTP interface will only work if your MX record points to the GWAVA SMTP interface for mail delivery, and if your domain and mail system SMTP are listed correctly in your GWAVA system.

GWAVA SMTP will then forward the clean mail to the SMTP Gateway specified during server activation. To view or change the domain and SMTP for your Mail system, go to **Server/Interface Management | <Server Name> |Server Management | Configure domains**.

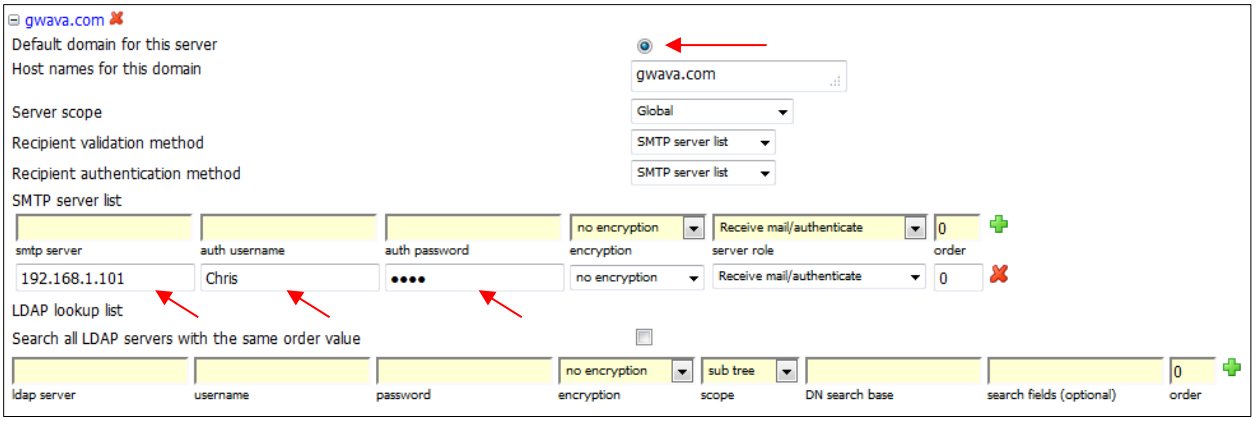


The default domain specified during Server Activation will be specified. Additional domains may be added through the new domain addition field along the top of the screen. As always, make sure you save all desired changes made to the page before browsing to a different section of the management console.

The Mail relay agent SMTP Server and Default domain MUST be correct for your system. If you have multiple domains, you must list the additional domains. GWAVA will only accept mail for the listed domain(s). Domains can be deleted or removed from the system by selecting the domain, then the red 'X' next to the selected domain name.

Select the desired domain to expand and modify the settings for the desired domain. The default domain settings are shown below.

When a domain is selected, it is expanded and allows for multiple settings for user mail validation.

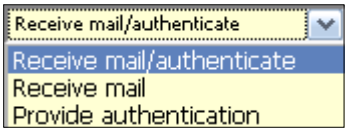


GWAVA checks for valid users for each message received, blocking those which are undeliverable due to an incorrect domain or nonexistent user for each domain. GWAVA must have a connection to an active SMTP server for each domain to verify the users. LDAP lookup is also supported. If users or messages are received which do not contain domain information, GWAVA checks these users against the default domain. Be sure to set the default domain for your system.

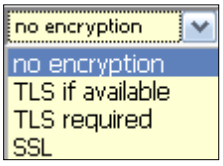
Multiple SMTP or LDAP servers are supported for failover purposes. If a SMTP server is unavailable GWAVA will send messages to the next available SMTP server listed according to the 'order' value. The 'order' values lowest numbers first, usually with the default SMTP listed as '0', second as '1', and so on.

If the SMTP server requires authorization, then the user name and password must be provided for each SMTP server listed. Generally, the authorization username and password will not be needed unless the SMTP server has been specifically configured to only accept authorized connections.

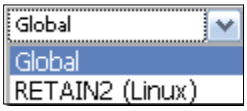
GWAVA shares the user list for each domain between the GWAVA modules, and specific SMTP servers can be selected to serve in different roles for each system, such as using one to receive mail, digests, and notifications, while another is used by QMS to authenticate users. Default settings allows SMTP servers to serve in all roles.



If the SMTP server requires encryption such as TLS or SSL, the setting must be correct.



If the GWAVA server is part of a GWAVA system network with multiple GWAVA servers, then the information from the domains can either be shared across the GWAVA network, or it can be made specific to this one server. For most all systems the option of 'Global' will work sufficiently.



LDAP (optional)

GWAVA supports the option to use LDAP user authentication instead of SMTP authorization for QMS authorization and recipient verification. In general, this will not be required for most systems; LDAP information is only required if you wish to use LDAP for lookup or authentication.

In order to use LDAP for user lists and authorization, the LDAP lookup information must be filled in.

For the LDAP server connection address, place DNS name or IP address of the server

The username and password need to be a full LDAP username including context. The user should have administrator rights.

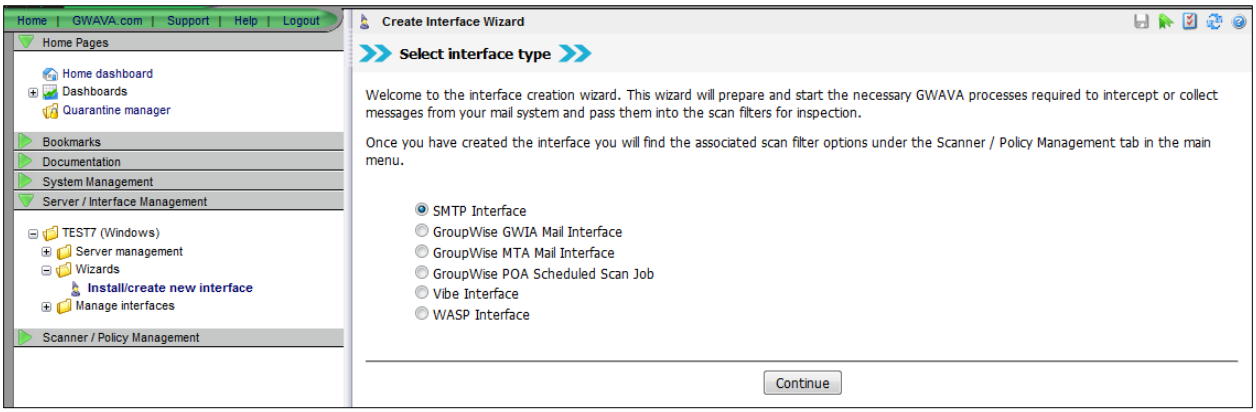
The DN search base can be set to specify the LDAP tree where GWAVA will begin to search for objects. For eDirectory this field can be left blank, though if set, it specifies a starting point for the search in the LDAP tree. (For instance: `ou=users,o=gwava`) If using Active Directory the DN **must be set** for the user list to work. (ie. `CN=users,DC=exg,DC=gwava,DC=com`)

Search fields are usually not necessary for any system to setup, but can be useful if desired. By default, most LDAP servers (including eDirectory and Active Directory) have an attribute applied to an object of the type "mail" which contains the object's or user's email address. If you have email addresses for users stored under an attribute other than mail you can specify the possible attributes by separating them with commas.

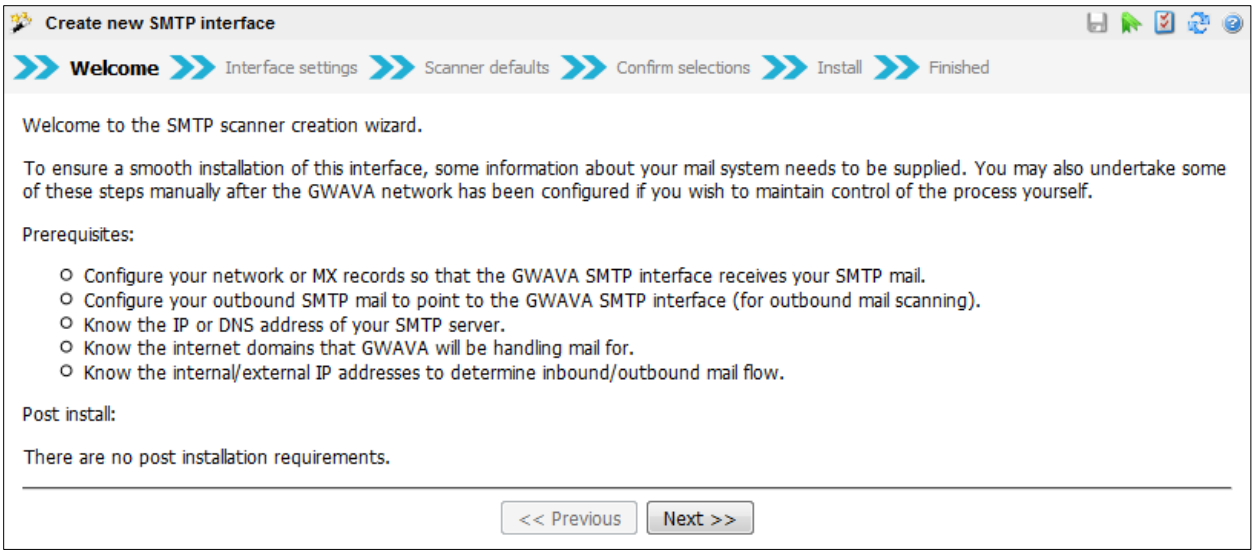
In the example below the LDAP server is set to search for the attributes ‘mail’ and ‘secondarymail’.

Once the Domains have been properly configured for the system the SMTP interface, and any other interfaces, may be properly created.

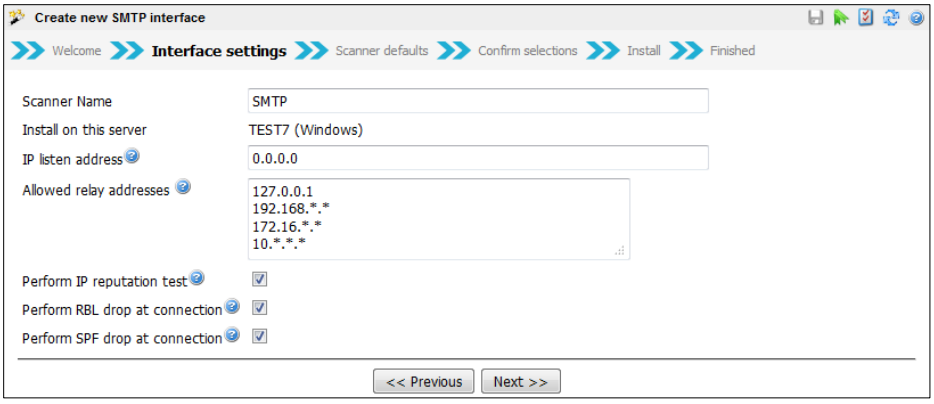
Open the Interface creation wizard, (found under **Server/Interface Management | <Server name>| Wizards | Install/create new interface**), and select the SMTP Interface and follow the instructions to install.



The SMTP interface creation wizard informs you of the information you must know to successfully create the interface.



The **Interface Name** is whatever you wish the interface to be named in the GWAVA server.



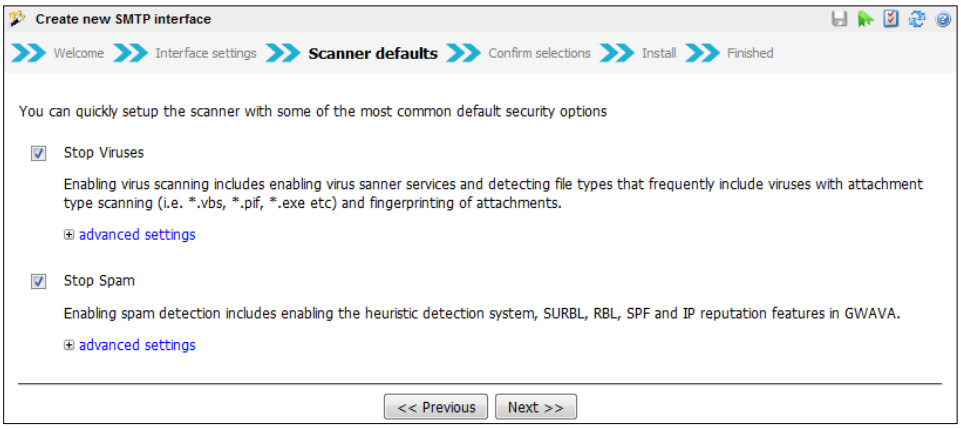
The **IP listen address** is the address that the SMTP interface will bind to and listen on. It should be the address of the GWAVA server. This should also be listed on the MX record for your domain. (If the SMTP interface resides on the same machine as the GWIA, then the GWIA must be changed to listen on a port other than 25, as the SMTP interface uses that port. Then inform GWAVA that the 'Mail relay agent SMTP server' – or GWIA – listens on a port other than default. This setting is found on the Server Configuration page. Append the port at the end of the address with a colon (`10.1.1.10:26`). See "GWIA and SMTP interfaces on the same box" for more details.

Allowed relay addresses are the source addresses which are allowed to send mail through the GWAVA SMTP interface. Your mail system SMTP address should be listed here, as well as any other mail sending source for your domain. Mail coming from these addresses will be treated as outbound mail. No source but these listed addresses will be allowed to send mail through the SMTP interface.

The red 'X' removes listed address ranges and the blue 'add…' link provides an extra address/ range box.

IP Reputation, **RBL**, and **SPF** drop at connection settings are recommended as default. This dumps any incoming message that fails these initial incoming tests, saving bandwidth and performance.

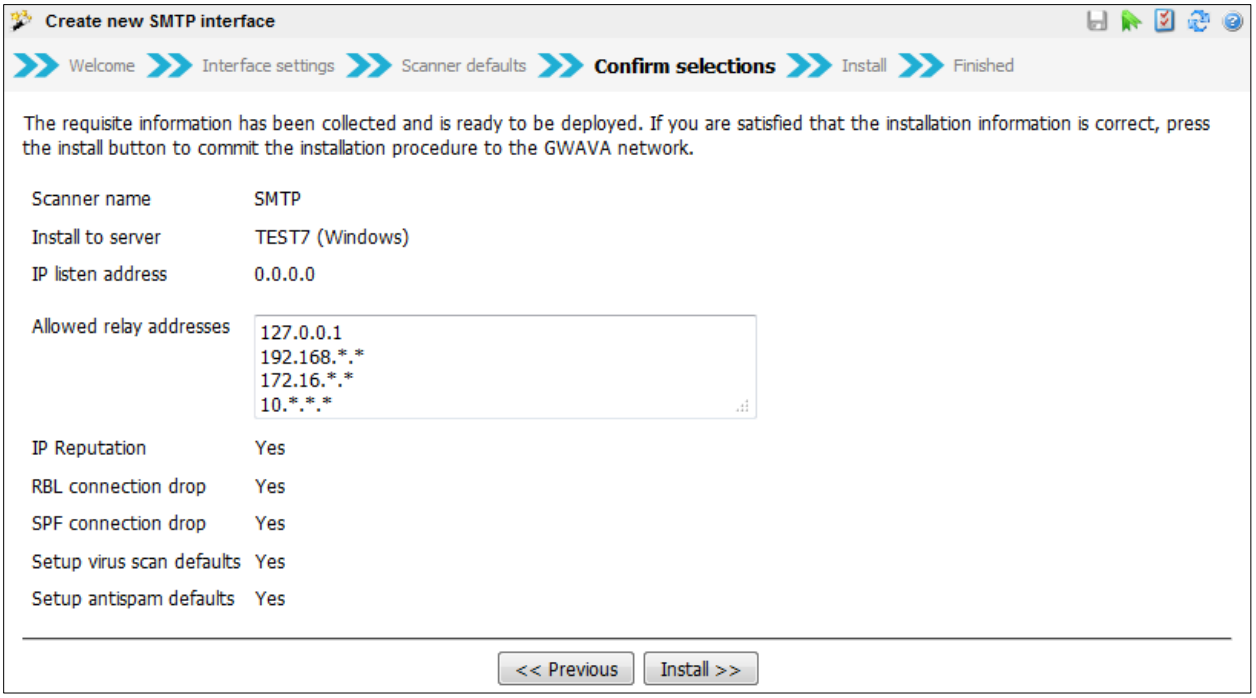
Select your default preferences, and click 'Next'.



Set the default actions for viruses and spam. These settings can be changed after interface creation.

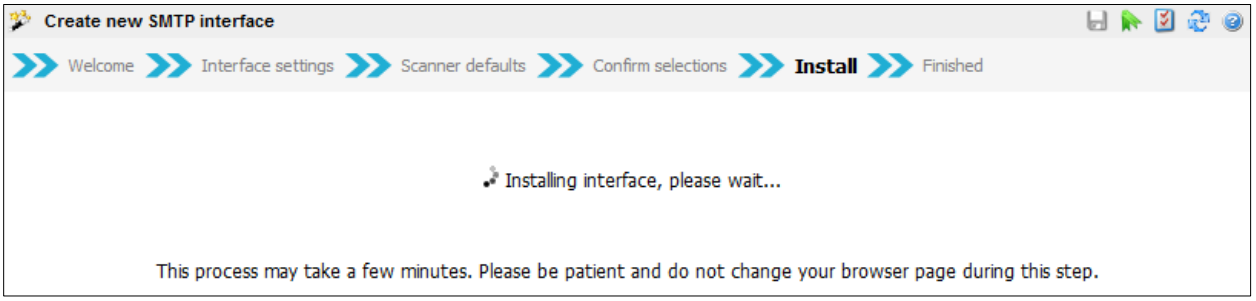
Click 'Next'.

Review and confirm your settings. If you wish to make changes, use the '**back**' button on your browser, correct the information, and Next.

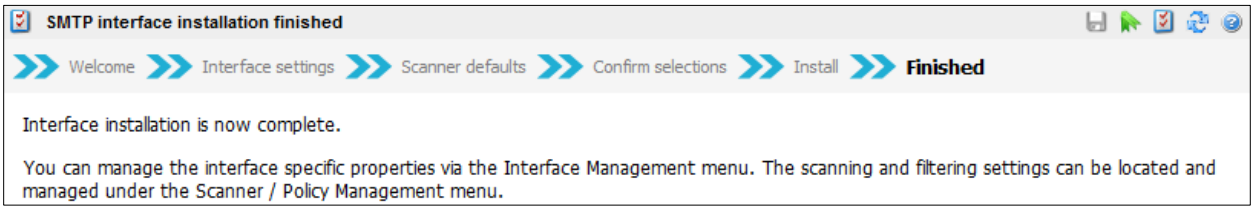


Click '**Install**' to continue.

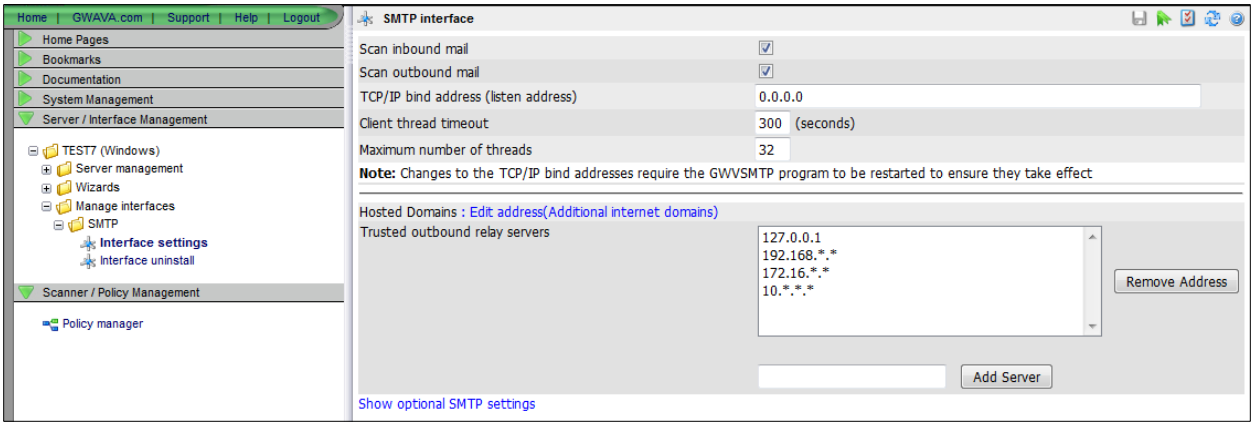
The interface will be installed.



Wait while the installation completes.



Once installation is complete, click 'Home' at the top left of the page to refresh the system, then navigate to the **Server/Interface Management | <Server Name> | Manage interface folder** to view your new SMTP interface.



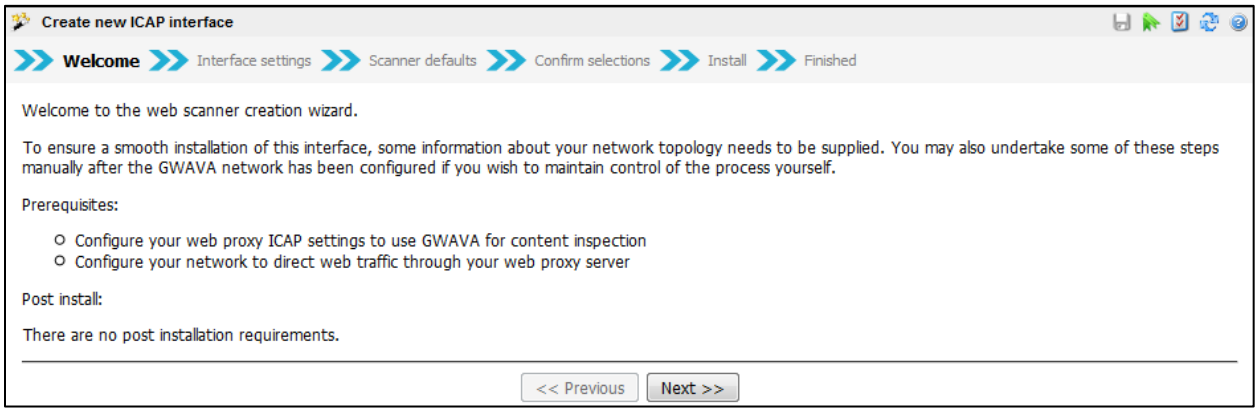
Your SMTP interface is now created and ready, and the policies are automatically managed until changed. For further configuration, see the 'Policy Manager' section.

Once the MX record pointing to the GWAVA SMTP is active, the SMTP interface will begin filtering mail.

Web Interface

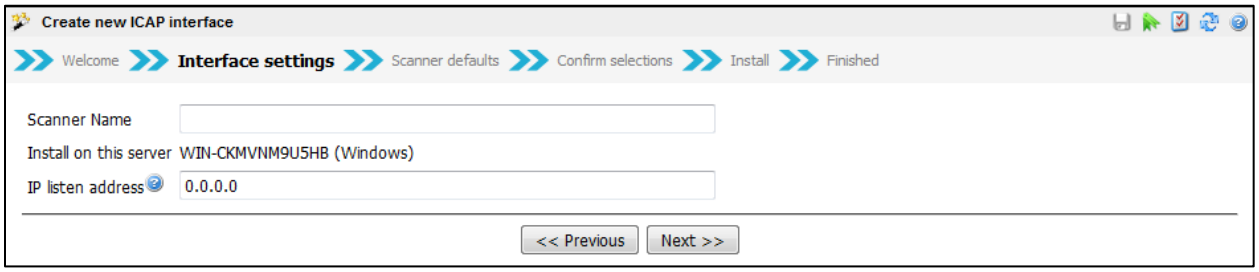
The Web Interface allows GWAVA to filter web traffic. The Web Interface can search all web traffic to block URLs, key words in web page text with body filtering, or it may be used to limit traffic through web user authentication. The Web interface works in conjunction with an existing ICAP enabled proxy, such as squid.

To install the Web Interface, select the Web Interface from the list and click ‘Continue’.



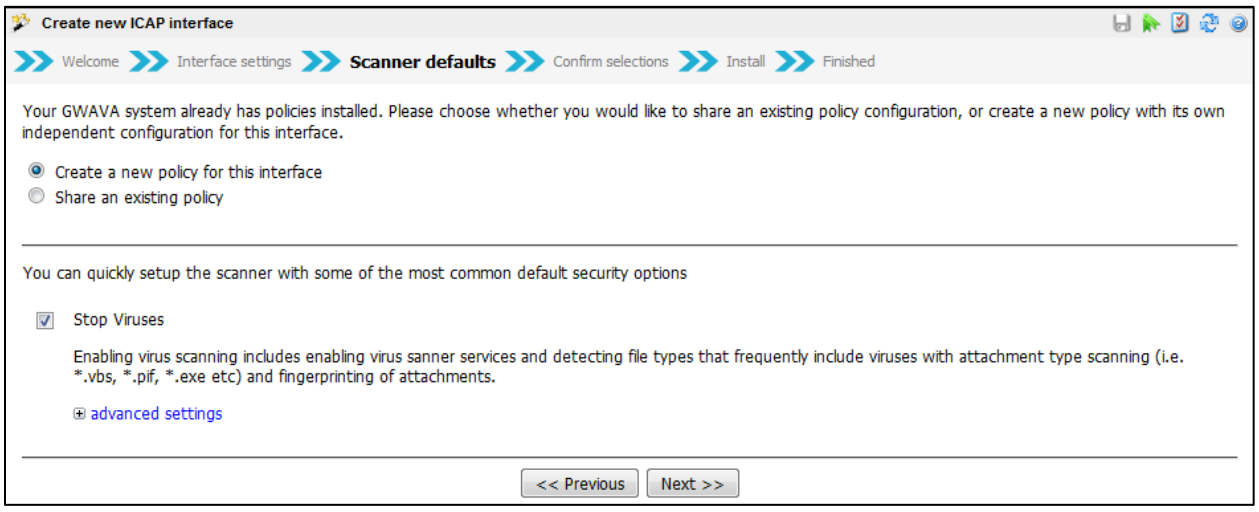
The Web Interface requires a connection through ICAP to the existing web proxy. If using squid, the configuration file needs to be modified. (See the squid configuration file addition in the appendix.)

After reviewing the necessary changes needed, click ‘Next’ to continue.



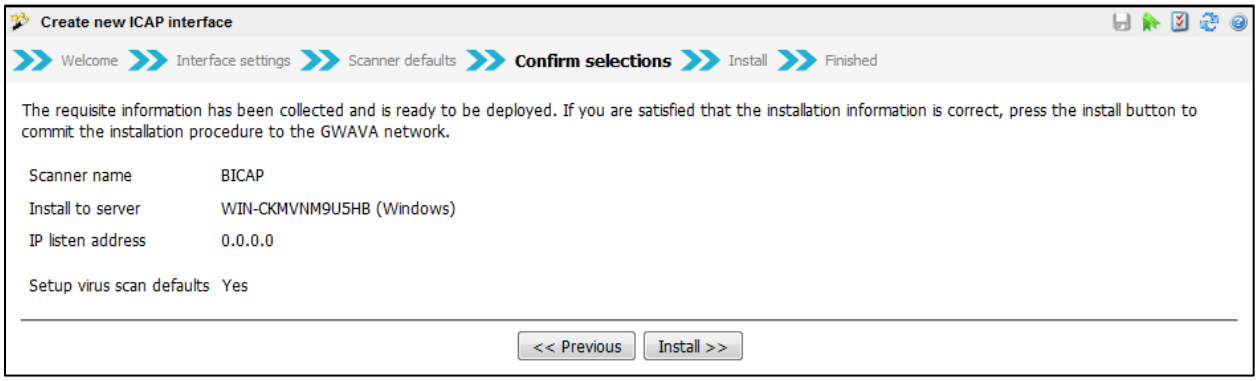
Name the interface as desired and will not affect scanning.

The IP listen address is the address that the web interface will bind to and listen on. This should be the address of the machine where GWAVA is housed, or the desired interface on machines connected to multiple networks.

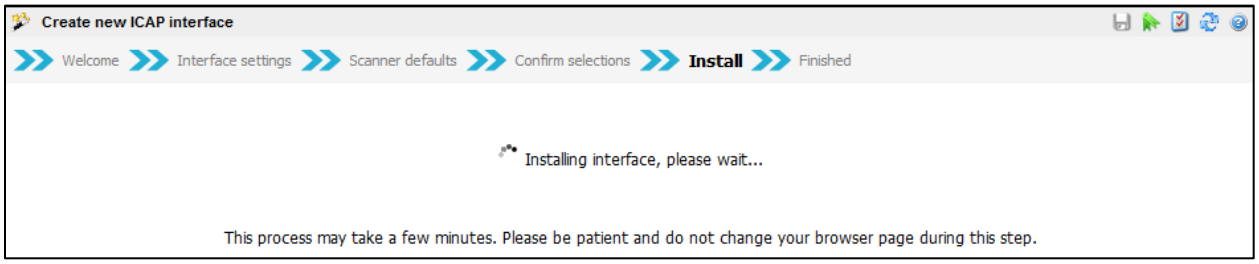


It is highly recommended to create a new policy for the Web Interface. Due to the architecture and use of the interface, many of the tests and options will not apply and may only serve to slow-down web service. One such option is the spam scanning engine, which, due to keywords on web pages, will end up blocking nearly everything and drastically slow down service. It is NOT recommended to scan for spam on the internet. Setting up an individual setting and then configuring it for the host system is highly recommended.

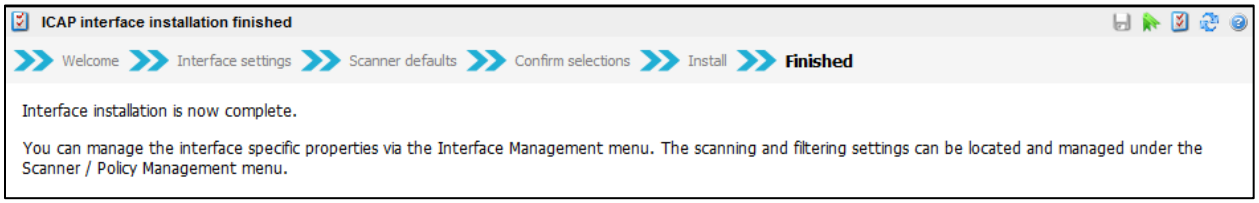
Though the Web Interface is subject to all the different scans and filters in the GWAVA system



Review the information and click 'Install' to create the interface. Select 'Previous' to correct or change any information.



Wait for the ICAP interface to install.

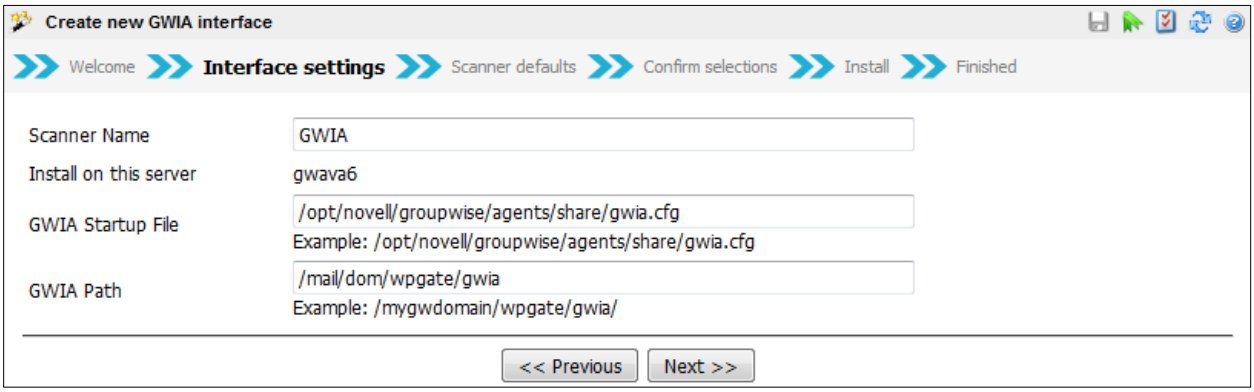


Once the interface has been installed, its settings can be managed through the **Scanner | Policy Management** menu.

GWIA Interface

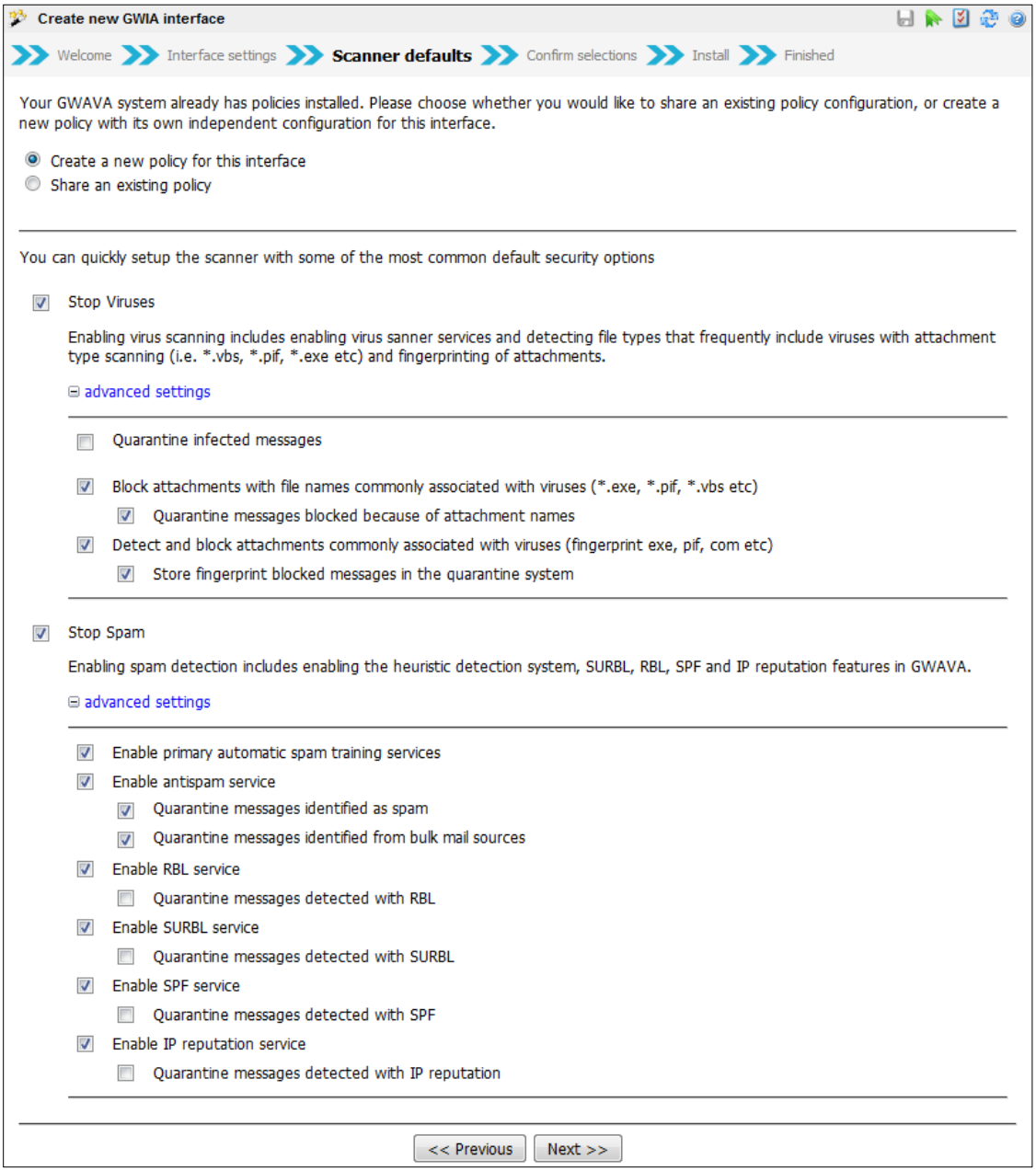
To install a GWIA interface, you must tell the wizard where the active GWIA directory and the GWIA configuration file are located. The GWIA interface puts startup information in the GWIA configuration file and adds the 3rd directory to the GWIA directory structure. To make the changes to the GWIA configuration file active, the GWIA must be restarted after the installation is complete.

Name the interface and provide the locations to the directory and file required. Use the example paths as your guide, though they are only examples and will differ from your actual paths. Always double-check your paths to ensure that the interface will install correctly.



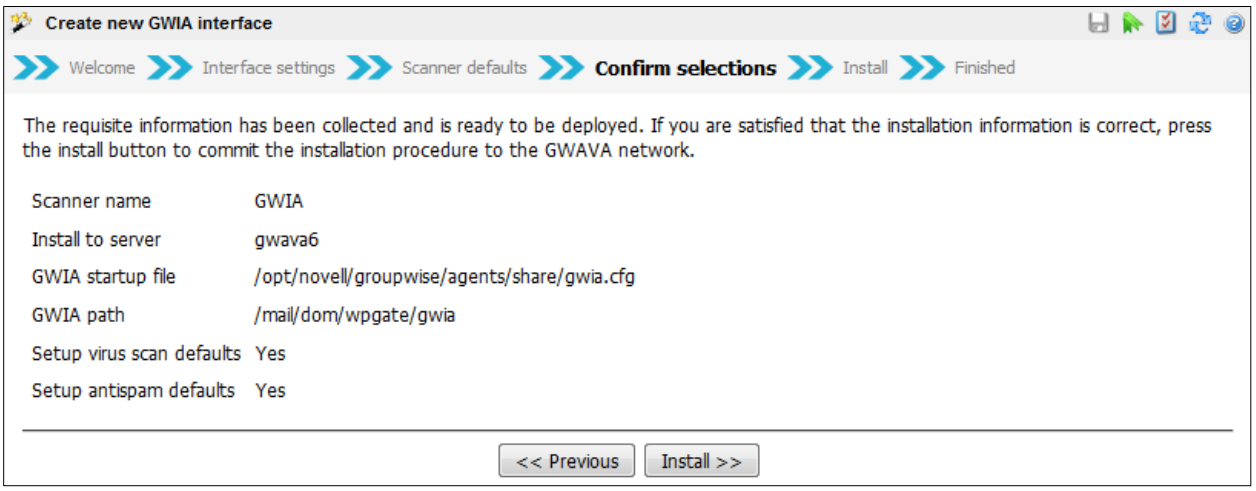
If the directory path is incorrect, your mail will not flow after the GWIA has been restarted to enact the changes.

Select your basic scanning setup. All the default options are shown below and are fairly self-explanatory. The virus and basic spam scanning options are for setup purposes only. These can all be changed and customized after the interface setup is complete. There are many other options to fine-tune the interface which are only available after the interface has been created. Select the basic setup options you wish to use as default and click Next.

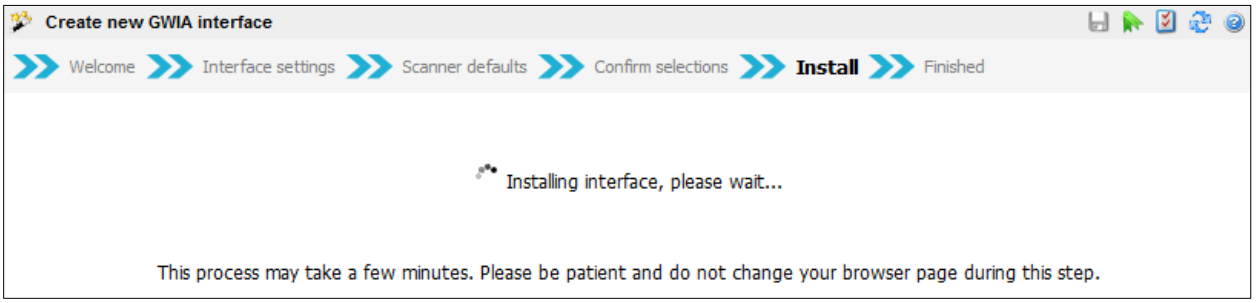


The wizard will ask for confirmation on the information provided. Double check all information and paths to ensure that the interface will function correctly.

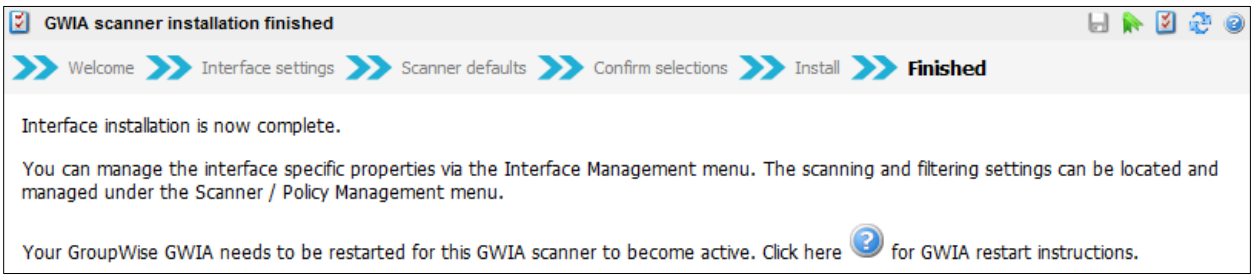
Select the install button when you have verified the information.



The wizard will display this page while it is working.



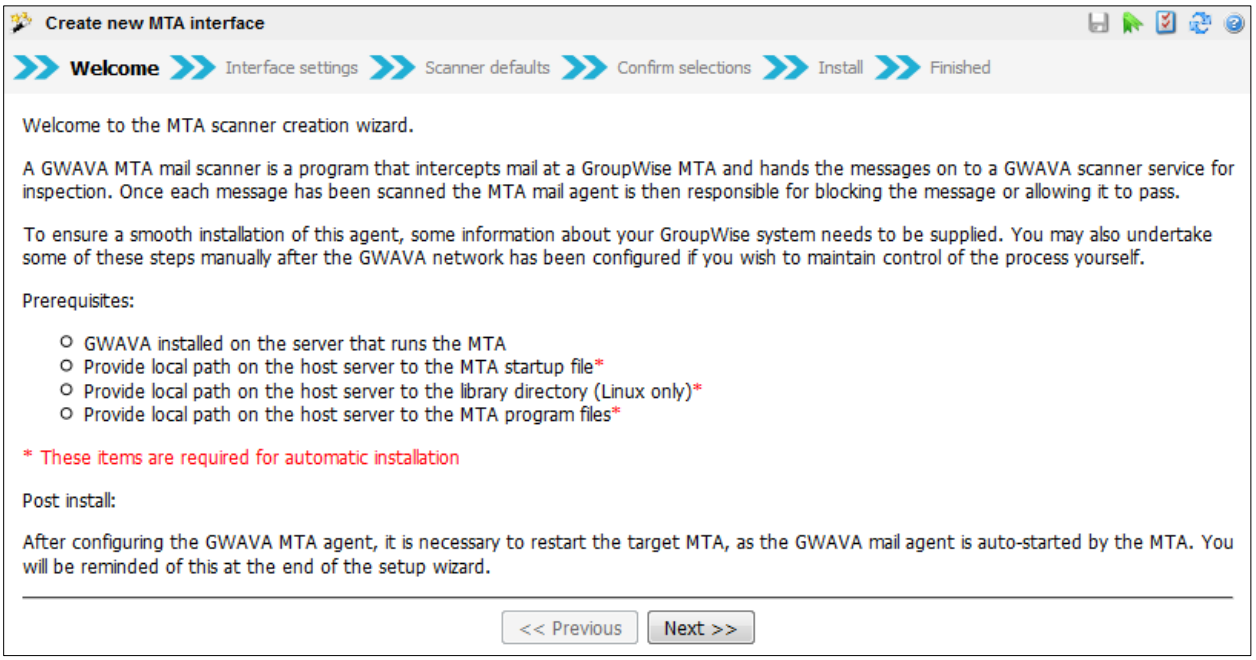
DO NOT browse away from the page until the next page is displayed showing a confirmation that the process is complete and detailing instructions to move forward.



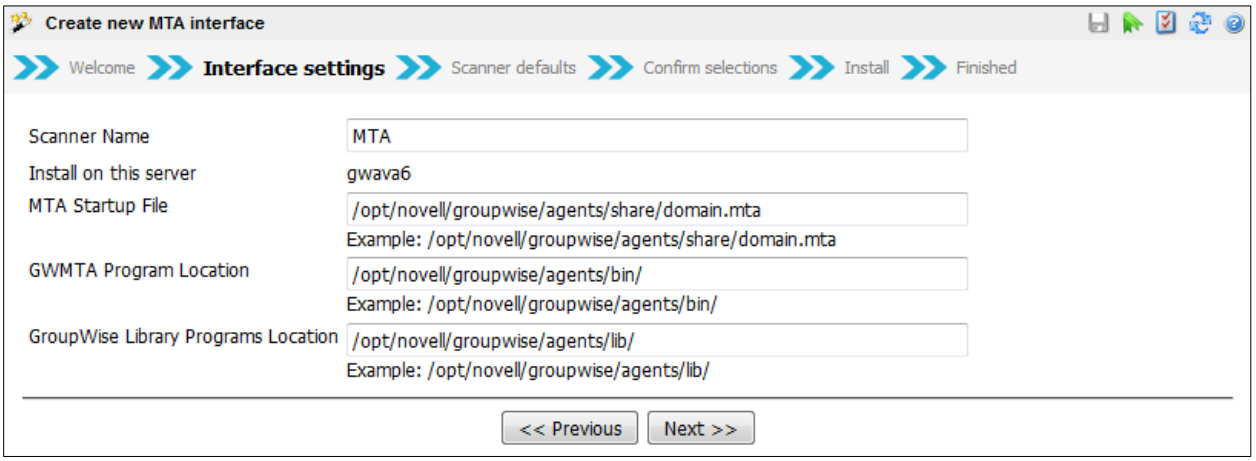
The interface installation is now complete, and the interface is now available for fine-tuning and customization.

MTA Interface

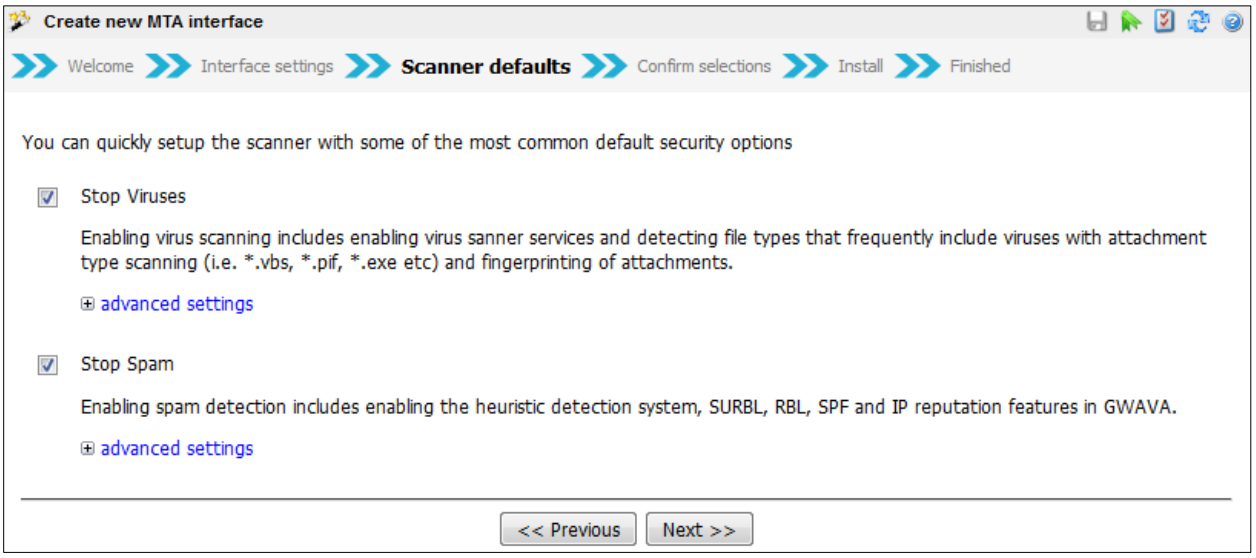
The GWAVA MTA interface can only be installed on a Linux platform. To create an MTA interface, select the MTA interface from the wizard and click next.



MTA interface creation lists the information that is required. The paths to the MTA startup and program files as well as the path to the library directory must be provided.

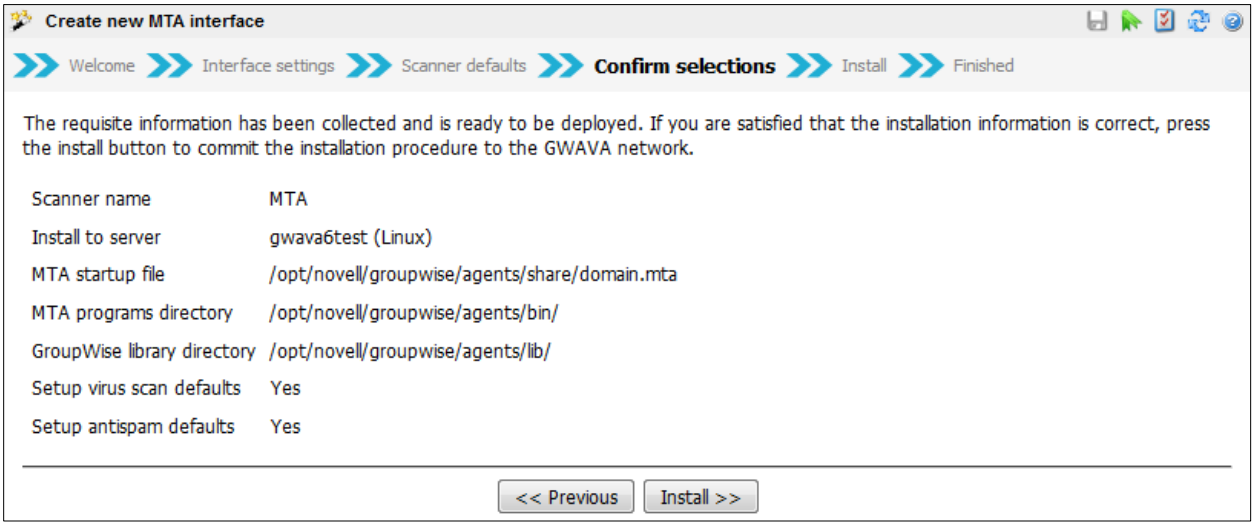


Provide an interface name and the paths to the files listed, (default suggestions are shown, but are not always correct for every system). Use the example paths as a guide, but know that the paths will differ from system to system.



Set your desired settings and click 'Next' to progress to the next page.

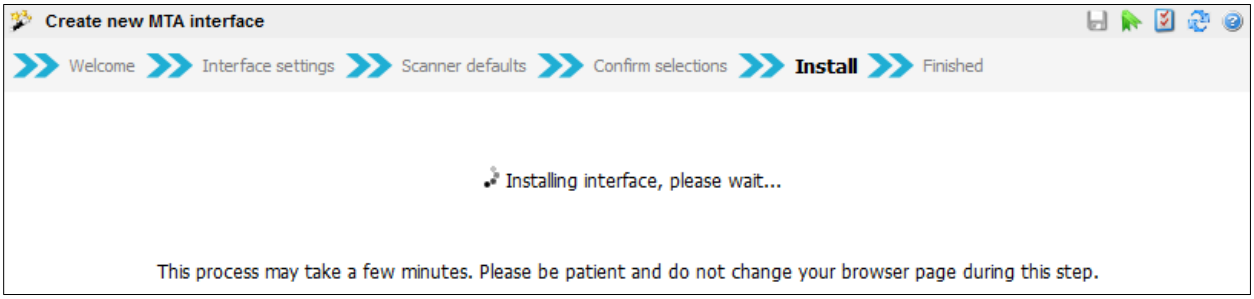
Due to environmental variables, the MTA interface will not function on Windows GroupWise systems.



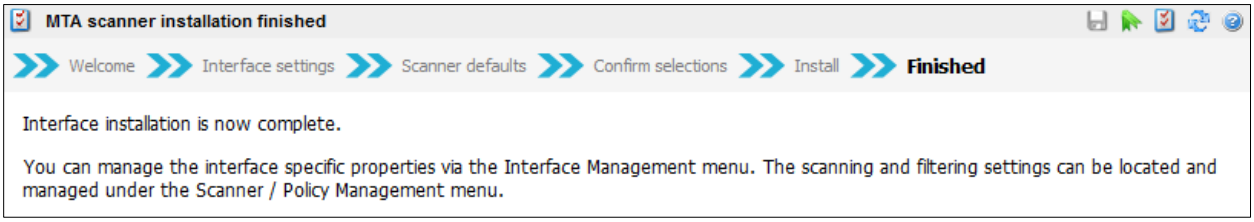
Double check and confirm the information provided.

Once the information has been confirmed, select install.

The interface will be installed.

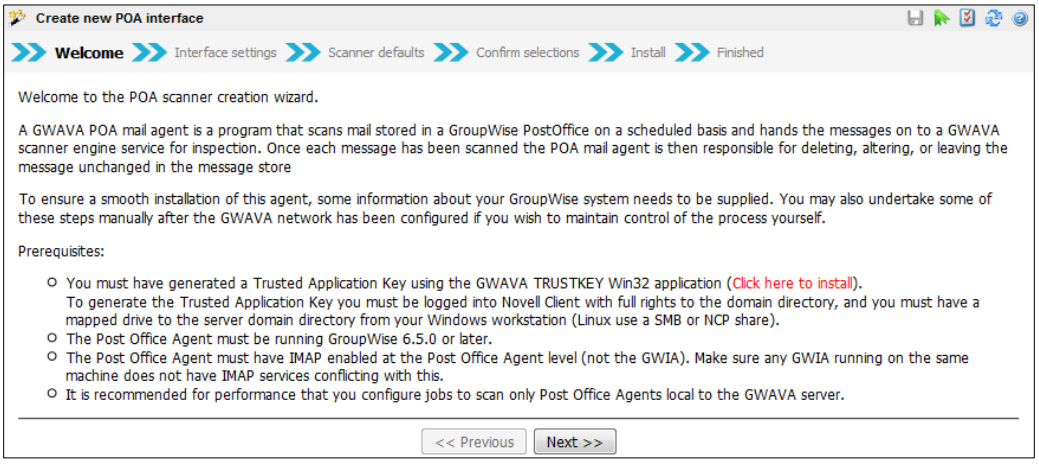


Wait until the following page is displayed. Your interface is installed and ready to use following a restart of the MTA.



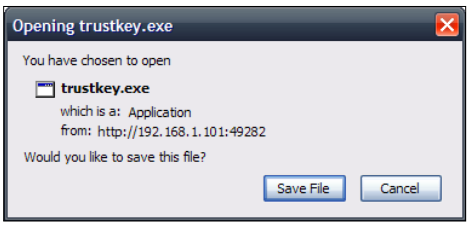
POA Interface

To install a POA scheduled interface, select the POA interface from the wizard menu and click next.

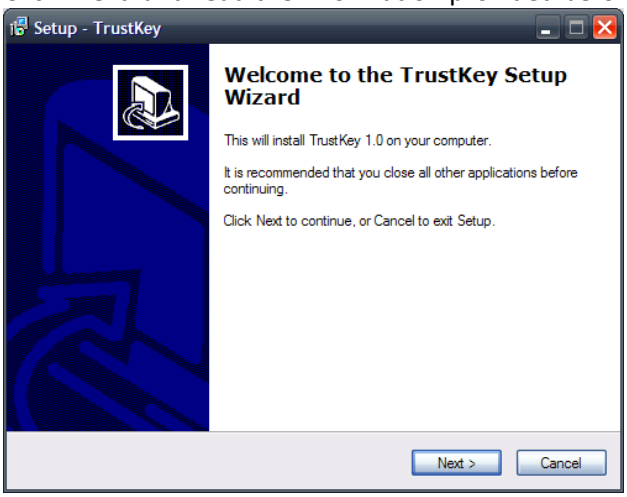


The POA interface connects directly to the POA through the IMAP interface. As such, it requires a trusted application key to be created and IMAP must be enabled and open on the POA. Download and install the TRUSTKEY application and generate the Trusted Application key. To generate a trusted application key, you must run the TRUSTKEY application from a windows workstation that is logged into the GroupWise system with Administrator rights. TRUSTKEY also requires access to the wpdomain.db file. If installing on Linux, this must be accessible through a SAMBA share.

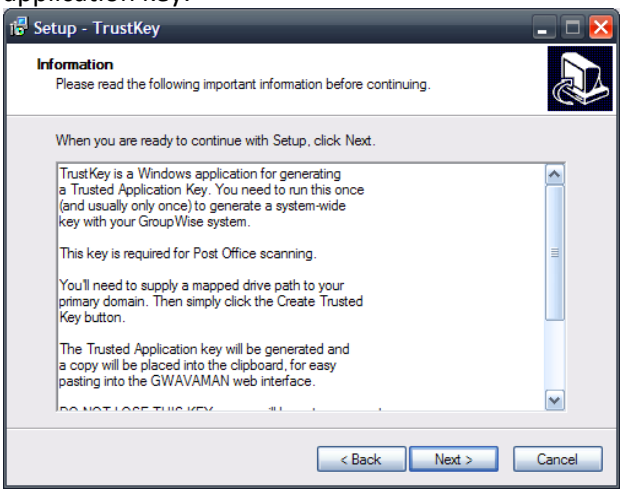
Click on the TRUSTKEY install link, and save then run the trustkey.exe application.



Click 'Next' and read the information provided before continuing.



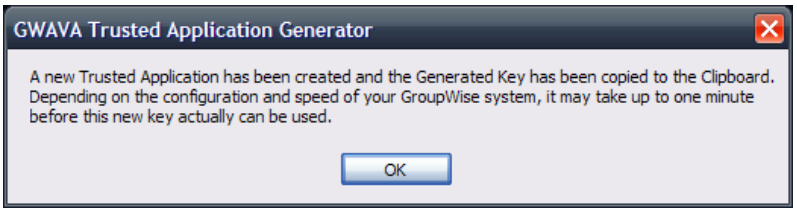
The Trustkey application will create a trusted application key for GWAVA to access the Post Office with administrator rights. The information dialog also details exactly what is required to create the trusted application key.



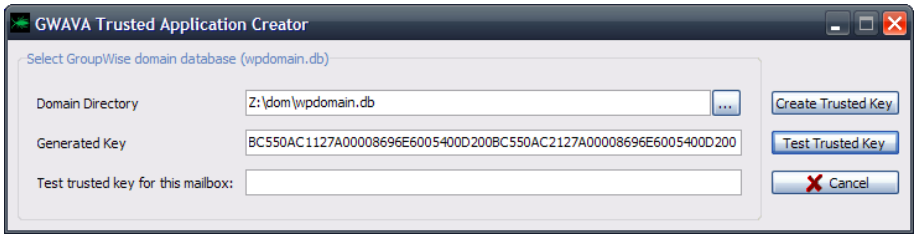
Click 'Next' to continue to the application creator window.

Browse to the domain directory containing the active wpdomain.db. This directory must be accessible from the Windows workstation where the TrustKey application is running. The Windows box also must be logged into the GroupWise system via the Novell client, with administrator rights. On Linux, this directory must be accessible through a SAMBA share.

After browsing to and selecting the wpdomain.db file, click 'Create Trusted Key'.

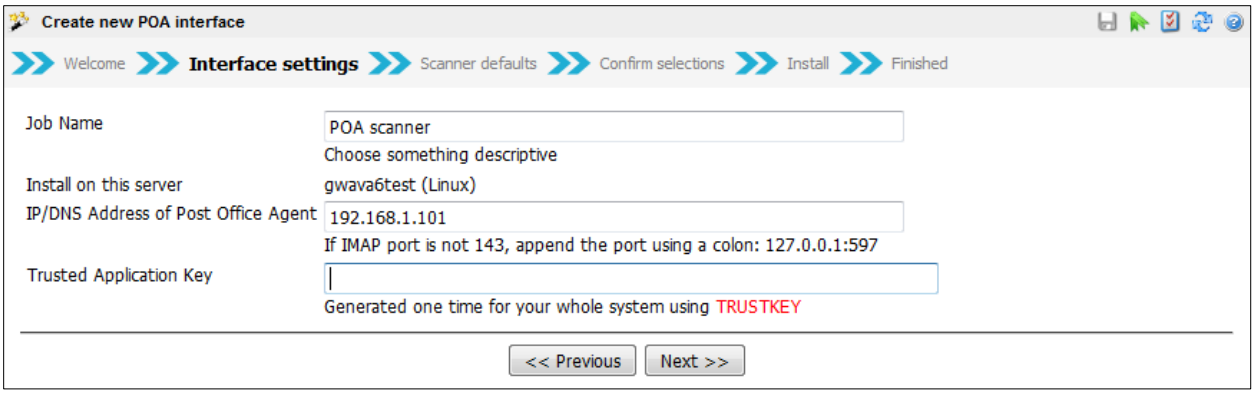


The TrustKey application will create a trusted application key and automatically copy it to the clipboard as well as display it in the 'Generated Key' box.

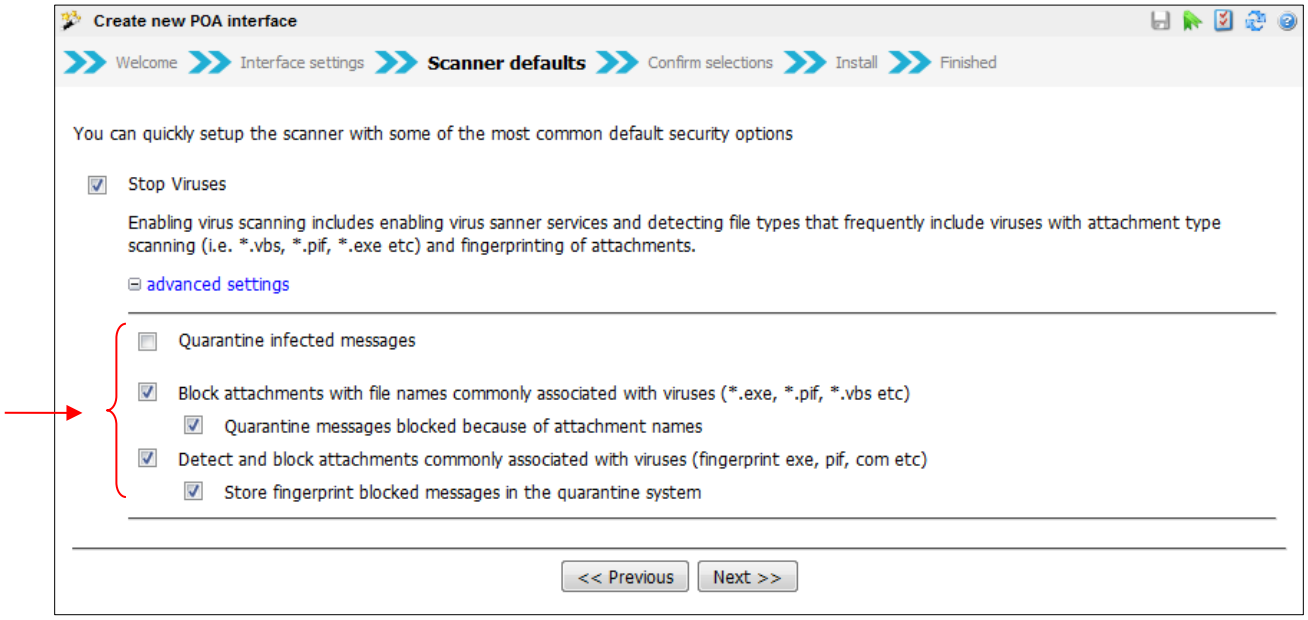


Paste the copied trusted application key into the POA interface creation wizard and fill out the post office job name as well as the IP address of the Post Office Agent. The IP address must have the IMAP port specified as shown if it is not default. (Default: 143)

The POA Job is not configured after creation. Ensure to continue to the configuration page and complete the required configuration and enable it or the interface will not run.

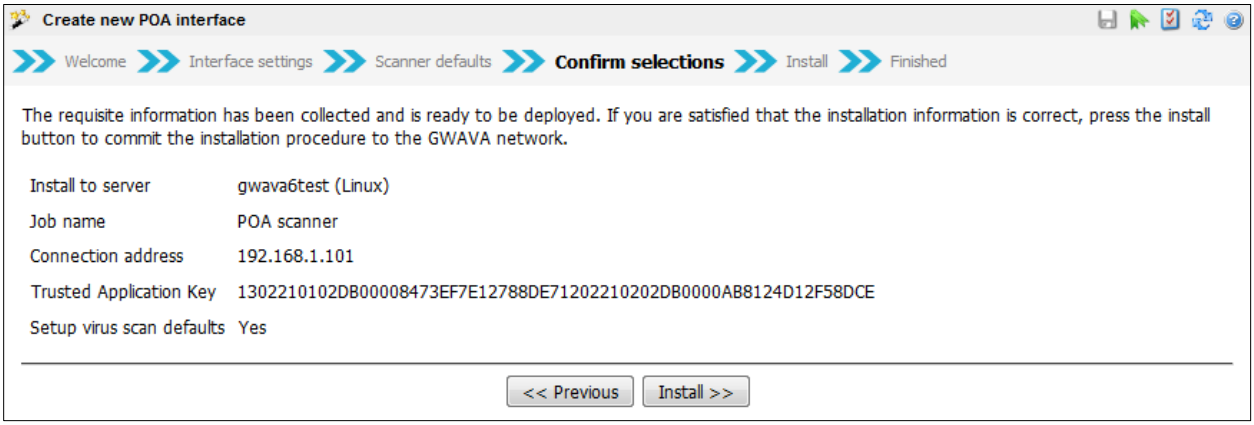


IMPORTANT: On the creation page, ensure that the 'Stop Viruses' box is checked, and then expand the 'advanced settings' link and **uncheck all other boxes**. If the interface is configured to delete email containing attachments, all mail with attachments contained in the fingerprinting and attachments lists will be removed from the post office. Removed mail may be unrecoverable.

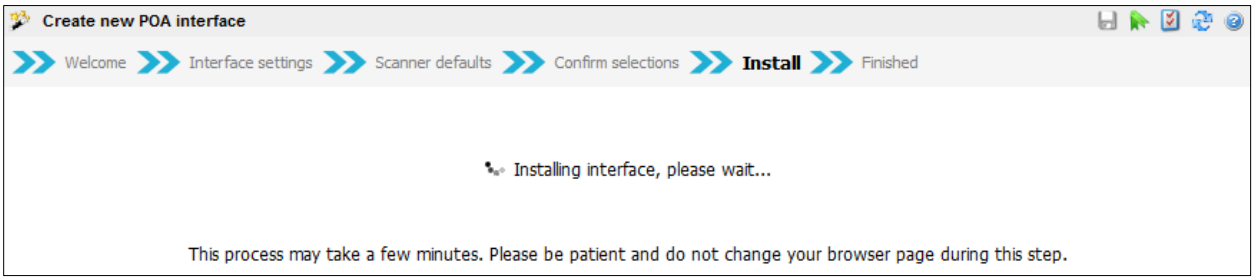


After verifying that the interface creation page looks identical to the one shown above, click 'Next'.

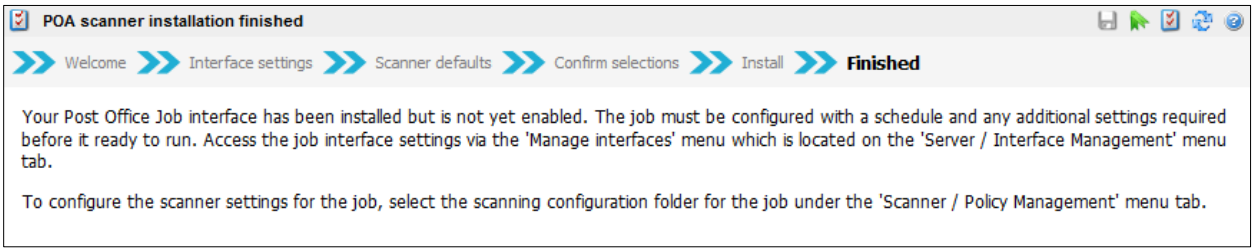
The interface will be installed.



Verify the specified information and select 'Install' if the information is correct. If you need to correct anything, use the 'Previous' button.



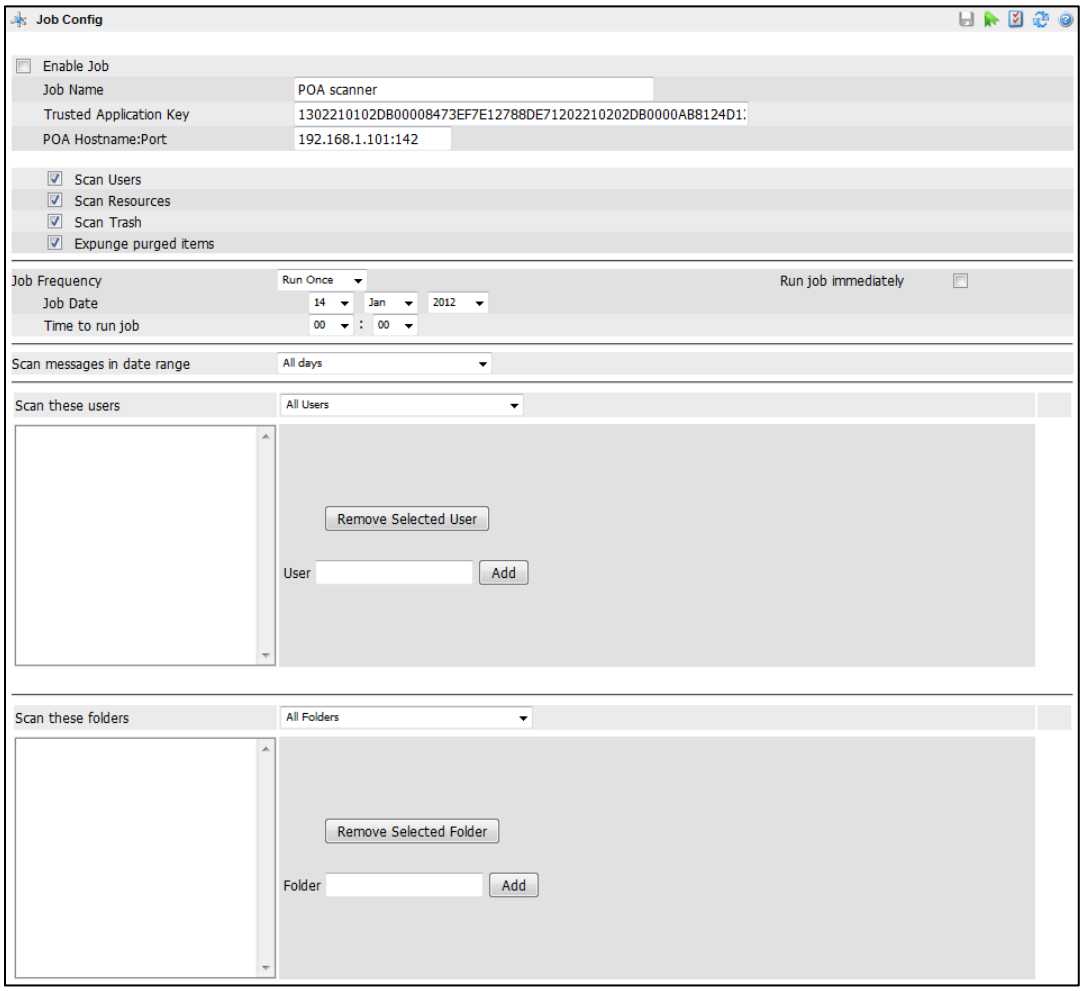
Follow the instruction to wait until the success page is displayed.



Once the job has been completed, click on the 'home' link at the top left of the page to refresh and navigate to the 'Scanner / Policy Management' menu and select the new interface and 'Job Config' to complete configuration.

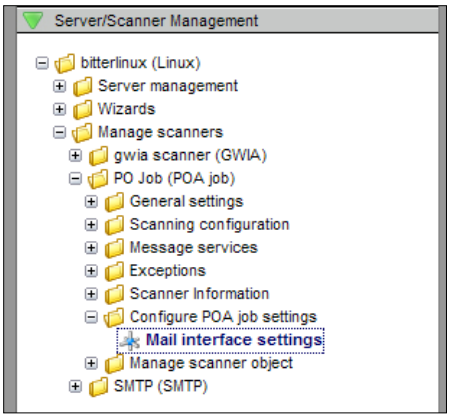
The first task to complete on the configuration page is to enable the job. If the job is not enabled, it will not run.

This page configures the job to include or exclude specific users, folders, and the job start time. Note: the POA job may cause the Post Office response time to lag, causing any connected clients to become sluggish. It is best to schedule the Post Office job to run during off hours, or at times when the Post Office is not under load.



To add specific users to be included, or to exclude specific user mailboxes, you must provide the mailbox name.

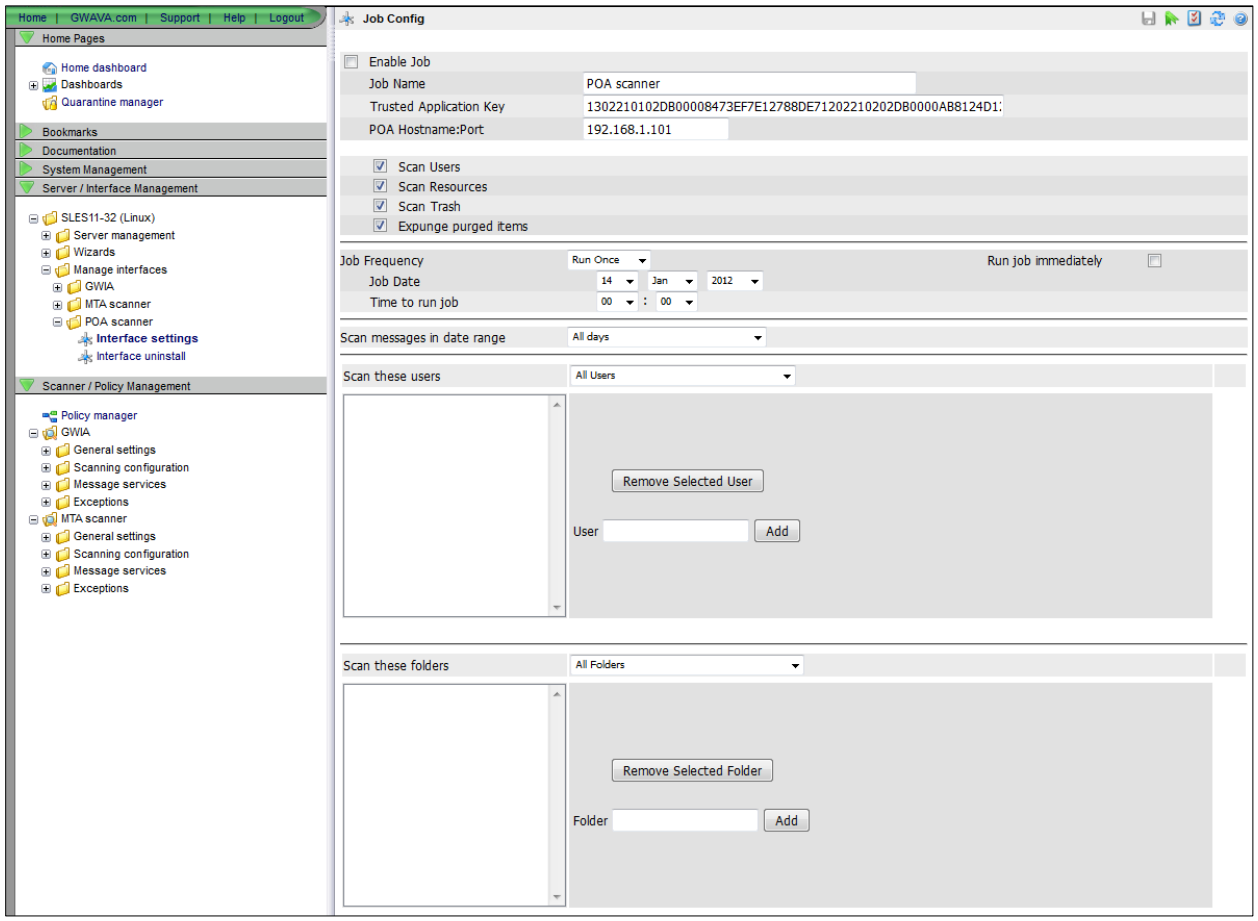
The same applies for Folders. If you wish to include or exclude specific folders, you must supply the folder name.



To specify whether the job will apply to all users or folders, only specified users or folders, or all but the specified users or folders, or to set a date range to scan through, use the drop-down menu for each section.

Once you have enabled and configured the job, make sure to select the ‘save changes’ button at the top of the window before browsing away from the page. Once the changes have been saved, the changes will be sent to the GWAVA system and will become active within a couple of minutes.

To access the POA Job settings page just described, browse to **Server / Interface Management | <server name> | Manage Interfaces** and expand the POA interface and select the 'Interface settings' object under the 'Configure POA job settings' folder, as shown.

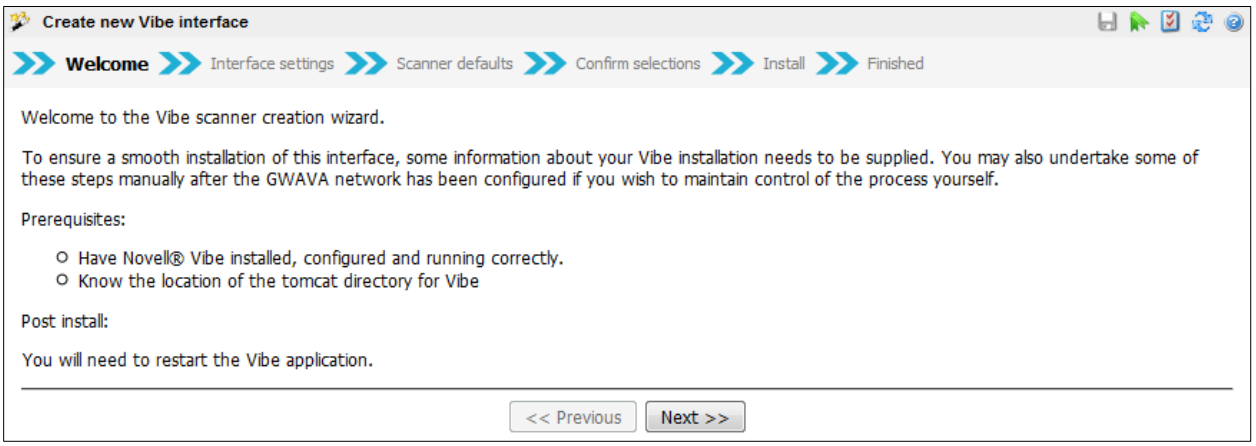


Be sure to finish configuring and enable the job. If the job is not enabled, the POA interface will not be active and mail will not be scanned.

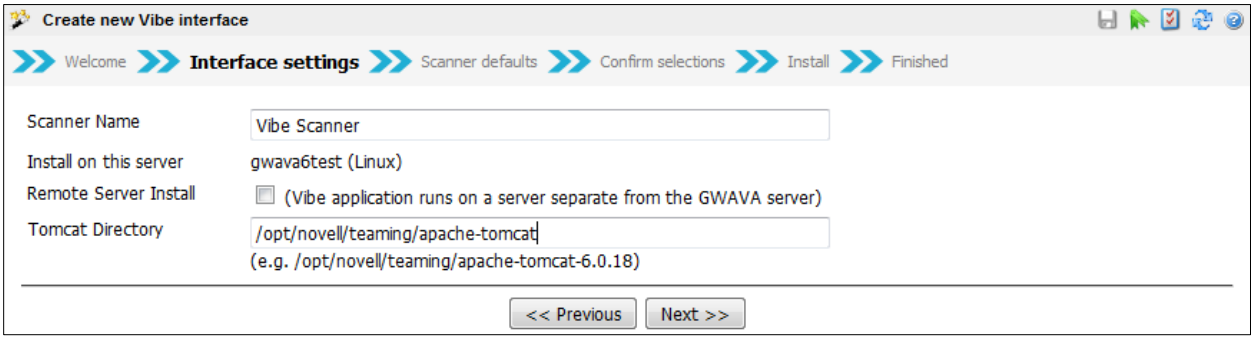
Vibe Interface Install

The Vibe interface filters all text and attachment workflow through the scanning interface, including input text, all attached files, email, and messaging. To install an interface in the Vibe system, Vibe must be installed and running correctly, and the tomcat directory of the Vibe servlet must be known. The Vibe interface may be installed either on the local machine or remotely, similar to a WASP remote interface.

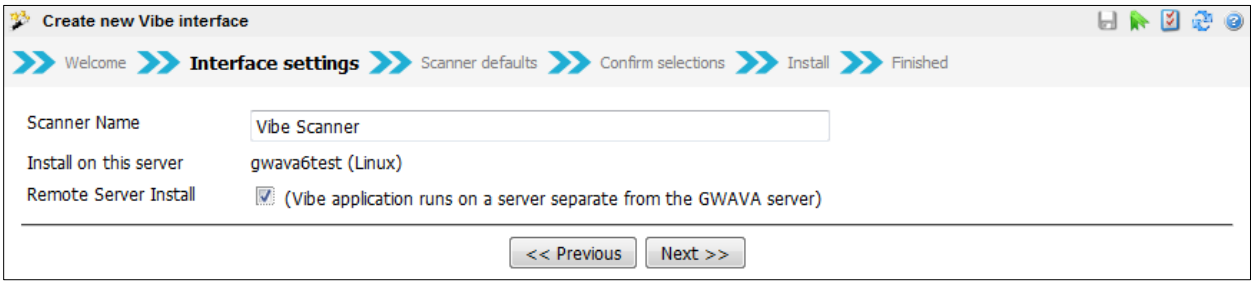
Open the New Interface creation Wizard and select the ‘Vibe Interface’ option. Click ‘Next’.



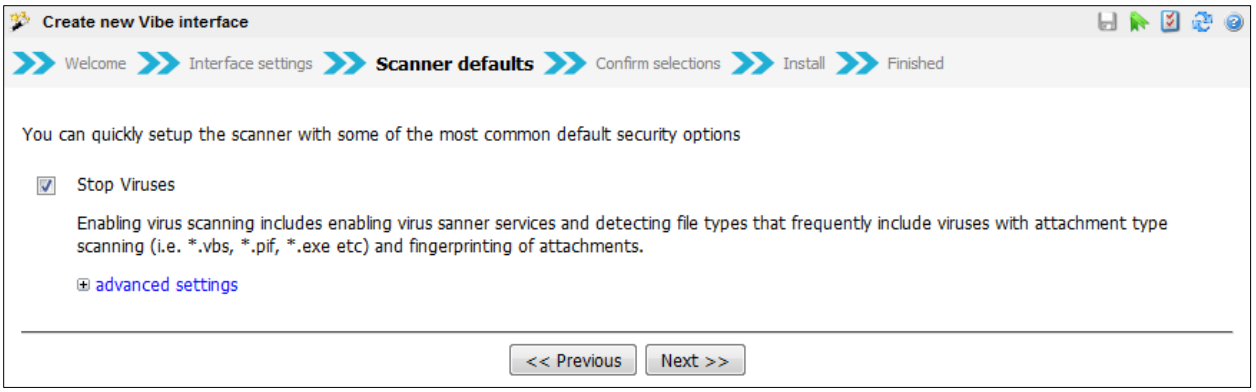
The wizard states the install process and the required information. Gather the information and select ‘Next’ when you are ready to install the interface.



Name the interface and input Tomcat directory serving the Vibe interface.



If the interface is to be installed on a remote server, select the 'Remote Server Install' option and select 'Next'.

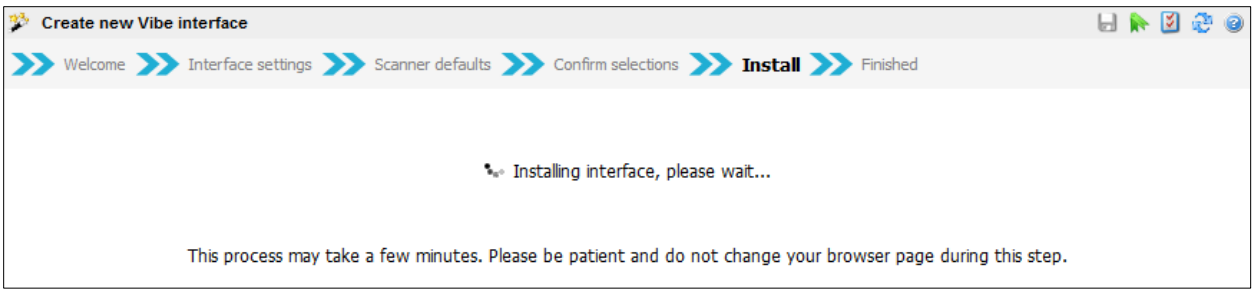


Select the scanning options and configuration for the interface. The interface settings may be changed after the interface is created, and defaults show the blocking of viruses and spam.

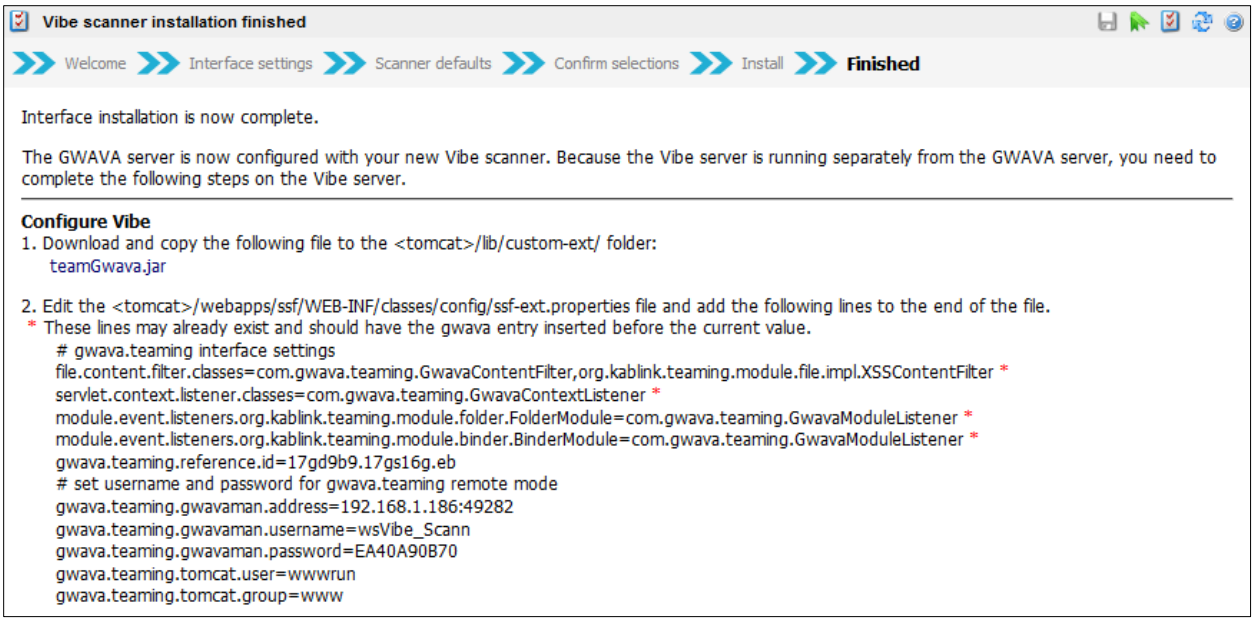
All other configuration for the interface, including keyword filtering, attachment size, attachment type, fingerprinting, oversize and undersize messages, and specific quarantine settings will all be available for configuration after the interface has been created.

Review settings and select 'install' when they are correct.

Wait for the interface to be installed.



After the Vibe interface has been installed, follow the ending instructions for both local and remote installations.



Remote installations will require manual editing of the Tomcat files, as the interface wizard will not have access to them during install. Input the specified lines around the indicated, existing lines in the **ssf-ext.properties** file, so the file section matches the one shown.

Local and remote installs require a restart of the Tomcat system to restart the tomcat server. Instructions on the restart of Tomcat are provided, select the "?" icon to show the instructions.

Now that the interface has been created, it is available to be further configured and customized.

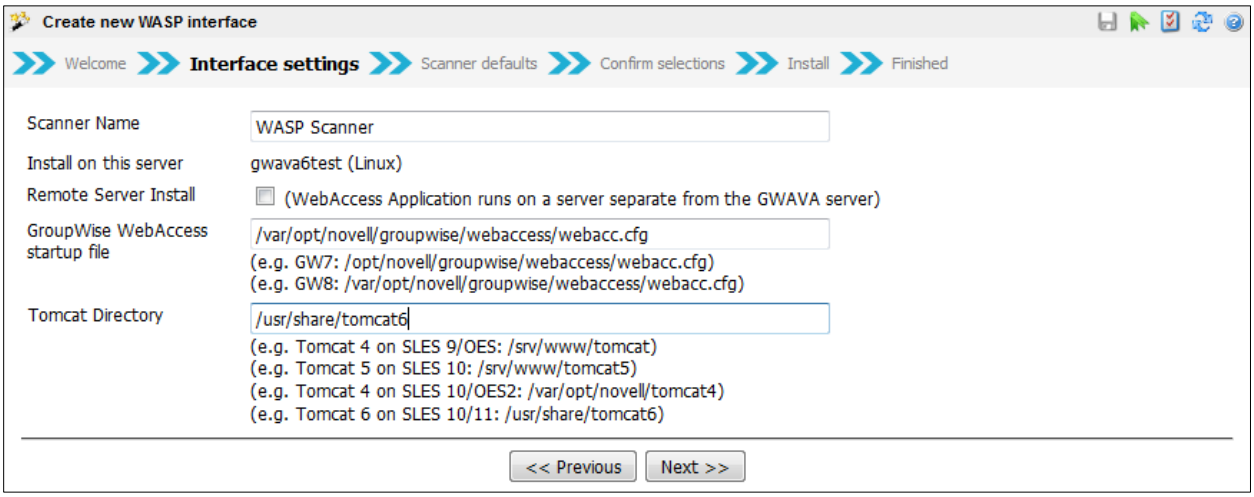
WASP Local Interface

To create an interface, you must know the correct information for the location of the Web Access directory and the active Tomcat directory. Click **Next.**

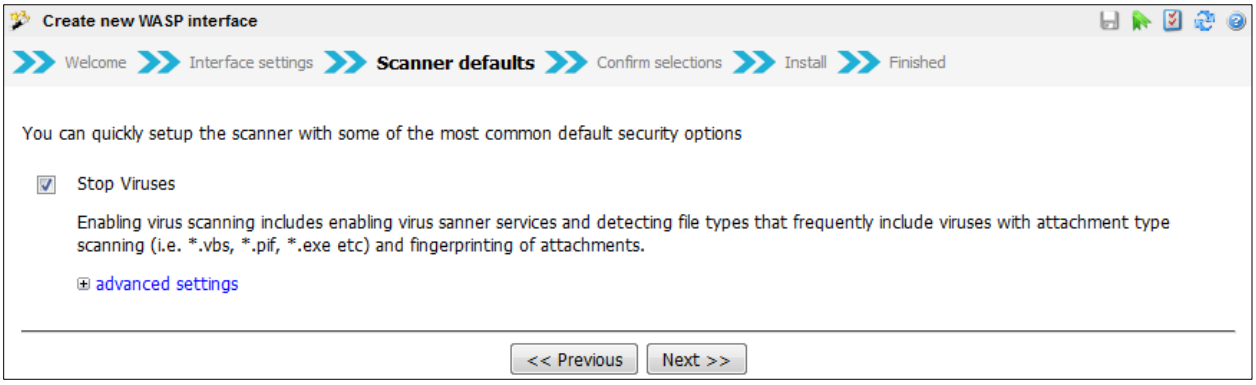
(The WebAccess startup file is the **webacc.cfg** – specify the entire path, including the webacc.cfg filename.)

(The Tomcat directory desired is the one containing the 'webapps' directory from which your WebAccess is run. In a standard SLES 10.x system, the path would be: /usr/share/tomcat5. If you have several instances of Tomcat on the same machine, locate the working webapps directory by searching the webacc.cfg file for the "Templates.path=…" line. It will specify the Tomcat path that WebAccess is using. The correct webapps directory will also contain a gw folder - …/webapps/gw.)

It is important to specify the tomcat instance that WebAccess is running on. There may be several instances of Tomcat installed on the same machine at the same time, depending on the way WebAccess was installed.

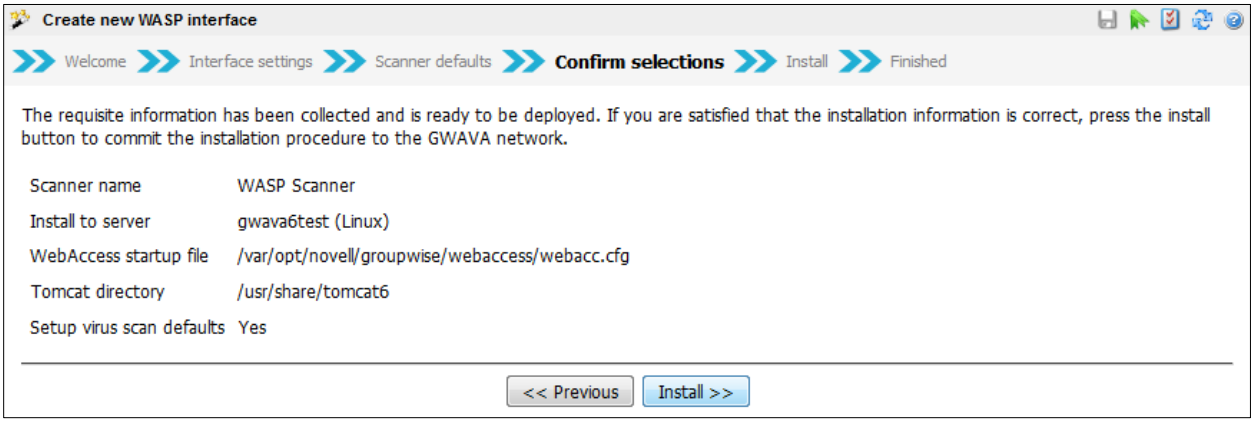


Enter the correct path and name information and click **Next**.

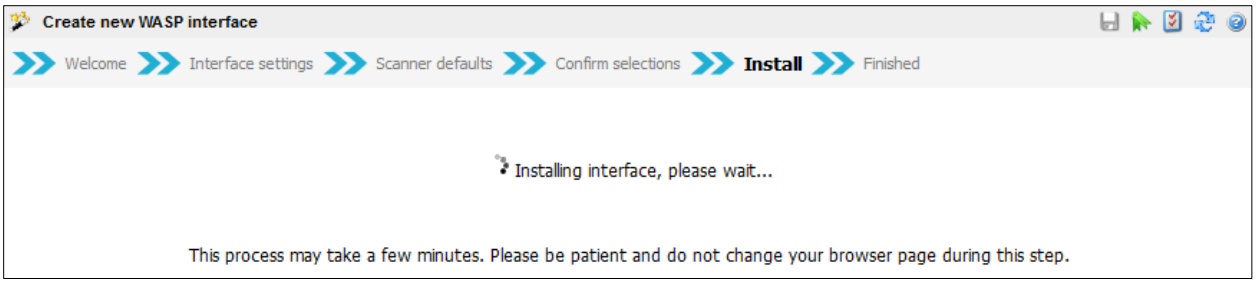


To enable protection from viruses, select “Stop Viruses” to enable the anti-virus engine.

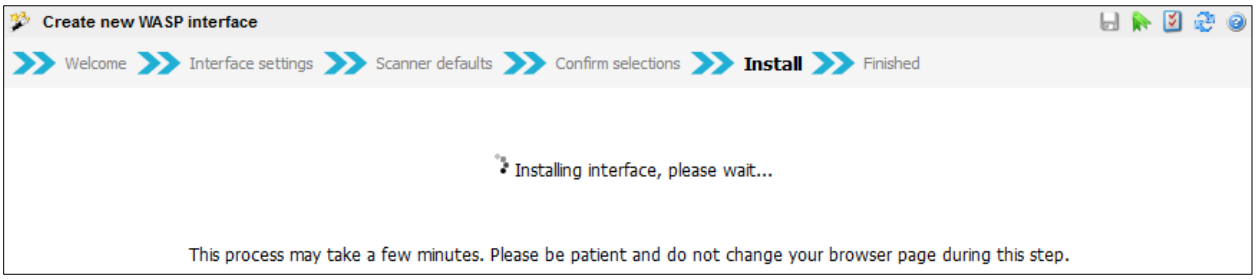
Click **Next**.



Double check all the information for accuracy, then click **Install** if it is correct. Use the previous button if you need to correct any of the information.



Wait until the next page appears. This may take several minutes depending on the speed of the machine and current load. Please be patient.



Once this page appears, your interface has been successfully created and you can browse away from the interface creation interface.

NOTE: Your WASP interface will be dormant until Tomcat is restarted, and a browser calls the Web Access interface. This is required to initiate the WASP servlet for the web server. Restart the Tomcat instance you installed WASP to before testing the interface.

WASP 2 interfaces rebrand the WebAccess login and mailbox screens to alert users that WASP 2 is in use. If you do not want this and wish to return to the original branding and artwork, the files were renamed and reside in the following directories:

For GroupWise 7:

```
<tomcat_path>/webapps/gw/com/novell/webaccess/images/splash.png
```

For GroupWise 8:

```
<tomcat_path>/webapps/gw/webaccess/<build_date>/images/install_watermark_n.png
```

WASP 2 has renamed these to *.bak, (or .bak0 if .bak already exists). Simply rename the file to the original and restart your WebAccess system to return them to default.

WASP Remote Interface

Running WASP 2 in remote mode means that WASP 2 needs to transfer the mime files via the network to GWAVA in order to be scanned. To create a remote WASP 2 interface, you will need the following information:

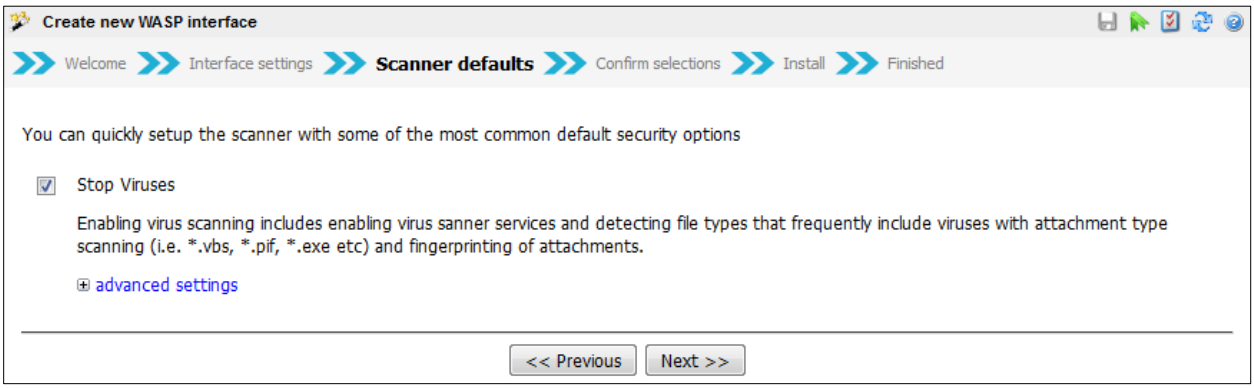
The location of the WebAccess configuration file on remote computer (webacc.cfg)

The location of the Functioning WebAccess Tomcat directory – Or IIS directory (The folder containing the 'webapps' directory. See notes above.)

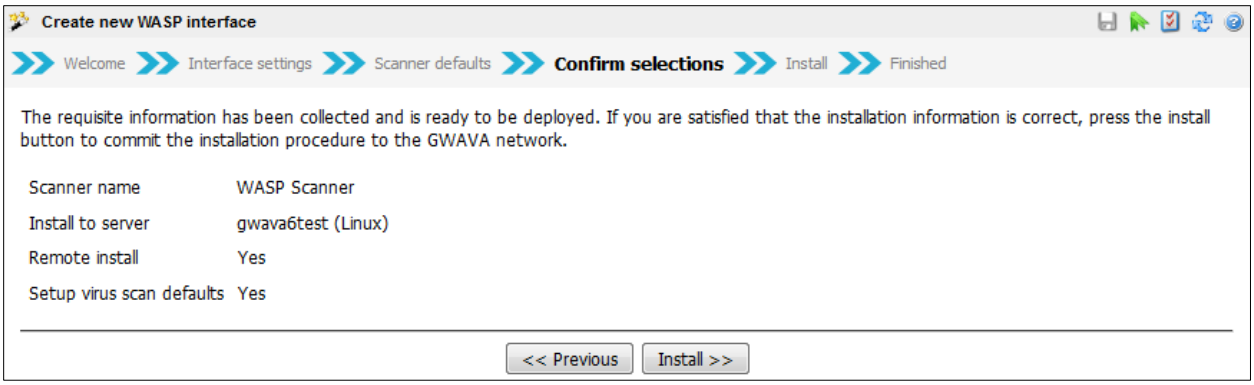
Start the interface creation wizard as above, but select the 'Remote Server Install' option instead of filling in the paths.

This triggers the remote install mode for the interface.

In remote mode, the installer creates a wasp user and password to connect to GWAVA. The Username is created automatically, but you must specify the password. The user and password will only be used by the wasp interface to connect remotely to the GWAVA server and gain access to the interface. Any password will do. Configure as desired.



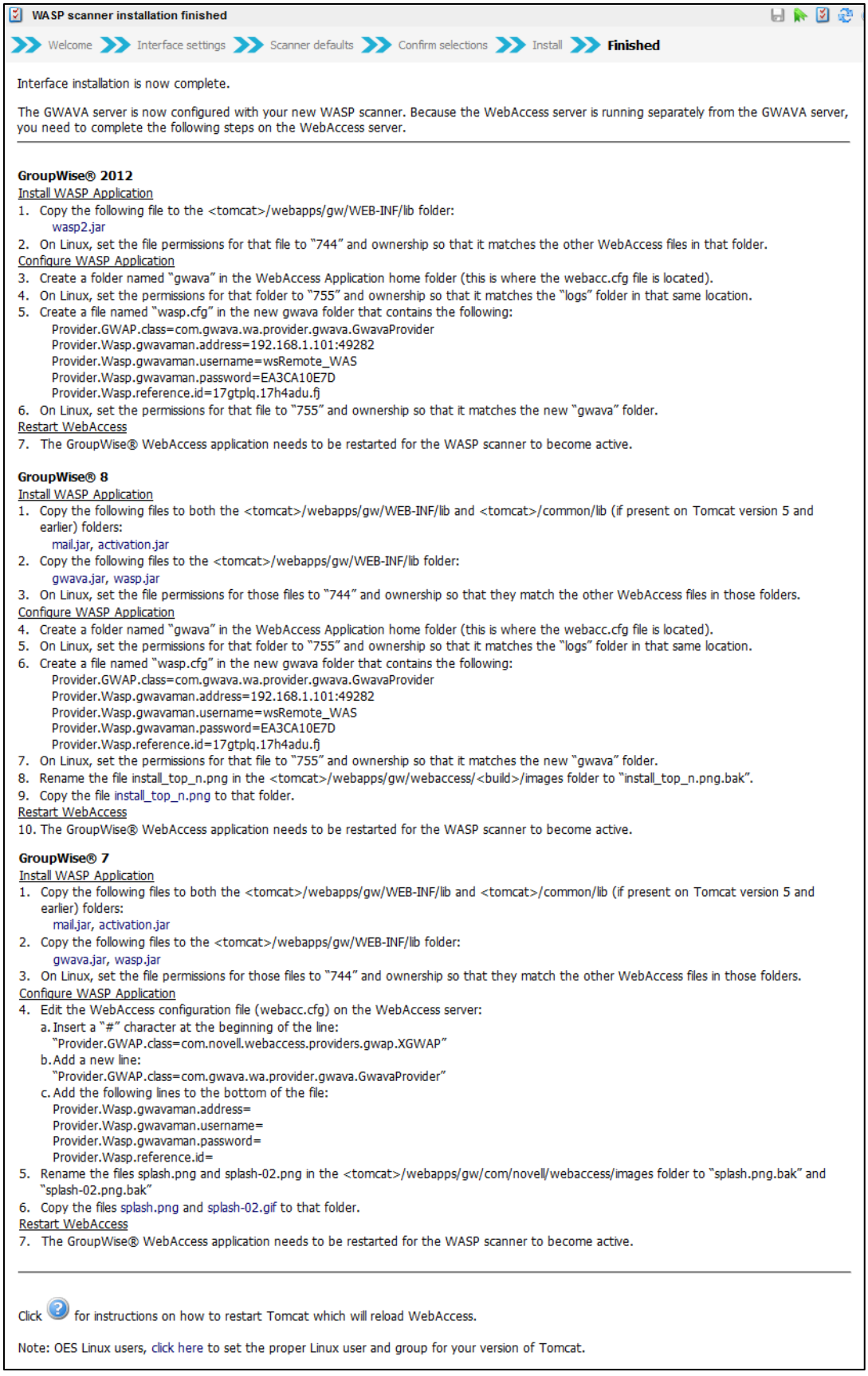
Verify all information, and click ‘install’ when the information is correct. Use the Previous button if you need to change any of the information before you Next.



You MUST wait until this page is shown. WASP 2 requires you to copy some files and edit the webacc.cfg on the remote machine for the installation to be successful. If the .jar files are not copied to the locations specified, or the lines supplied are not added to the webacc.cfg, then the remote install will not be able to connect to the GWAVA server and perform scans. **Make sure you copy the supplied lines before browsing away from this page.**

The following page contains instructions that must be followed; the steps must be completed before WASP 2 will function correctly.

The files that need to be downloaded are linked from this page. Create a backup of the current versions of the files you are copying over. Clicking on the name will download the necessary files you need to copy to the locations defined. You must restart Tomcat after the files have been copied over, and the lines added, before the WASP 2 interface will become active.


WASP scanner installation finished
Welcome
Interface settings
Scanner defaults
Confirm selections
Install
Finished
Interface installation is now complete.
The GWAVA server is now configured with your new WASP scanner. Because the WebAccess server is running separately from the GWAVA server, you need to complete the following steps on the WebAccess server.
GroupWise® 2012
Install WASP Application
1. Copy the following file to the <tomcat>/webapps/gw/WEB-INF/lib folder:
wasp2.jar
2. On Linux, set the file permissions for that file to "744" and ownership so that it matches the other WebAccess files in that folder.
Configure WASP Application
3. Create a folder named "gwava" in the WebAccess Application home folder (this is where the webacc.cfg file is located).
4. On Linux, set the permissions for that folder to "755" and ownership so that it matches the "logs" folder in that same location.
5. Create a file named "wasp.cfg" in the new gwava folder that contains the following:
Provider.GWAP.class=com.gwava.wa.provider.gwava.GwavaProvider
Provider.Wasp.gwavaman.address=192.168.1.101:49282
Provider.Wasp.gwavaman.username=wsRemote_WAS
Provider.Wasp.gwavaman.password=EA3CA10E7D
Provider.Wasp.reference.id=17gtplq.17h4adu.fj
6. On Linux, set the permissions for that file to "755" and ownership so that it matches the new "gwava" folder.
Restart WebAccess
7. The GroupWise® WebAccess application needs to be restarted for the WASP scanner to become active.
GroupWise® 8
Install WASP Application
1. Copy the following files to both the <tomcat>/webapps/gw/WEB-INF/lib and <tomcat>/common/lib (if present on Tomcat version 5 and earlier) folders:
mail.jar, activation.jar
2. Copy the following files to the <tomcat>/webapps/gw/WEB-INF/lib folder:
gwava.jar, wasp.jar
3. On Linux, set the file permissions for those files to "744" and ownership so that they match the other WebAccess files in those folders.
Configure WASP Application
4. Create a folder named "gwava" in the WebAccess Application home folder (this is where the webacc.cfg file is located).
5. On Linux, set the permissions for that folder to "755" and ownership so that it matches the "logs" folder in that same location.
6. Create a file named "wasp.cfg" in the new gwava folder that contains the following:
Provider.GWAP.class=com.gwava.wa.provider.gwava.GwavaProvider
Provider.Wasp.gwavaman.address=192.168.1.101:49282
Provider.Wasp.gwavaman.username=wsRemote_WAS
Provider.Wasp.gwavaman.password=EA3CA10E7D
Provider.Wasp.reference.id=17gtplq.17h4adu.fj
7. On Linux, set the permissions for that file to "755" and ownership so that it matches the new "gwava" folder.
8. Rename the file install_top_n.png in the <tomcat>/webapps/gw/webaccess/<build>/images folder to "install_top_n.png.bak".
9. Copy the file install_top_n.png to that folder.
Restart WebAccess
10. The GroupWise® WebAccess application needs to be restarted for the WASP scanner to become active.
GroupWise® 7
Install WASP Application
1. Copy the following files to both the <tomcat>/webapps/gw/WEB-INF/lib and <tomcat>/common/lib (if present on Tomcat version 5 and earlier) folders:
mail.jar, activation.jar
2. Copy the following files to the <tomcat>/webapps/gw/WEB-INF/lib folder:
gwava.jar, wasp.jar
3. On Linux, set the file permissions for those files to "744" and ownership so that they match the other WebAccess files in those folders.
Configure WASP Application
4. Edit the WebAccess configuration file (webacc.cfg) on the WebAccess server:
a. Insert a "#" character at the beginning of the line:
"Provider.GWAP.class=com.novell.webaccess.providers.gwap.XGWAP"
b. Add a new line:
"Provider.GWAP.class=com.gwava.wa.provider.gwava.GwavaProvider"
c. Add the following lines to the bottom of the file:
Provider.Wasp.gwavaman.address=
Provider.Wasp.gwavaman.username=
Provider.Wasp.gwavaman.password=
Provider.Wasp.reference.id=
5. Rename the files splash.png and splash-02.png in the <tomcat>/webapps/gw/com/novell/webaccess/images folder to "splash.png.bak" and "splash-02.png.bak"
6. Copy the files splash.png and splash-02.gif to that folder.
Restart WebAccess
7. The GroupWise® WebAccess application needs to be restarted for the WASP scanner to become active.
Click for instructions on how to restart Tomcat which will reload WebAccess.
Note: OES Linux users, click here to set the proper Linux user and group for your version of Tomcat.

General Administration

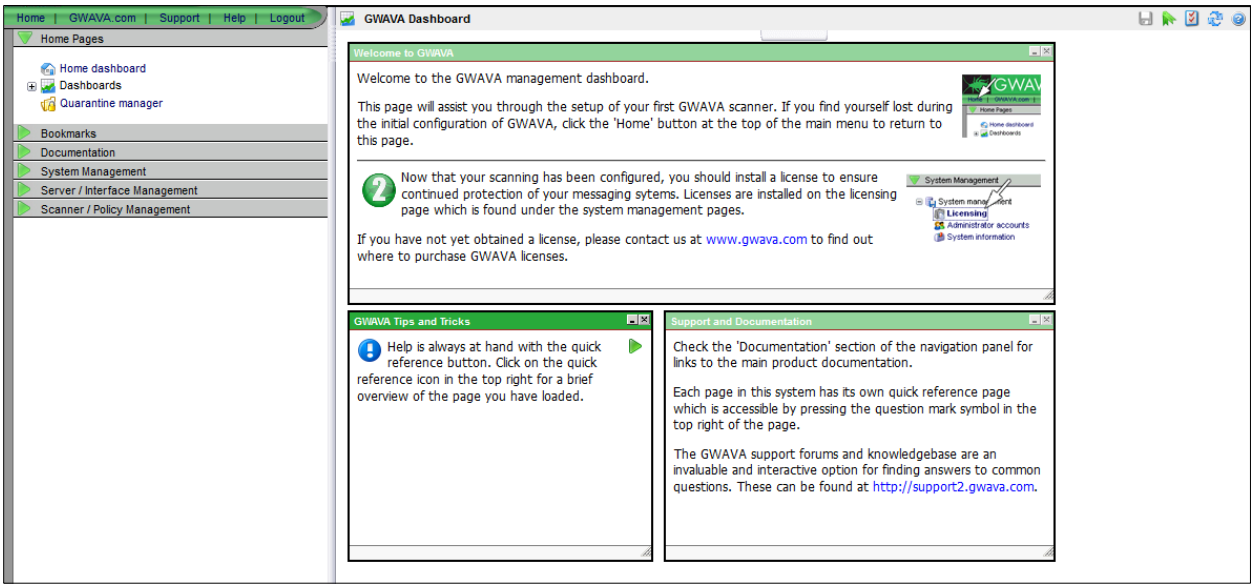
GWAVA administration is completed between two interfaces: the management console, and the QMS management console. The management console runs all administration of the main GWAVA system and interfaces: interface creation, configuration, updates, server settings and management user accounts. The QMS management console contains the administration over the quarantine system: digests, user accounts and login rights, release rights, and Quarantine database size.

GWAVA Management Console

When you log into the GWAVA Management console, you will view the default user Dashboard. This page displays default gadgets and basic info for your GWAVA system.

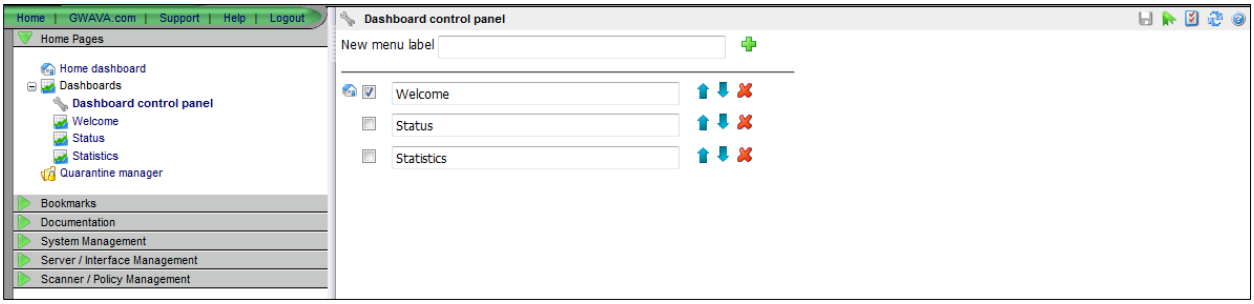
The System Status window shows the blocking statistics for your server as well as your evaluation deadline, if you have not licensed your GWAVA system. The statistics window has the option to change the statistics to represent the total, day, last hour, or current hour statistics for each of the shown statistics.

Dashboards



GWAVA has a user-defined area which opens by default, which can be filled with ‘gadgets’. Though there are three default dashboards already defined, the dashboard area was created with the expectation that each system administrator will create and configure their own personal dashboard.

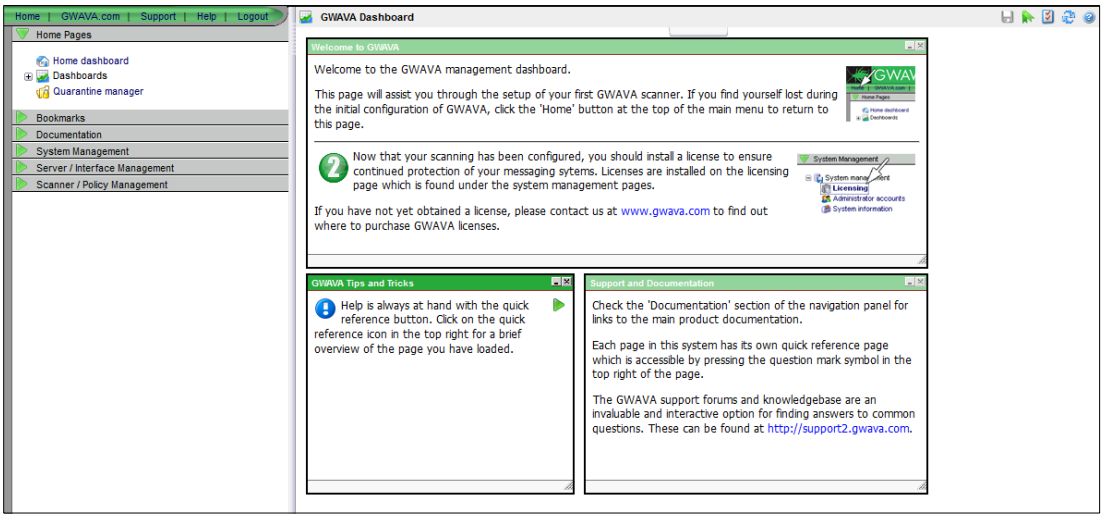
Dashboard Control Panel



The Dashboard control panel allows for the management of multiple dashboards, and the creation of new dashboards. The dashboard is the default page displayed when users' login to the GWAVA Management console. The default dashboard for the homepage is indicated by check mark and little house next to the dashboard name. To change the default dashboard, select the desired dashboard by placing the checkmark in the box next to your choice, and save the changes.

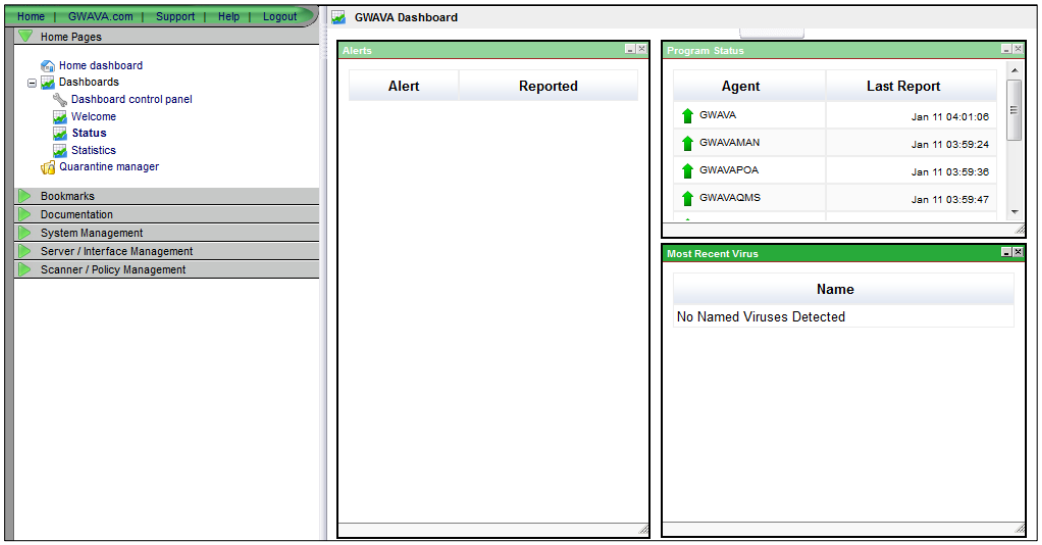
Multiple dashboards may be created or deleted. The current dashboards may be removed, renamed, or reconfigured. The dashboard control panel allows for the creation of new dashboards, renaming or removal of old dashboards, and the selection of the default dashboards.

Welcome



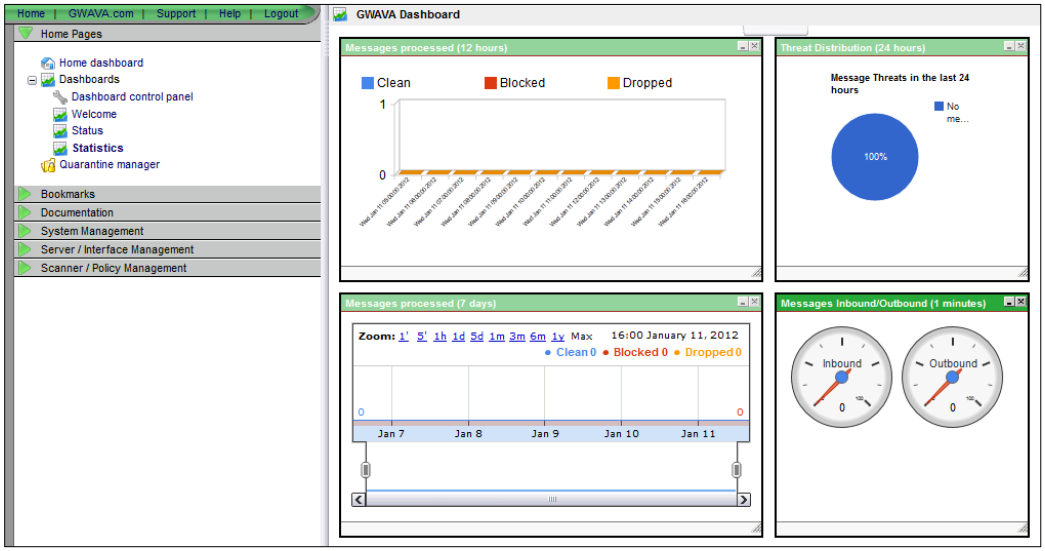
The Welcome dashboard is the default dashboard for upgrades and new installations of GWAVA, and will be the page seen on first login. The Welcome dashboard has gadgets showing tips, tricks, new information, and links to documentation. The welcome dashboard is not meant to be a permanent default page, but will remain default until changed. As with all dashboards, the welcome dashboard may be configured at any time.

Status



The status dashboard displays the general status of the GWAVA system; modules reporting working status with the date and time last reported are listed, as well as any alerts and detected viruses. Known viruses will be named, while unspecified or unnamed viruses will remain unnamed. All virus hits are reported.

Statistics



The statistics dashboard contains basic statistics for the entire system with all interface stats available to be monitored. The statistics vary from total messages processed in the system and breakdowns of different blocked messages to the number of operational threads and system loads according to time of day.

Configuring and customizing Dashboards

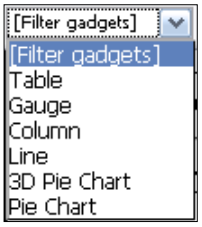
Dashboard pages are essentially blank pages which can be filled with configurable modules called 'gadgets'. Gadgets are gauges, charts, and graphs tied to different statistics and information in the GWAVA system. Different gadgets display information such as statistics on message flow, system load, detected viruses, blocked connections, RBL hits, and user traffic.

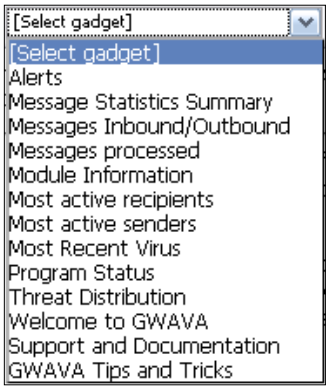
Configuration of any new or existing dashboard is accomplished by adding and removing gadgets to the desired dashboard and configuring the gadget to the desired specifics. Each gadget, after being added to a page, may be moved to any desired location on the dashboard, and the size of the gadget and, or the containing frame.

To add or configure a gadget, open the desired GWAVA dashboard, or create a new dashboard page and select the dropdown tab from the top of the dashboard window to show the gadget selection interface. Clicking on the tab again will either show or hide the gadget selection menu.

Select the desired gadget type and gadget from the dropdown menus and select the add button. The different gadgets may be selected by gadget type, and then desired statistic, or from the desired statistic first, followed by the desired gadget type. Not every gadget type is available for each statistic, as some statistics would not function well in a gauge, graph, or chart form, and is best represented in the forms available.

The currently available gadget types and statistics include the ones shown.





After selecting the gadget desired, some gadgets offer more configuration options, such as time frame, scope of a chart, or the top limit of a gauge. If a gauge offers further configuration, configure the gauges to achieve the desired information needs and select the green plus sign to add the gadget to the dashboard.

Moving gadgets is simple; click and drag the desired gadget to the desired location and orientation in the dashboard window by selecting the top of the containing frame. Different frames may also be sized as desired by selecting the bottom right corner of the desired frame. The mouse pointer will be changed from the system default arrow to a 'move' or a 'resize' arrow. Place and configure the gadgets as desired to create a customized dashboard.

After modifying, moving, adding, removing, or resizing any module, the 'Save Changes' icon must be clicked, or the settings will not be saved. As GWAVA is updated, further gadgets may be added to the GWAVA system.

Quarantine manager

The Quarantine Manager link opens the Quarantine Manager in a separate browser window or tab. The Quarantine Manager can also be accessed from any browser through the following URL:

`http://<GWAVA_server_address>:49285`
The Quarantine Manager is covered later on in this document. Please see the Quarantine Manager section.

Bookmarks

The Manage quick access pages link allows the administrator to provide quick access to any page with the bookmark icon in the top right-hand corner. This may shorten browsing times to often visited pages deep in the folder structure of an interface, such as interface statistics or exceptions.

Documentation

Online documentation is linked from the documentation menu, as is the quick install guide, which will not only guide you through basic installation instructions, but will also help in the immediate basic setup for interfaces and management.

System Management

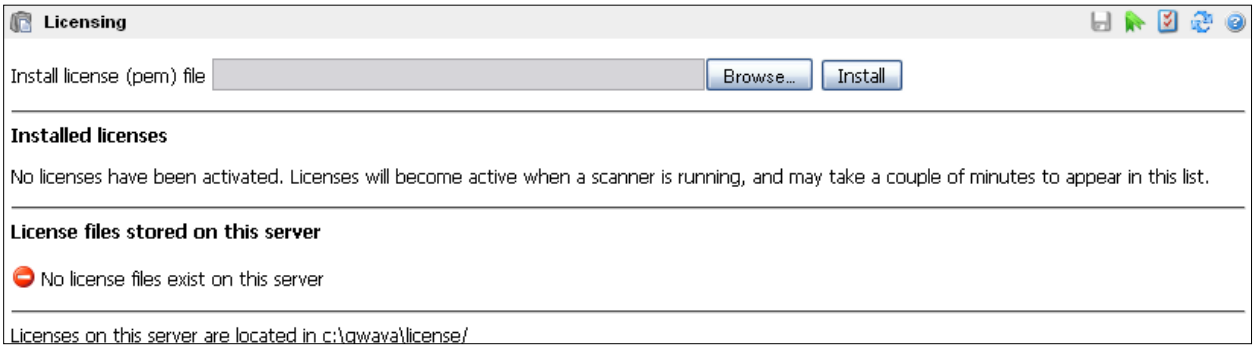
Under the System management link, default settings for the system are listed. The settings here are the base used when creating interfaces. Each interface's settings may be modified individually after interface creation, but by changing the default settings here each interface will be created with the basic default settings correctly.

System Management contains two sections: System management and Advanced. Most work will be completed through the System management section, while the Advanced section contains tools which should be generally left alone unless specified by support.

System Management

Licensing

GWAVA must be licensed to use for longer than 30 days and WASP 2 requires a similar license. These licenses may be obtained by contacting the sales representative for your area. Please visit http://www.gwava.com/company/contact-us.html to contact your sales representative.



If no licenses are present, the window will state that no licenses have been found. To install a license, select the 'Browse' button and locate the unzipped license file (.pem). After the license file has been located and selected, click the 'Install' button and the license file will be uploaded to the GWAVA server. GWAVA will look for, and recognize the license file in a few minutes. If impatient, restarting GWAVA will trigger the system to look for the license file on startup. Keep an archive copy of the license file for disaster recovery. The license storage location on the GWAVA server is listed at the bottom of the screen.

Admin accounts

Admin accounts allow you to add and remove administrator accounts from the GWAVA system. These accounts will have full administrator rights to GWAVA Management, as well as default full administrator rights to the Quarantine system.

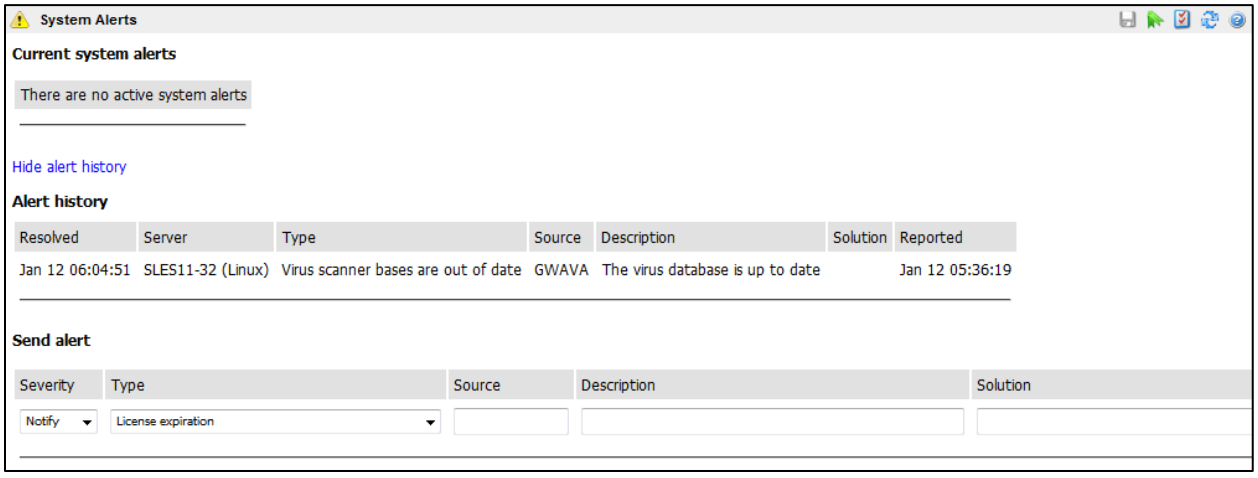
You may enable or disable four state checkboxes preference from this interface. Four state checkboxes may also be enabled or disabled from any configuration window where the preferences icon is displayed in the top right-hand corner.

System Information

System information displays exactly that. The Server name, ID, operating system, activation date, address and general status are shown. The status of each of the different running pieces of GWAVA are listed here, along with their latest report-in date, time, and location. This page provides basic information on the system at a glance.

System Alerts

The System Alerts page displays all the system alerts active, as well as alert history. An Administrator can issue an alert to the system if desired, by selecting the alert and type, then selecting the Send button. Descriptions, severity, source, and solutions may be added to any alert generated from this window.

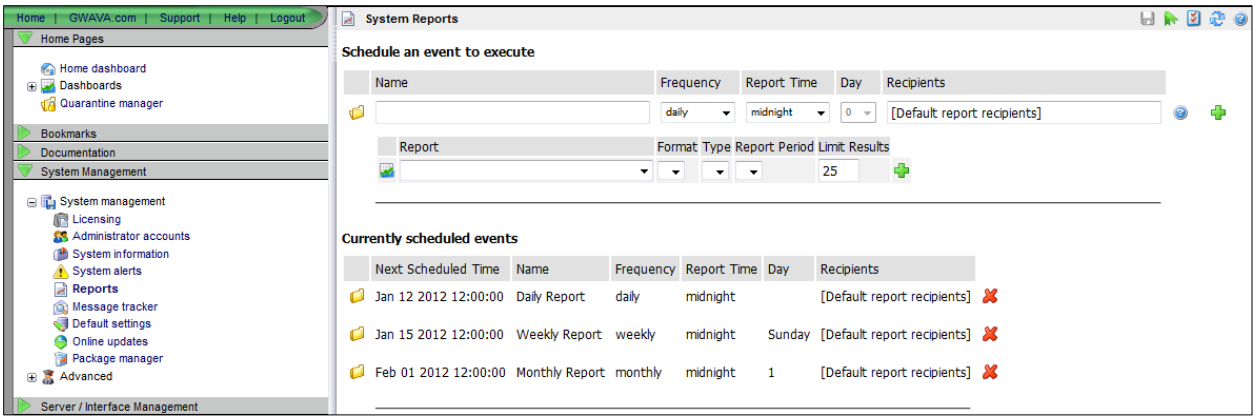


Reports

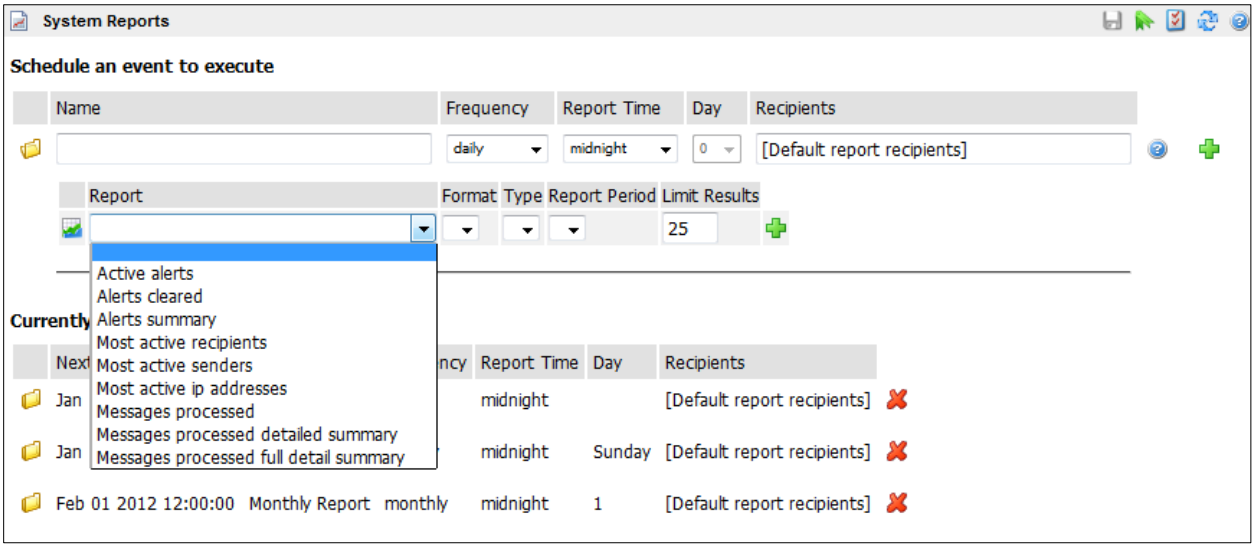
The Reports function allows the Administrator to setup, send out, or receive regular system reports on the functions and different status of the system. Reports include statistics on:

- Active alerts
- Alerts cleared
- Alerts summary
- Most active recipients
- Most active senders
- Messages processed
- Messages process with a detailed summary
- Most active IP addresses

There are different types of reports based on time frame: daily, weekly, and monthly. Reports are sent to the specified recipients in the list.



To create and send out a report, specify the name, frequency, and time for the report, and then add the report modules desired to be included in the report.



Add as many or as few report modules to any desired report, but a report should have at least one module to be of worth. Result lists may be limited to a manageable size, and the default is set to 25 items.

Daily Report — **Jan 10 2012 12:00:00**

The reports below were generated and e-mailed to you by a GWAVA scheduled event. If you do not want to receive these reports please reply to this email and the administrator can remove you from the recipient list.

Detailed summary of messages processed between 01/09/12 00:00:00 and 01/10/12 00:00:00

Total Connections	Inbound	Outbound	Dropped Connections	Client Conversations Terminated	Messages Scanned	Blocked	Quarantined	Recipient Exception	Spam	RBL	SURBL	SPF	IP Reputation	Source Address
7340	4	0	0	0	7340	2108	1916	0	0	0	0	0	0	80

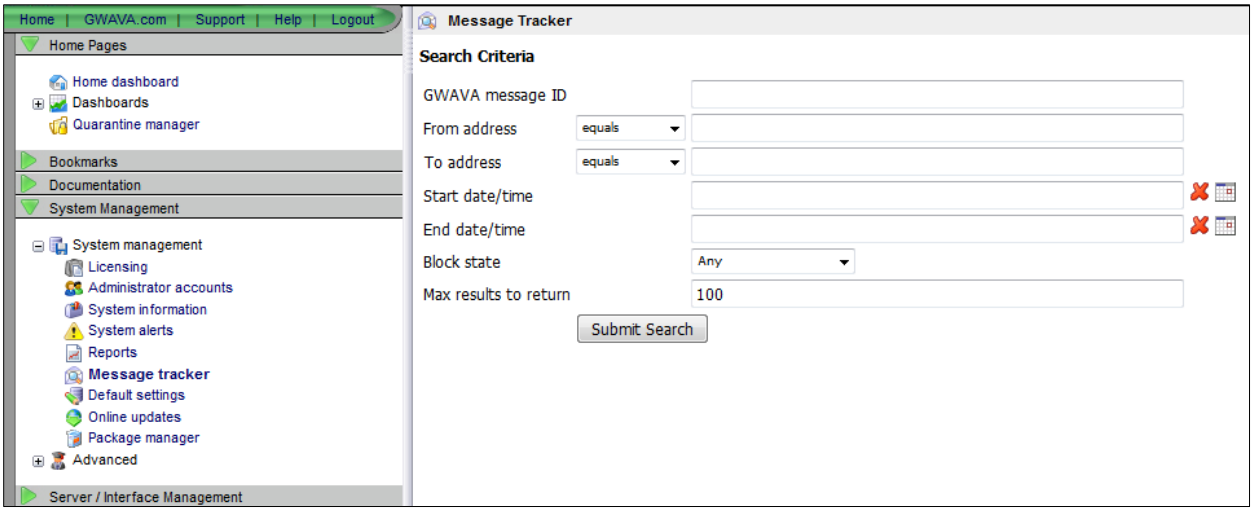
Most active senders between 01/09/12 00:00:00 and 01/10/12 00:00:00

Email Address	Count
ithaqua@mythos.com	630
computingresources_support@hotmail.com	626
photographyschool@hizingawrld.net	282
cthulhu@mythos.com	259
e-rios1985@hotmail.com	189
castrojesse7657@hotmail.com	180
amy.richardsonspm@hotmail.com	179

Reports may vary on exactly what is specified to be included and how many items are displayed. The Reports are subject to change and may end up being quite long, yet may be incredibly detailed and helpful in monitoring and managing the mail system.

Message tracking

GWAVA contains the ability to track all messages which pass through the system, report when they passed and what action was performed on the specified message, and for what reason the action was taken. To access the Message tracker, select 'Message tracker' from the System Management window.



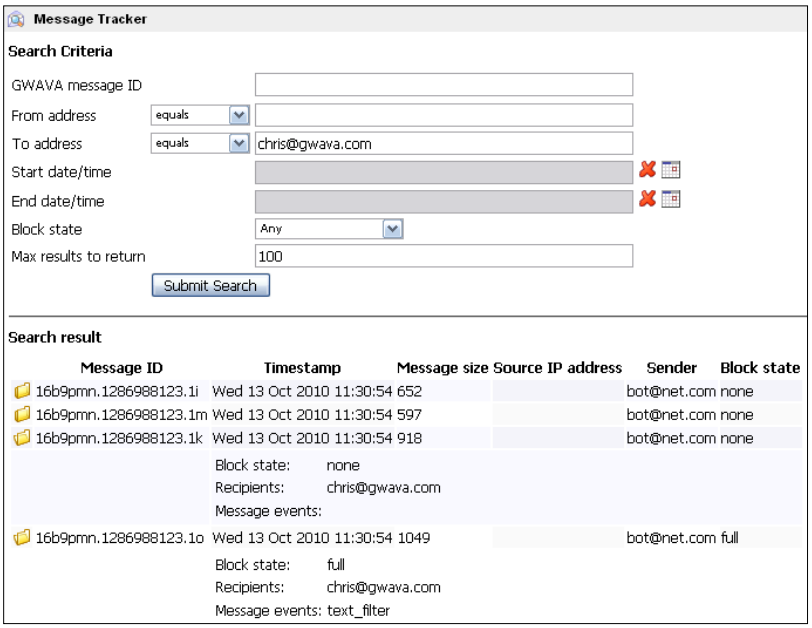
To track the path of a message through the system, specific information must be known about the message. GWAVA will search through the records to find a message which fits the criteria provided. The tighter the criteria provided, the smaller the results list will be.

Search terms can include:

- GWAVA Message ID
- From and To address
- Timeframe window
- Block state

The GWAVA Message ID is most useful to re-track a message that has been located beforehand, as the message ID's are unique, the result will be the specific message desired. The rest of the criteria is useful to find a message from a specific sender, to a specific user, during a specified timeframe. Setting the Block state search option limits the resulting pool of messages to only those which have either been passed through, or which have been blocked by GWAVA. A search may be performed on one criteria.

Messages that show up in the search may be expanded by clicking on the corresponding folder to display the pertinent information: all recipients, the block status, and a responsible interface event causing the block.



The full message text is not available in the tracking window. Blocked messages are available to the owner or administrator via QMS. Messages which have not been blocked have been passed to the resident mail system for normal processing.

Default settings

This page displays and allows editing of the default settings used when adding a new server to the GWAVA network. The settings listed here are used to fill out the Configure Server page, which the interfaces read from. It is vitally important that the information supplied for this page is correct for the mail system.

The Administrator email address and name supplied here will appear on all mail notifications and digests sent by the GWAVA system. Any responses to these mail items will be sent to the Administrators address. The Mail relay agent SMTP Server and the QMS SMTP Authentication server are the connection addresses used by GWAVA when sending notifications, digests, and authenticating users for access to their mail in the quarantine system.

Online updates

When a notification that updates are available for the GWAVA system shows on the GWAVA management homepage, this page is where the update is performed. Different update servers may be selected as the source for updated code. The ‘beta’ server contains unproven code and should not be used on a production system, unless specified by support. The default download servers should be sufficient for most systems.

If the system requires a proxy to access the internet on port 80, then the proxy settings must be provided under the 'Proxy Server Configuration' section under Server/Interface Management |<server name> | Server management | Configure server. There is a link on the update page leading directly to the appropriate page. (The Proxy Server Configuration settings may need to be 'shown' before they are accessible.)

To initiate an update, select the desired update server, and select 'Submit Update Request'. Once an update request has been initiated, GWAVA will contact the update server and begin the download and update process.

Package manager

The Package manager allows the addition of third party and additional plugins to be added and installed to the GWAVA mail system.

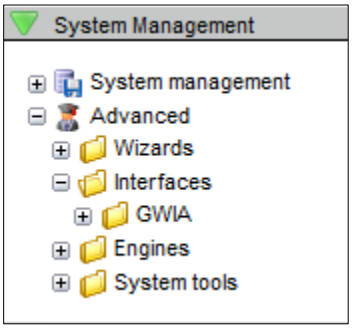
To use the Package manager, browse to and select the desired package by using the 'browse' button, then click 'upload' to load the plugin to the GWAVA system. The uploaded package is usually zipped, and the GWAVA system can unzip and install the package.

To unzip, install, or uninstall any third-party plugin package use the associated icon under the 'Actions' column. The 'Actions' column will only display the available actions which will identify themselves on mouse-over.

After a package has been unzipped and installed, the GWAVA system may require a restart to initialize the package. See the documentation included with the additional package for details.

Advanced

The settings in the advanced section of the menu contain categorically organized items for your system. This menu provides scanning configuration identical to the scanning configuration under **Server/Interface Management**, but differs in that the advanced configuration items are organized by each individual component.



It is recommended to use the Server/Interface Management menu for configuration. The advanced section should only be used by support or under the instruction of support. Items listed under 'Advanced' which are listed under the Server/Interface Management section are explained where they

reside under the **Interface management** section. The menu items which are separate from the interface tree are found under **System tools**.

System Tools

System Tools contains powerful tools which modify the core system of a GWAVA server. These tools are not to be used on a regular basis, and should not be used unless instructed to do so by GWAVA support. Editing the database, removing objects and modifying Servers in the GWAVA network may render the GWAVA system inoperative. Only proceed with such operations if you fully understand the process and possible repercussions and on instructions by GWAVA support. The System Tools section will be added to as necessity requires, and new menu items will be self-documented within the system.

Network, Server & DB Tools

Replication manager

The replication manager is a tool to push settings found in the current GWAVA system to other servers in a GWAVA network. The connection between two GWAVA servers is created during server activation. Instead of setting up the GWAVA server as a 'new server', select the new server to become part of an existing GWAVA network. If chosen to do so, the manager will assist in replicating the existing configuration database and settings across multiple servers.

Database Editor

The database editor allows both the viewing and the editing of the GWAVA configuration database. This can be used in coordination with GWAVA support. Do not use the database editor without explicit instruction and aid from GWAVA support.

The editor prompts you to spawn a new window and then offers the option to open the selected table in either viewing only, (default setting), or in the editing mode, which allows changes to be committed to the database. The editor also includes a search function which passes queries to the database and allows the response to be limited to a desired level of results. Changes to the database in the editor are immediate. To exit the editor, simply close the window.

Server Maintenance

Standard core functions for GWAVA maintenance are listed here. Removing and renaming a GWAVA server from the GWAVA networks correctly severs or renames a connection between two GWAVA servers. Removing a connected server from a network should be done prior to uninstalling the GWAVA server in order to avoid connection issues with the remaining GWAVA server(s).

Due to updates and changes in the GWAVA interface, it may be necessary to rebuild the system Menu's. Selecting this option causes the GWAVA system to discard the current menu tree and system in the GWAVA interface, and recreated them from the current system files. If a new item has been installed or downloaded to the GWAVA system during an update and a menu rebuild is appropriate, you will be notified on the default GWAVA home page, under the system status window. The notice will be a link

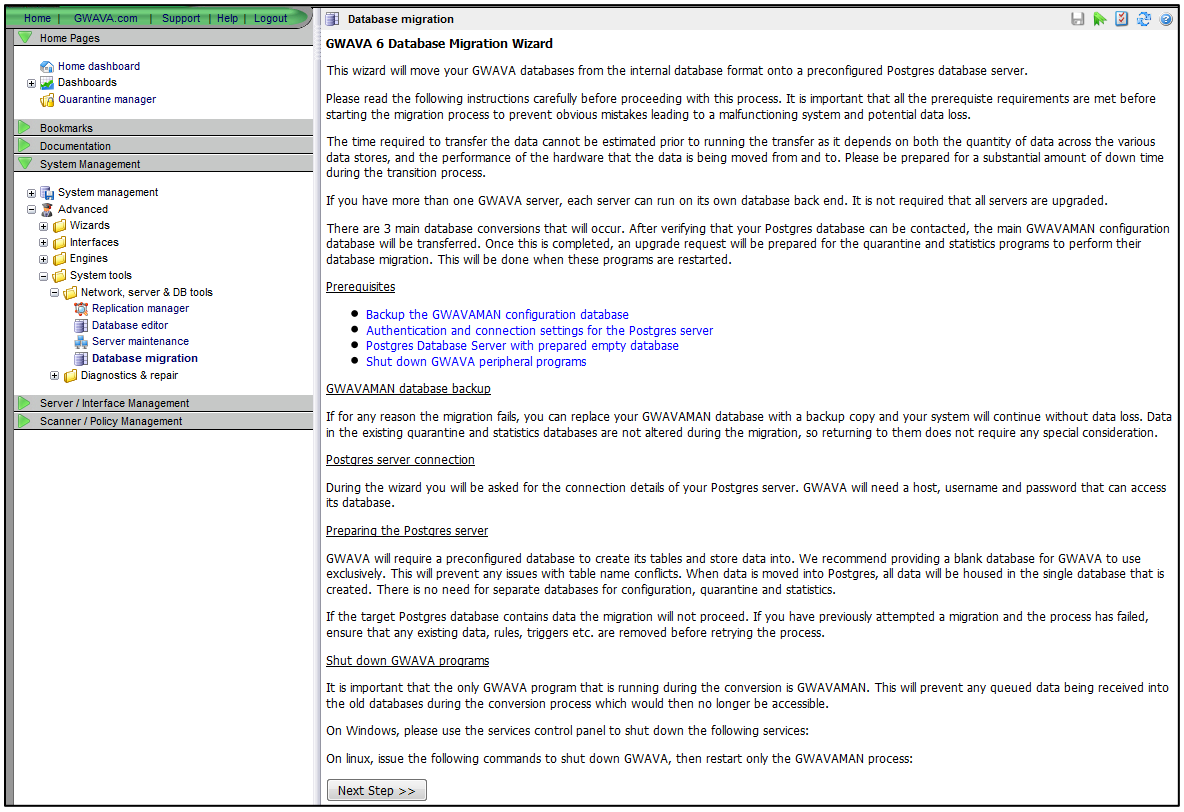
which initiates a menu rebuild. Utilization of this option under the system tools should not be necessary under normal operation.

Database Migration

The Database Migration tool migrates the internal SQLite database to an external Postgres database. Migration is a relatively simple process which is automated by GWAVA, however, database migration may take some time, and may take quite a long time depending on the size of the internal database. During database migration GWAVA services and scanning will be unavailable.

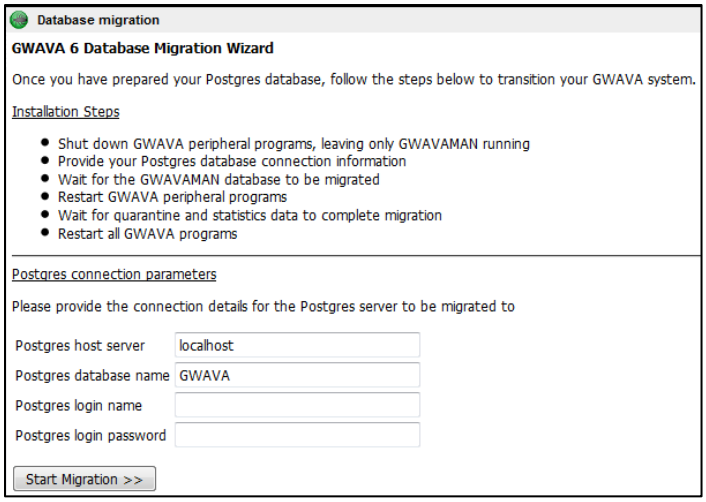
All maintenance, installation, tuning, and administration of the Postgres system is the responsibility of the system administrator. GWAVA offers no technical support for third party programs.

The Database Migration itself has detailed instructions in place. Read all of them before proceeding with the database migration. The migration process consists of several steps and pre-requisites which must be completed before continuing. Once all steps are completed, the migration can continue.



Shutting down all peripheral programs to gwava, except the 'gwavaman' process will leave the administration interface functional and accessible for the migration process. **It is critical that all peripheral GWAVA processes be shut down before the migration is started.**

The migration itself may take quite some time depending on the size of the SQLite database, and during this time GWAVA will not scan mail and messages will not be passed through the system.



Enter the connection information to a pre-created, blank, Postgres database, and select the 'Start Migration' button to begin the migration. Once the migration has been completed, the peripheral GWAVA processes need to be started to initiate the quarantine and statistics data migrations. Once those have completed, the entire GWAVA system needs to be restarted in order to complete the migration. Once restarted, GWAVA will be functioning from the Postgres database.

Diagnostics & Repair

The diagnostics section of the GWAVA management interface is designed for troubleshooting use and works in conjunction with the base components of the system. These tools should not be played with or used without full understanding of the effects. Use of these tools without the guidance of support may cause serious issues with the GWAVA system and network.

Server/Interface Management

The Server/Interface Management is setup in a directory tree-view organized around tasks. The Server management offers active setup information on the GWAVA server. The Wizards menu contains all interface creation options. The Manage interfaces menu contains all currently active and created interfaces and their configuration options.

Server management

This menu contains all of the active settings in the GWAVA system for the GWAVA server. Editing and saving changes in this section changes the active settings in the GWAVA server within a couple of minutes.

Server status

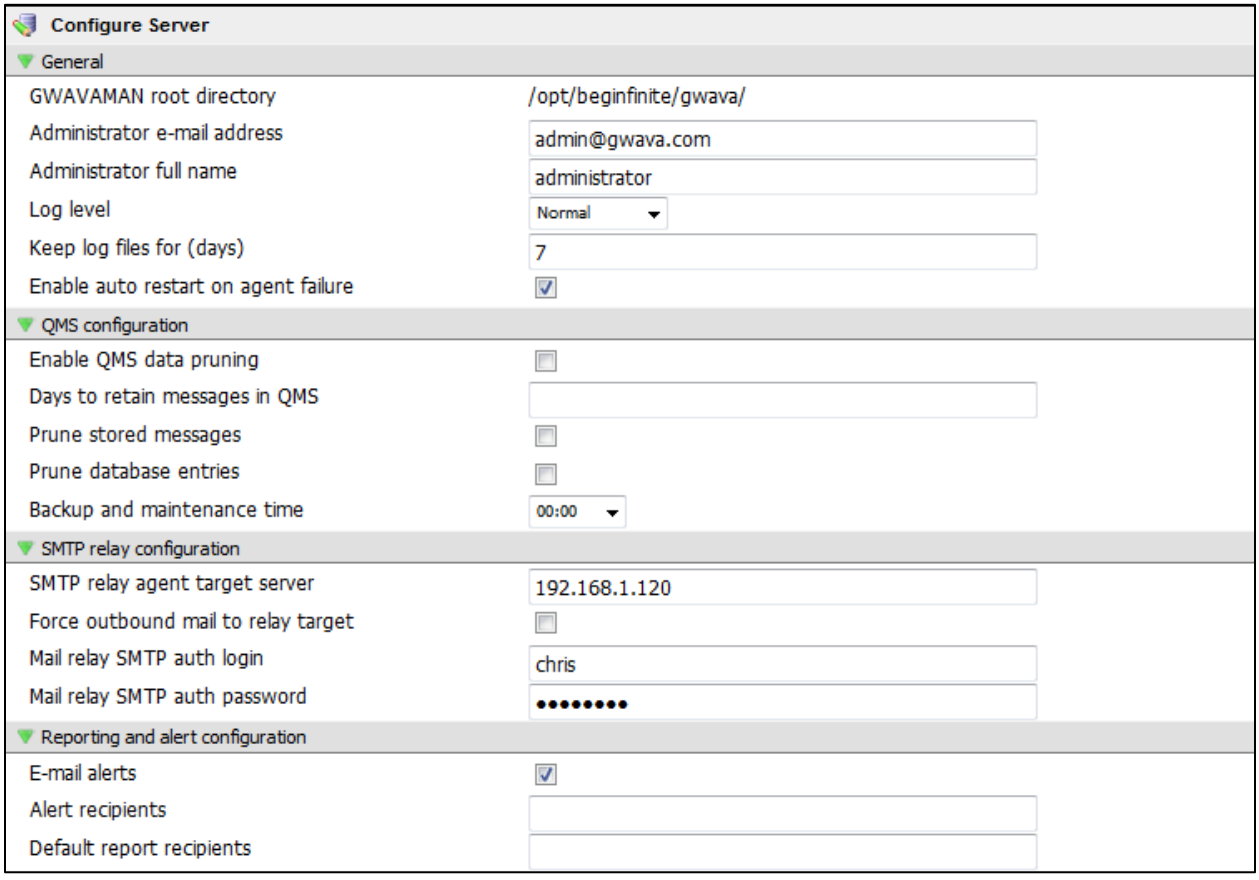
The Server status page displays the basic status and rundown of the server and the platform it detects as the running system. The server name, up time, server time, database ID, object, and record count, thread count, and replicator status and queue are listed.

Configure Server

In the Configure server window, all of the connection settings for the server are listed as well as the log level, statistics, and reporting settings. The administrator address and name configured on this page will be used for alerts.

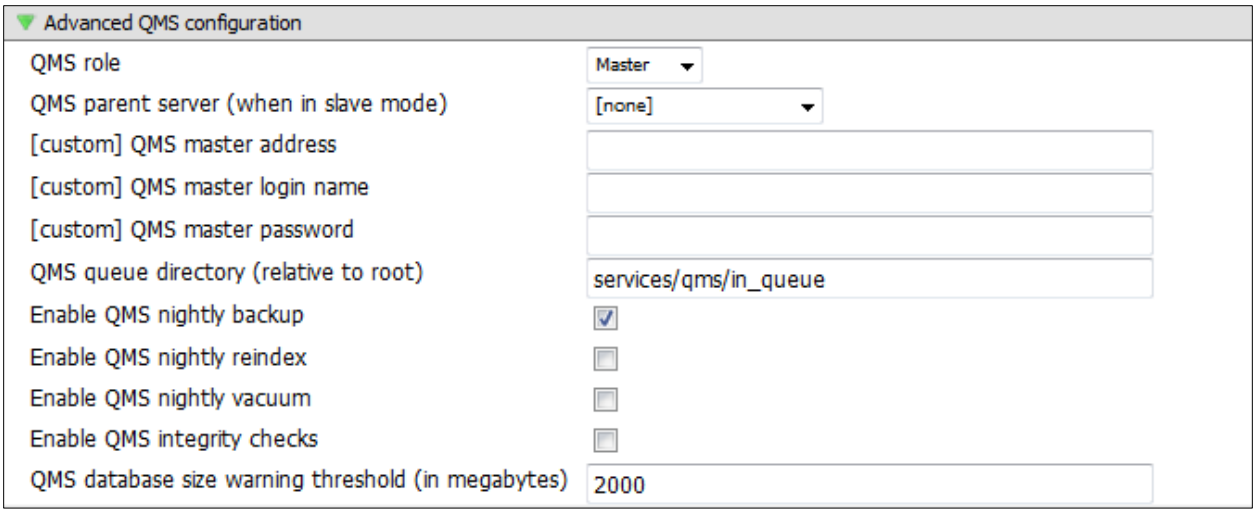
The Admin name and address is the default source address for digests and notification messages sent by GWAVA to users in the system. If replied to, the messages will return to the address listed here.

The QMS authentication server should be the connection to the GWIA for GroupWise systems, in order to allow user-level access to the quarantine manager for each user's respective quarantined mail.



If your GWIA requires a special greeting, or authentication type, or you use an external SMTP server which requires special authentication or login information, this is where GWAVA is informed of the connection. For most systems, the only configuration performed on this page is the "Maximum SMTP send threads" variable. This determines the maximum amount of threads which GWAVA will use to send notification or digest messages to the GWIA or receiving SMTP gateway in the mail system. This should

be less than the total number of receive threads open on the GWIA or the SMTP agent, to ensure that the mail system is not overwhelmed when digests are sent.

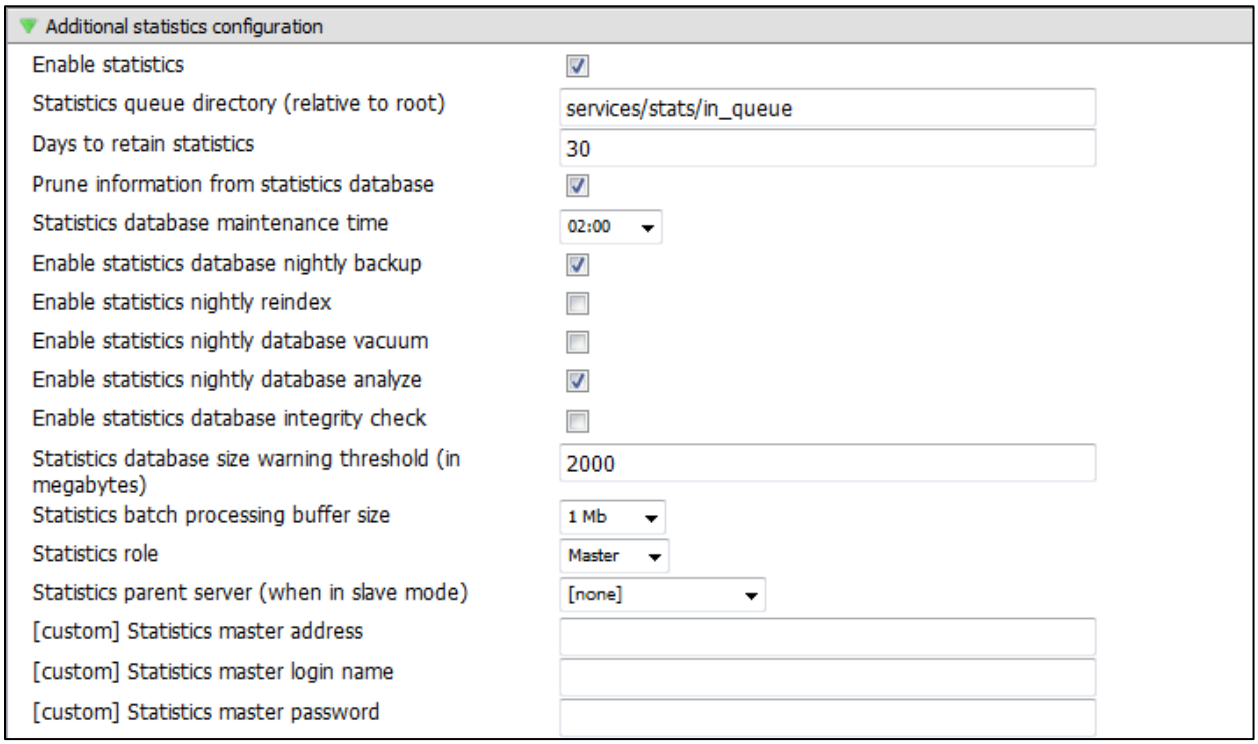


The Advanced QMS Settings allow the function of newer QMS tools to help clean and maintain the QMS database. The nightly backup and integrity checks do exactly as they say. The database vacuum and reindex services clean out bad links and files, and reindex the files in the database for faster searching. The database vacuum and reindex services normally do not need to be used, and should only be triggered under the direction of support.

The QMS role is an option to allow all QMS data to be stored in a central location when utilizing multiple GWAVA servers in a system. The 'Master' role sets QMS to have all quarantine data copied to that server from 'Slave' QMS servers. Slave QMS servers will contact the Master QMS and copy all quarantined data and messages to the master, storing all quarantined messages in a central location. This should not be changed unless multiple GWAVA servers exist in the system.

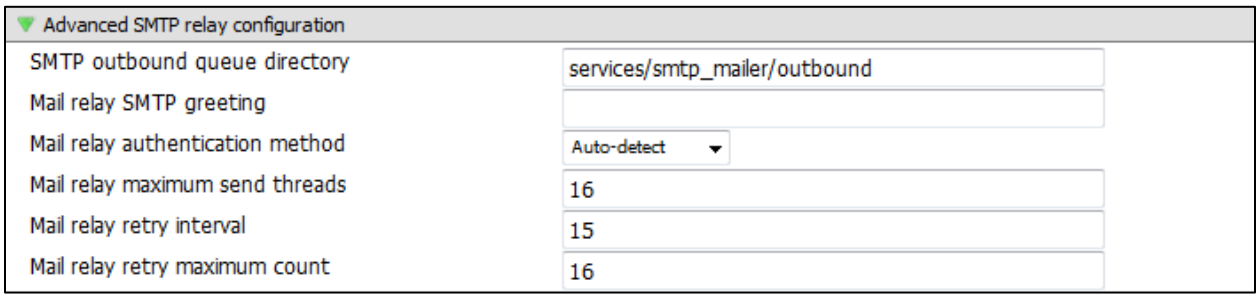
Advanced Statistics settings

Settings enabling the collection and governing the statistics engine in GWAVA are set here. Defaults are shown. If records of statistics are to be kept, backup of, as well as retention time of statistics should be set as desired. Be careful not to retain stats for a long period, as busy systems can quickly amass very large statistics databases.



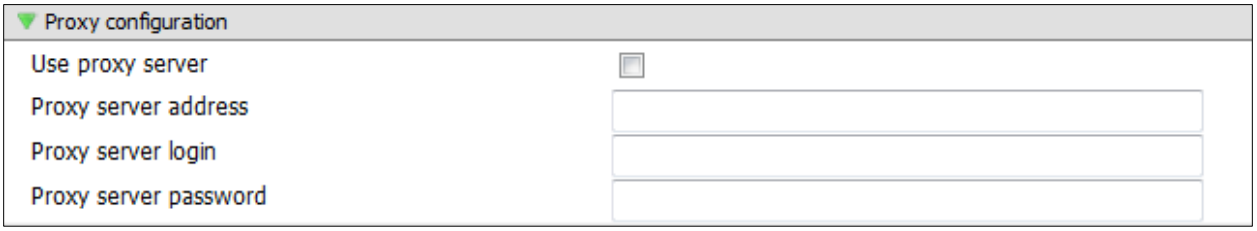
Advanced SMTP Relay Configuration

If additional SMTP settings are required to allow an SMTP relay to function correctly, the settings are located here. Limitations on sending threads and retry intervals as well as authentication methods can be configured to suit the requirements of the host system.



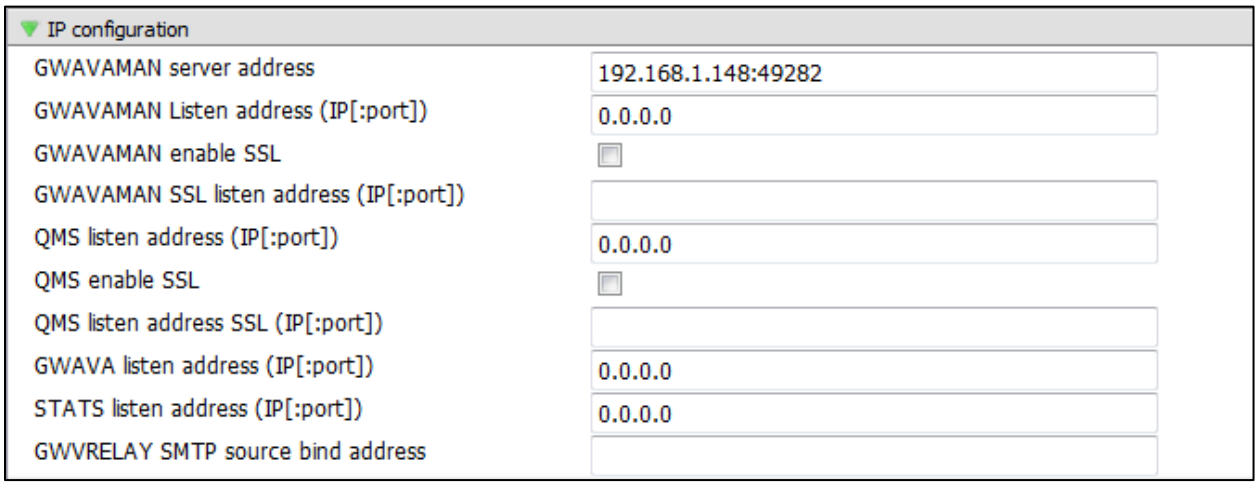
Proxy Configuration

If your system accesses the internet through a proxy, add the information here using the syntax proxy.myfirewall.com:8080. If a proxy is not used, this should be let blank.



IP Configuration

The connection addresses for the different objects in GWAVA are listed and configured on this page. *There is no reason to configure these settings on standard GWAVA installations unless the GWAVA server has been installed to a cluster*. These settings should not be changed unless instructed by GWAVA support.



SSL

SSL configuration is offered under the 'SSL Configuration' section at the bottom of the page. If the system requires SSL for security or for integration into an existing system, ensure that all the required information is prepared for the server.

The ciphers shipped with GWAVA are weak. The strength of the ciphers can be tested with: https://ssl-tools.net/mailservers

To update the SSL Cipher List, go to **Server / Interface Management | (Server Name) | Server Management | Configure Server | SSL Configuration | SSL Cipher List**

In the SSL Cipher List field, paste:
`EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA`

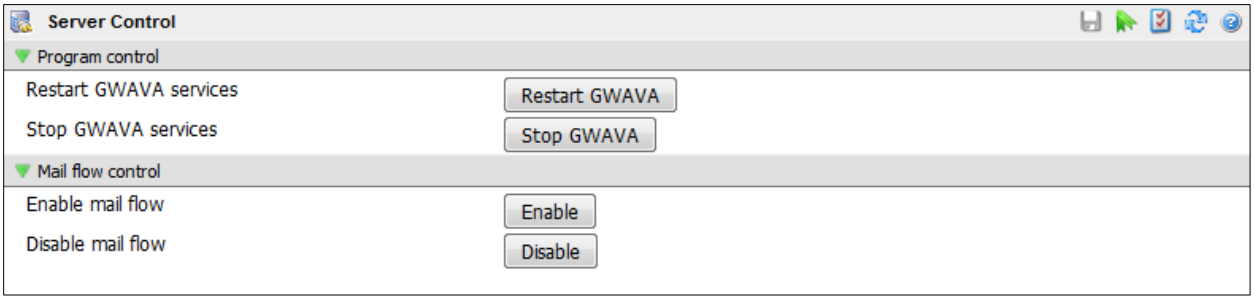
Advanced

If it is required to ignore the .com fingerprint in body of the message text, this option may be set here. Messages containing references to domains or link types, but which are not from those domains, may be blocked doe to the links. If this is a problem, it may be disabled.

Configure Domains

All domains for which the host mail systems receive mail must be listed on this page, as either the default domain or as an additional domain; otherwise, GWAVA will not accept mail sent to a domain(s) not listed. This section is covered under the SMTP interface creation section.

Server control

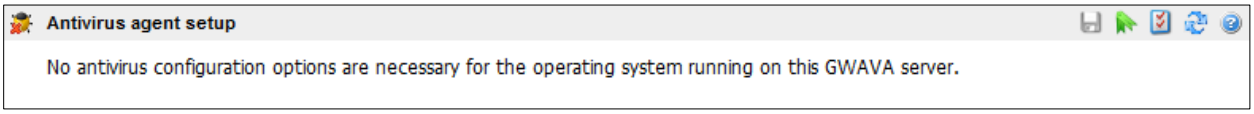


The GWAVA server functions can be controlled from this section; stopping or restarting GWAVA and mail flow. This is useful if there is a need to pause the mail flow in the system or if GWAVA needs to be restarted or worked on.

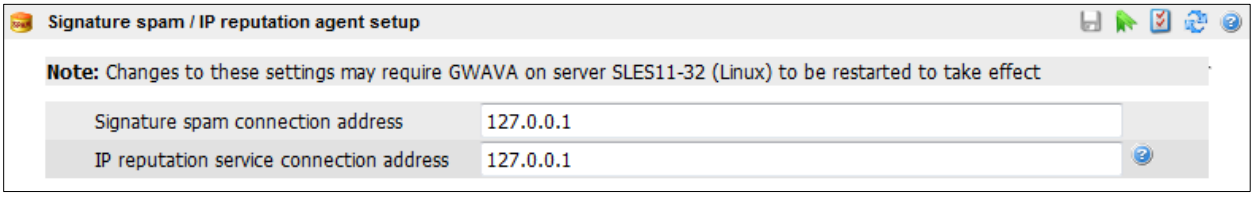
Antivirus agent setup

GWAVA comes with the Antivirus engine automatically setup and active. This page gives information on the Antivirus agent. The antivirus will connect to the internet and download virus updates hourly,

therefore the antivirus only needs to be configured if the network utilizes a proxy to access the internet. (Proxy server settings are specified during server activation, and may be added or configured later on the **Server/Interface Management | <Server name> | Configure Server** page under the **Proxy Server Configuration** section.)



IP Reputation Setup

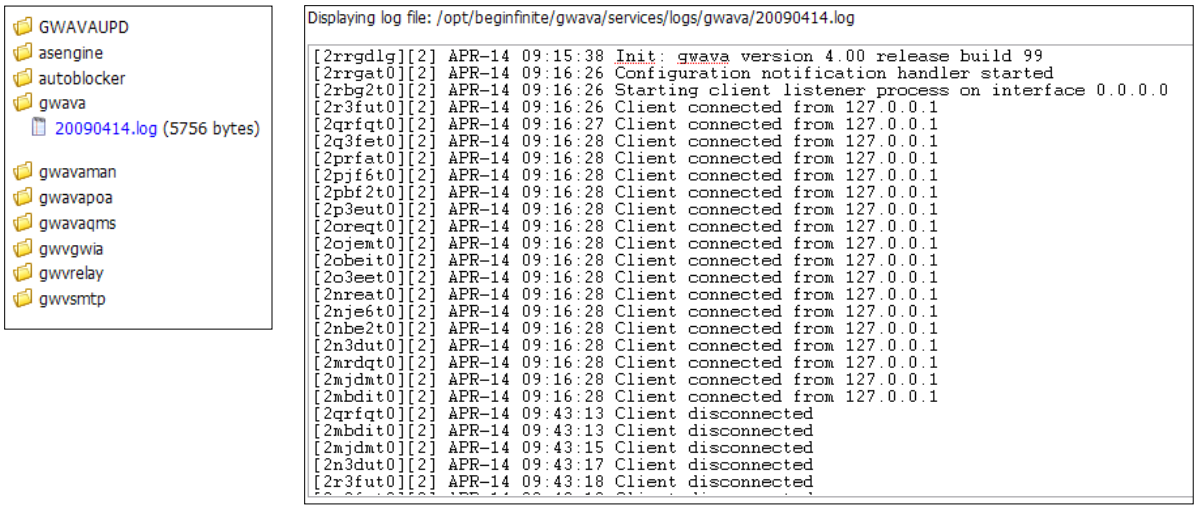


The GWAVA scanning system can provide signature and IP reputation services to other GWAVA servers in the same network. If a secondary GWAVA server is to provide the interface service, the connection information for that server must be specified via IP address. The default configuration is to have the local host provide the scanning service.

Logs

GWAVA keeps logs for each major module in operation, with the logging level determined by the server configuration. For most situations, leaving the log level at normal will be sufficient. The Log menu option allows the admin to view the logs from the GWAVA management console. The logs are also available in the file structure for offline viewing. The file location is listed at the top of the log page:

```
<Where gwava is installed>/gwava/services/logs/<module>/<log>
```

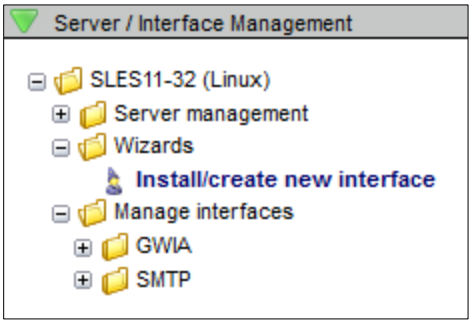


The different modules perform different tasks. The main modules to view, if desired, are:

gwava – the main interface
gwavapoa – post office interface
gwavaman – management
gwavaqms – quarantine manager
gwvsmtp – GWAVA Smtp service

Wizards

This feature is covered under the interface creation section.

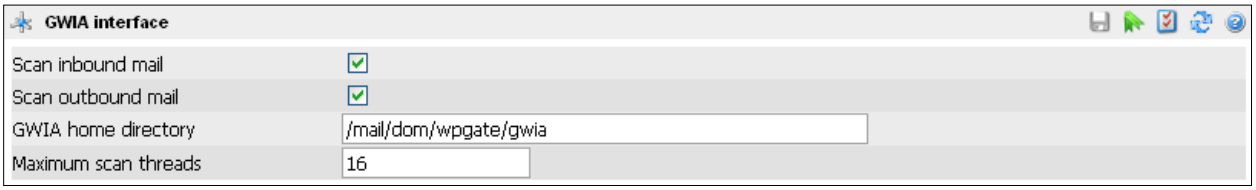


Manage interfaces

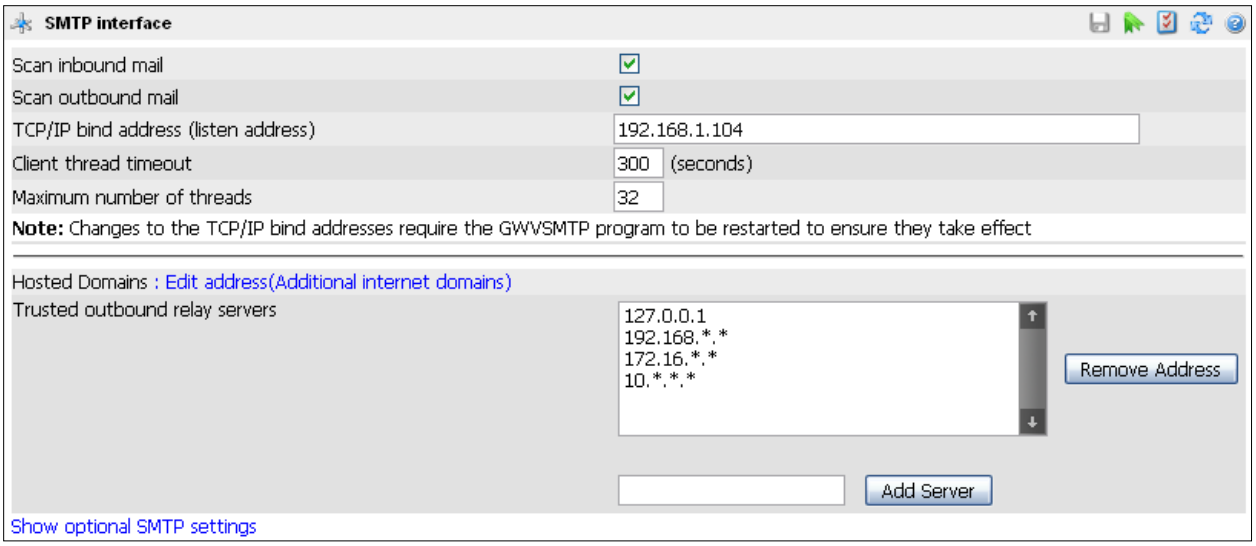
The Manage Interfaces menu option contains the settings for each interface, organized under each interface's name. To bulk modify interfaces, the interfaces must share an interface engine. See the 'Advanced' section for more information.

Interface settings

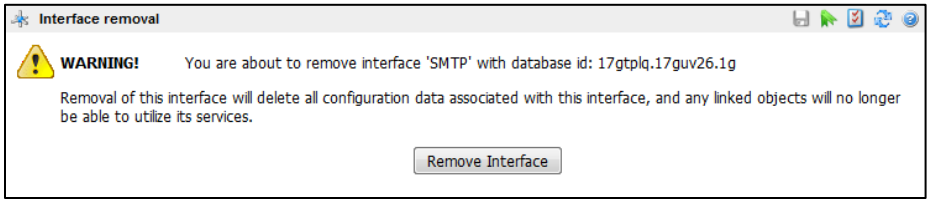
This menu item lists the basic connection and interface settings for the different interfaces specified during each interface's creation setup wizard. Each interface type will have a different interface setting page with only the information that each interface deals with. For instance, a GWIA interface's interface page only lists the home directory and mail flow settings, as that is all which is required to interface with a functioning GroupWise Internet Agent.



The following is a SMTP interface, which requires a binding TCP/IP listening address, and any other connection settings, depending on your network setup.



Interface Uninstall

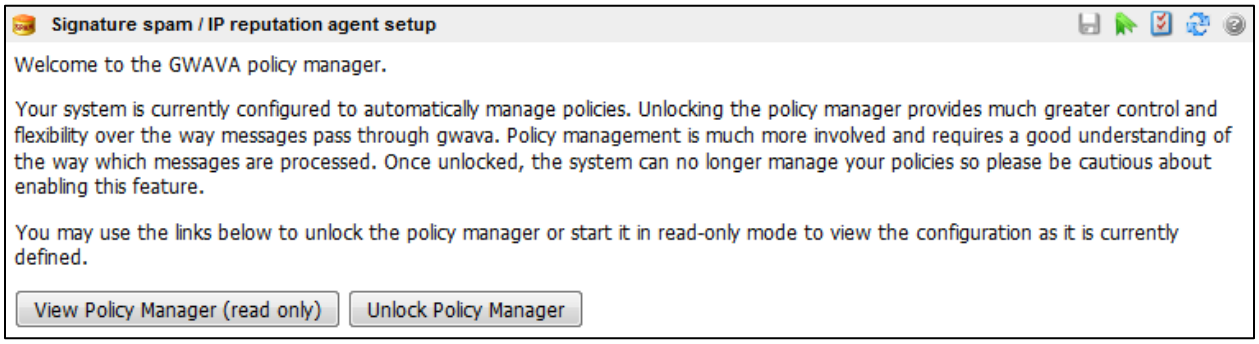


When you select the uninstall option you are prompted to confirm that you wish to remove the entire interface. Be aware, there is no restore option for uninstalled interfaces. Uninstallation does not remove abilities or associated policies from the system, but it does remove the interface from the selected options in those policies and configurations.

Scanner / Policy Management

Policy Manager

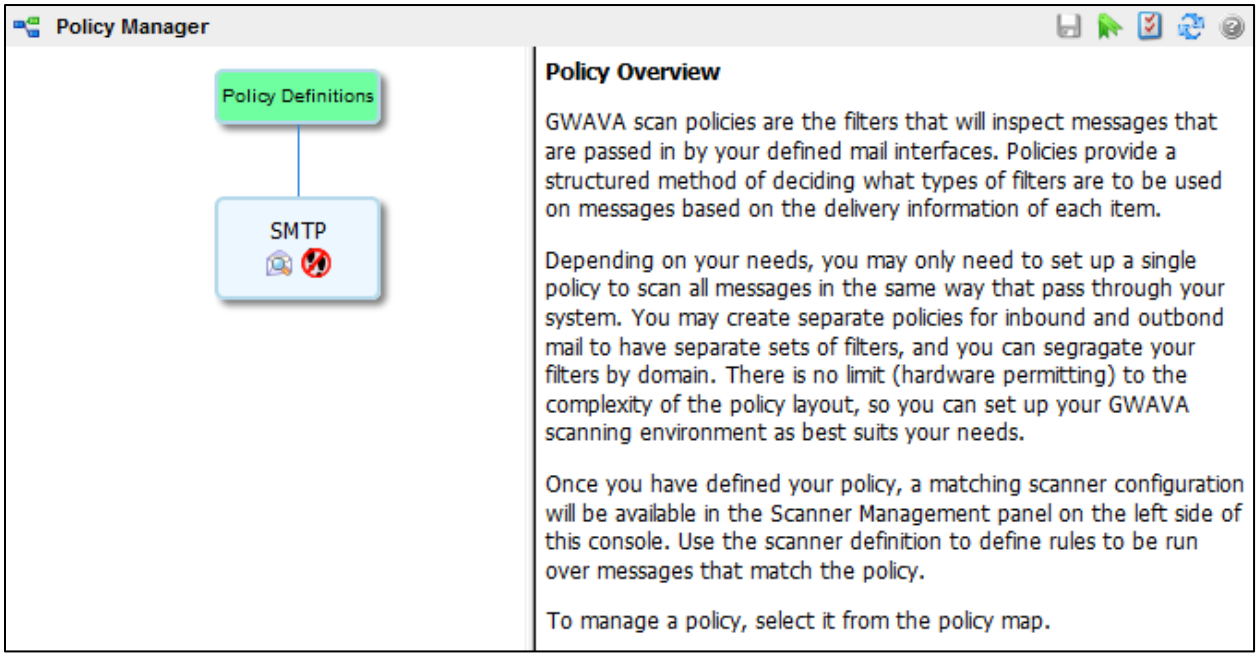
GWAVA introduces the 'policy' to the GWAVA interface. Polices are utilized mainly for multi-tenant systems; systems with multiple domains, interfaces, or both. GWAVA and the Policy Manager disassociate domain settings from the interface, allowing multiple managed domains under the same interface, or vice versa. If, for example, multiple domains are hosted on a large system with load balanced SMTP servers, the policy manager can implement several different scanning profiles through a single or multiple SMTP interfaces all controlled by the same GWAVA server. A policy may also be used to manage several completely separate domains hosted on the same SMTP server, through the same SMTP scanning interface, with different criteria for each domain.



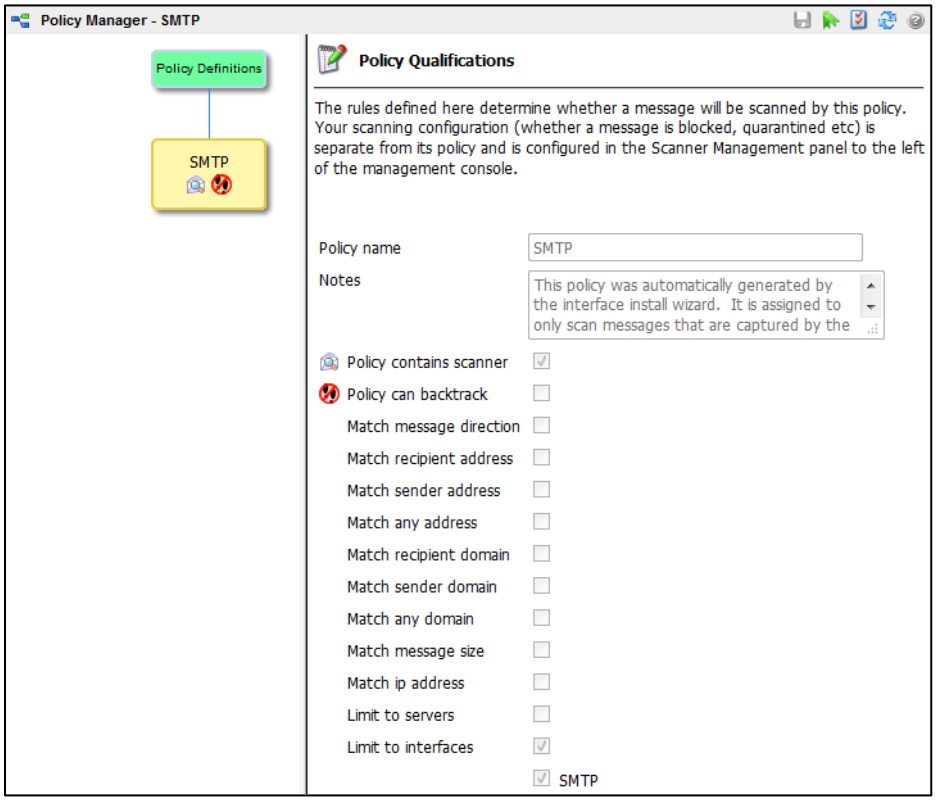
By Default, the Policy Manager automatically creates and manages policies for interfaces. Unlocking the Policy Manager permanently disables automatic management. If the GWAVA system is setup to only utilize a single domain and interface, or the different domains managed are to have the same scanning policy, then the Policy Manager should be left to manage the policy automatically. Policies are required for scanning to be completed, as they are the framework for all mail flow and dictate what mail 'qualifies' for scanning.

The active policy can be viewed at any given time, but once the policy manager is unlocked, or opened in editing mode, the GWAVA system will no longer automatically manage the policy. This means that every time an additional interface is added to the system manual manipulation of policies is required.

The simplest way to deal with the Policy Manager is to allow the Policy Manager to be automatically managed by the system.



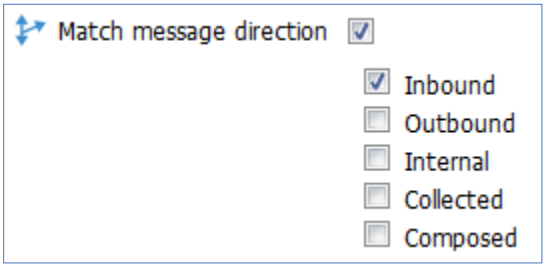
Viewing policies in read-only mode displays all the pertinent information in a grayed-out text. Selecting the different parts of the existing policy tree will display the policy active on each section.



Every automatically created and configured policy contains identifying notes, and will be tied to the interface that it was created with.

All gray text and settings are locked and cannot be modified.

One of the most useful ways to use the read-only Policy Manager is to check active direction scanning settings. If mail is unintentionally being caught on outbound scanning, it can become a difficult situation to detect or understand. The Policy Manager can quickly display which scanning directions qualify for scanning with the system in question simply by selecting the desired policy and checking the scanning direction settings. With a policy, a selected option restricts the filters, limiting only mail qualifying with the selected options to be scanned.



The different settings are as follows:
Match message direction – restricts direction scanning
Inbound – Scans inbound messages
Outbound –Scans outbound messages
Internal – Messages with destinations within the system.
Collected – Scans messages which are being stored in the system
Composed – Scans "draft" messages which have been created, but not sent

In the displayed example, only inbound mail will be scanned according to this policy. Outbound, internal, collected, and composed mail will be exempted from the policy. If, however, the message direction option is left unchecked, then all directions will be scanned according to the rest of the policy.

How mail qualifies for scanning is described in the 'How mail flows through a policy tree; Qualification' section below.

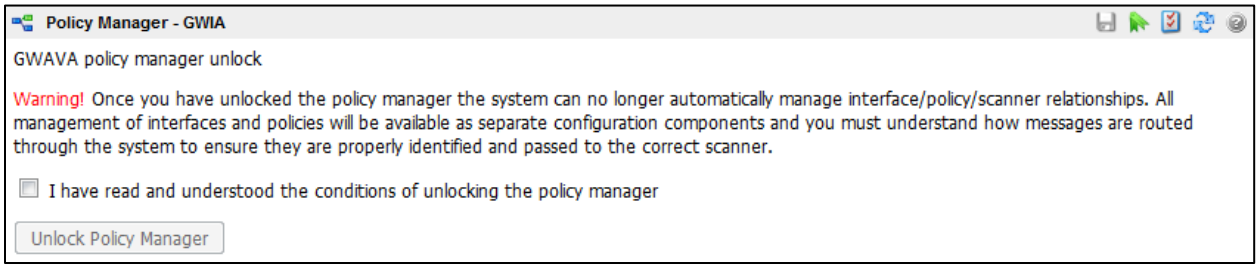
Any automatically created policies with previously created scanners will be displayed as root-level policies with their own scanning configurations.

If multiple interfaces are configured on creation to share a policy, only the one policy will be shown, but it will be connected to both interfaces. All scanning configuration may be edited or changed under the Scanner/Policy Management menu tree.

For scanning settings, please see the next section, Scanner / Policy Management, where all scanner settings, configuration, exceptions, and message services are configured.

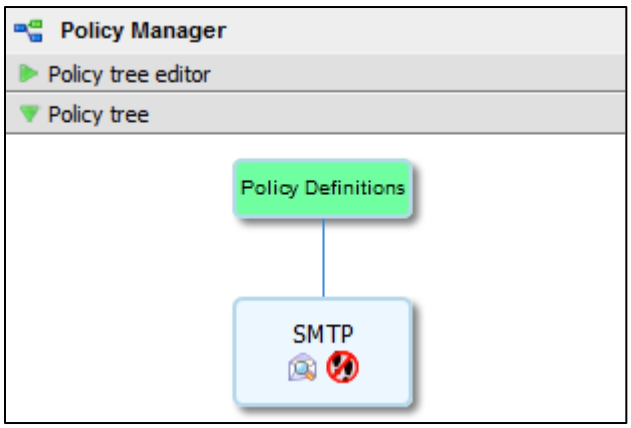
Unlocking the Policy Manager

To unlock the policy manager for direct editing, the administrator must verify that they understand that they are disabling the automatic management.



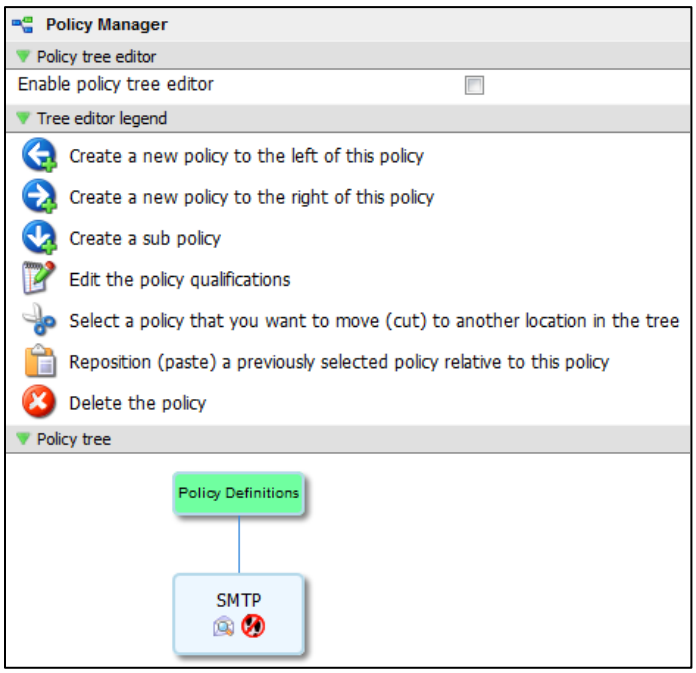
Select the checkbox then click the 'Unlock Policy Manager' button.

Once the Policy Manager has been unlocked, select the blue link to continue. This page and warning will not be displayed again.

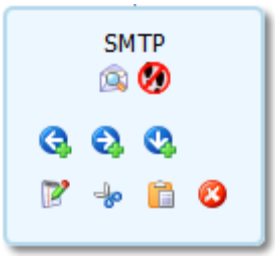


When unlocked, the policy tree has an additional drop-down menu to enable editing of the tree, called 'Policy tree editor'.

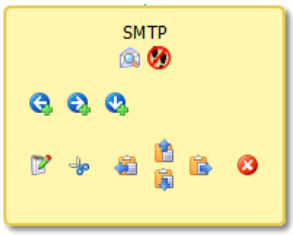
Opening the Policy tree editor exposes a checkbox as well as an additional drop menu explaining all of the editing icons.



When the checkbox is selected to enable editing of the policy tree, the editing icons are displayed on each policy as shown.

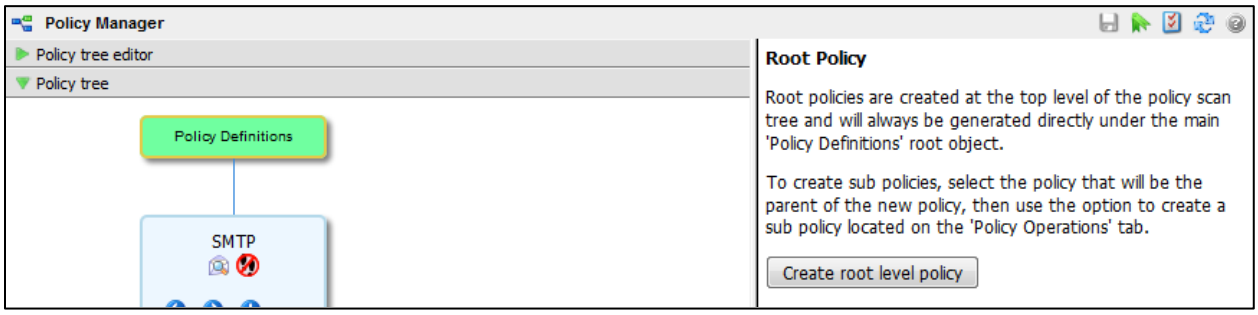


To create a new policy under, below, or next to an existing policy, enable the policy tree editor and then find the desired parent policy. Select the appropriate icon and complete the wizard displayed in the information window. The wizard is a standard policy creation wizard and is nearly identical to the interface creation wizard. Upon wizard completion, the new policy is created.



To move a policy, enable the policy tree editor and select the scissors, (cut), icon on the policy that is to be moved. Then find the policy that is to be the parent or neighbor to the newly 'cut' policy and select the clipboard, (paste), icon. After the paste icon has been selected, locate the appropriate arrow designating the new location for the policy. All arrows are relative to the location of the 'paste' selected policy; left of, right of, sub policy, or parent of the selected policy.

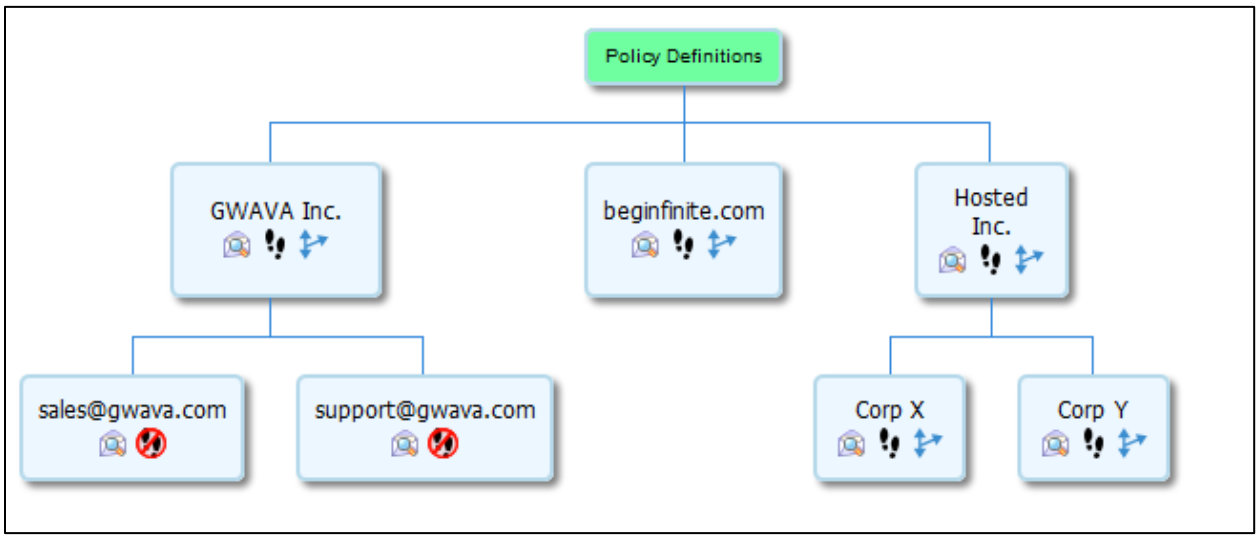
Policies may also be created at the root of the policy tree without selecting the tree editor. Simply select the 'Policy Definitions' button at the top of the tree then select the 'Create root level policy' button in the information window. This will spawn the policy creation wizard. Completing the wizard will create a root level policy.



How Mail flows through a policy tree; Qualification

Mail flowing through the GWAVA system must 'qualify' for specified criteria before it can be scanned by the policy. Any mail that does not qualify for the policies defined will simply pass through the system untouched and unmodified. Due to this qualification, any system with multiple domains must not only add those domains to the configure domains page, but each domain must either have a policy connected to it, or must qualify for a general policy in order for that domain's mail to be scanned. The qualifications will be covered with the example below.

The policy tree dictates how mail will flow through the system, and is useful for Multi-tenancy setup and control regardless of how many interfaces the policies are tied to. The following system has been setup to show some complexity available for system mail flow and to explain the system.



Multi-Tenancy and Policy Trees

In the example, five different domains are active and hosted on the same SMTP server: GWAVA.com, beginfinite.com, hostedinc.com, corpx.com, and corpy.com. The different domains require different scanning settings and message services. GWAVA.com mail is scanned differently from the beginfinite.com messages.

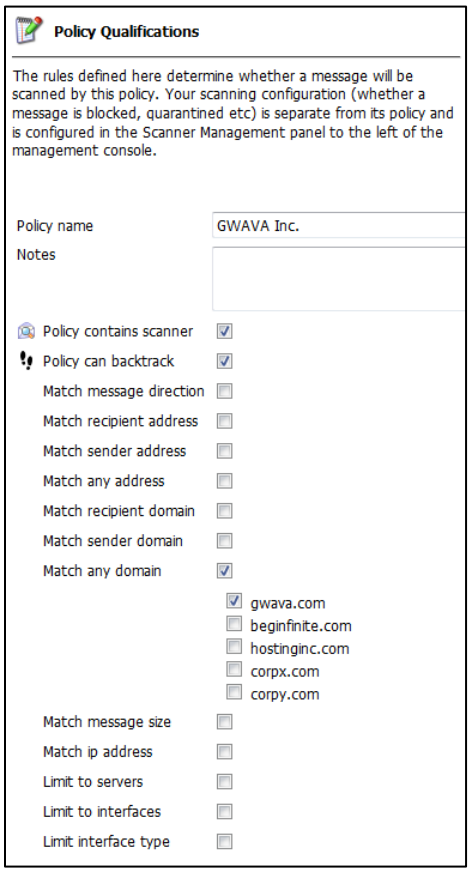
In addition, a hosting company is also present which manages two domains for customer organizations that require their own scanning configurations.

In addition, the general settings for the gwava.com domain are insufficient for both the sales and the support users, which have different requirements for message services. With policies created for each of them, all their scanning and message service requirements can be fulfilled.

This configuration is tied to domains, message direction, and sender addresses, and all contain a scanner. It is important to assign policies to contain a scanner; otherwise the policy will not scan the mail.

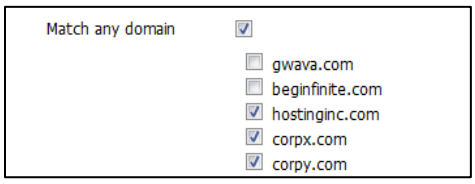
(In the event that a message is sent to multiple recipients matching several or all of the different domains, the message will be 'split' and copies scanned according to each individual policy, then sent to their respective recipient(s) in each domain.)

When messages come to the GWAVA system through an interface, the GWAVA system compares the mail to the policy tree to find any policy that the mail qualifies to be scanned by. All of the qualifying criteria are displayed in the information window. (Mail flow is explained in more detail on the next page.)



Criteria selected in the qualification window limits the amount of mail that the policy may match. The more active criteria enabled on a policy, the harder it is for mail to qualify.

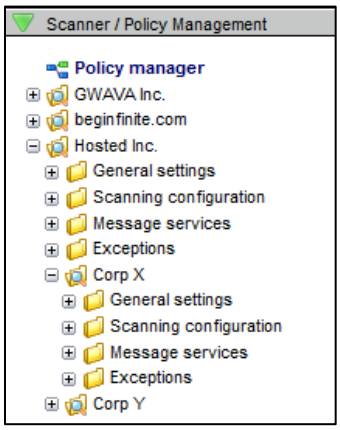
The displayed policy only requires that mail be sent to the gwava.com domain to qualify for the scanner. With this configuration, only mail that is sent to the gwava.com domain will be scanned by the GWAVA Inc. policy.



With the above example, the Hosted Inc. organization is hosting not only their own, but two additional domains which they manage and provide base service to in addition to specific services for each domain. To provide that service, the Hosted Inc. policy must contain bindings to all three domains. The messages will then be moved further down the tree to the sub-policies that also apply to their respective domains for Corp X and Corp Y, with their specific scanning criteria.

For example, messages sent to Corp X will be scanned according to the Hosted Inc. policy and then the additional Corp X policy as well.

Policies which appear underneath another policy, sub policies, automatically inherit the scanning limitations of the parent policy as mail moves through that configuration first.



See the Hierarchy section in the appendix for more information.

Because sub policies are subject to the parent policy, when specific configuration of the scanning engine is performed, the sub-policies are found nested underneath their parent.

Sub-policy scanning configuration contains all the same settings that a parent scanner contains, and can be configured independently. When configuring nested policies for scanning, it is wise to ensure that the parent scanner does not contain any unwanted scanning configuration to minimize conflicts which could disrupt mail flow.

Specific Policy Settings

Policy contains scanner

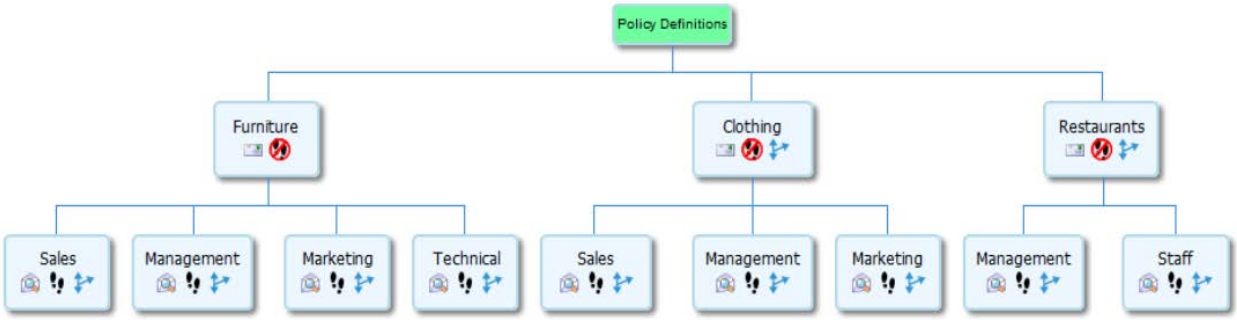
The 'policy contains scanner' setting is useful in complex configurations, but can be useful for some standard configurations as well.

The policy management structure allows mail to be categorized as it flows into the mail system and scanned according to each category the messages 'qualify' for. Examples of different possible categories include: inbound and outbound mail, sales and marketing departments, technical and executive mail, or students and teachers. Each of these categories can be clearly defined by the receiving users and each group has different scanning needs. The 'policy contains scanner' setting becomes very useful and

necessary when managing increasingly complex settings including multiple sets of categories and users in a policy tree.

In an example of such a complex policy tree, we'll use a single organization containing three very different departments. A simple setup would contain a policy for each department, which functions wonderfully until each department also has its own sales, management, marketing, and technical staff requiring different scanning rules to accommodate mail needs. It is important to correctly setup a policy tree when dealing with complex configuration to maintain a simple, and easy to read, setup.

In understanding how to create complex scanning configurations, it is helpful to create organizational policies, or 'container policies'. Container policies are organizational categories and do no scanning of their own, but are placeholders or containers to meaningfully organize the policy tree.



The different departments shown above are containers for the different organizations and scanning policies. In the above layout, scanner settings are configured and independently implemented for each department within the organization, and it is easy to visually identify the structure and layout of the GWAVA scanner.

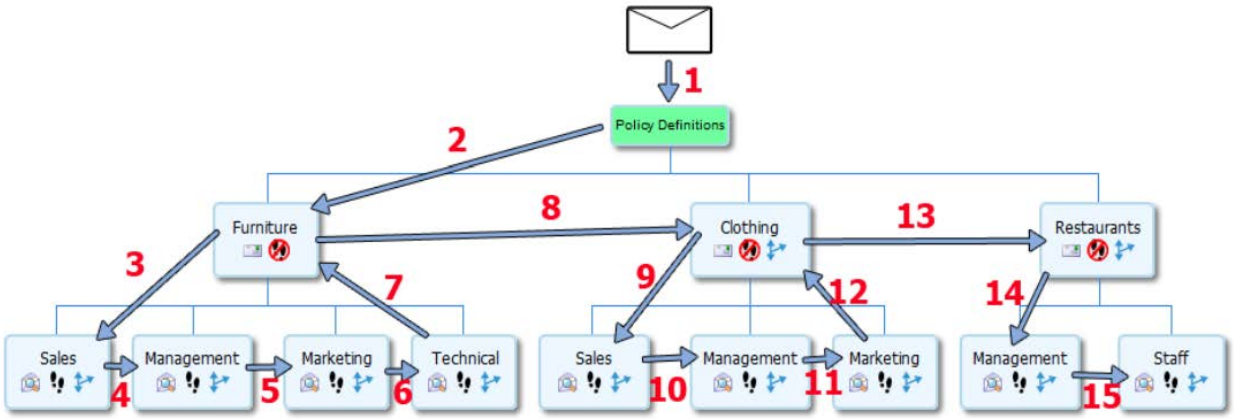
Keep in mind that this layout represents which scanner configurations will be used to inspect messages does not necessarily reference or depend on the server or MTA that messages are passing through. Referencing the diagram, this layout would be well suited for an IT department that has a single SMTP the mail comes into. Even though the mail is all passing through the same entry point, GWAVA will pass every message through the policy manager to be sorted, categorized, and scanned according to the policy that the messages qualify for. A message that comes for a sales representative from the clothing branch will be scanned by the rules for his organization, and none of the others.

Backtracking and Mail Flow

Backtracking is mainly used with complex policy structures. In most systems the backtrack option should be left enabled. To correctly explain backtracking it is necessary to look at mail flow in slightly more detail.

Backtracking is related to the way in which mail 'walks' the policy tree looking for a qualifying policy, or the correct scanner, to use for any particular piece of mail. The comparison movement is top to bottom,

left to right. This process is shown below, where a message for a 'Staff' member of the 'Restaurants' department is sent mail. When their messages are received they will systematically walk the tree in the following manner.



With this defined path for mail in a policy system, it is easy to see what will happen with mail. Messages are passed and compared to every policy in a system, and scanned and released appropriately.

If a message does not qualify for any of the policies, then ends up without a policy at all and will pass through the system without being scanned. This ability is useful for only scanning a portion of mail for a particular set of users. An example where disabling backtracking would be useful is when the system is required to scan the mail in the clothing department for the sales, management and marketing but no one else.

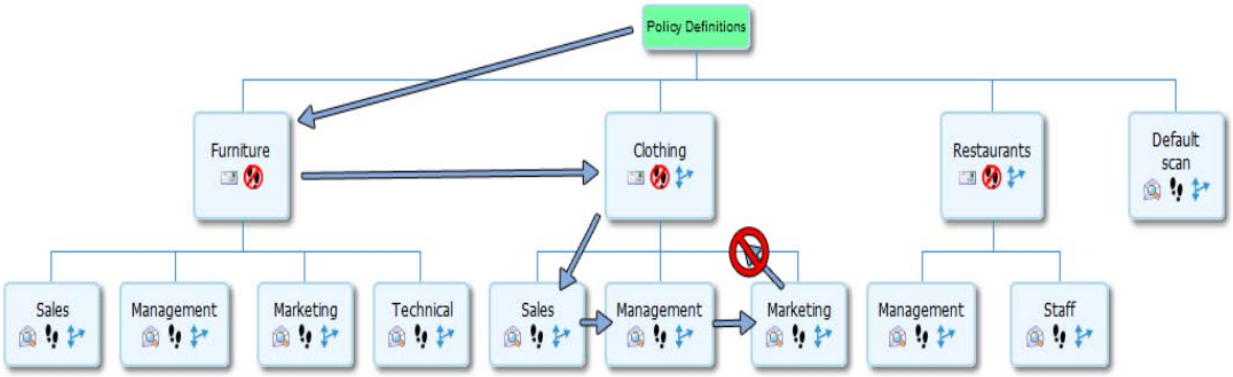
If all messages are to be scanned, a default or generic scanner policy can be created to scan all messages which do not qualify for any other policy. This ensures that all mail is scanned. As shown below, the policy has been modified to include a default, generic policy.

Backtracking becomes effective when all mail that is not for a specific department that is managed should be scanned by the default scanner, but messages within a department that have not been targeted for scanning should be ignored.

The policy tree shown below shows a situation where a message might have been received for someone in the IT department. The IT department requires that their mail is not scanned. As the message passes down the tree, it does not pass into the 'Furniture' container because it does not qualify (likely by a domain qualification), then moves on to the Clothing container, which it qualifies for at a high level (again, likely the domain '*@*clothing.company.com'). At this point the message passes over all of the child policies looking for a match for the message, but it does not qualify for any other policy.

At this point, the backtracking feature kicks in. Normally, the next step for the mail is to go back up to the 'Clothing' policy and move right, but the message hits the 'no backtrack' option at the root policy and graduates from the policy tree without completing the tree walk. The result of this is that the IT

department’s mail bypasses scanning, as it is prevented from continuing to the final destination of the 'Default' policy by disabling backtracking.

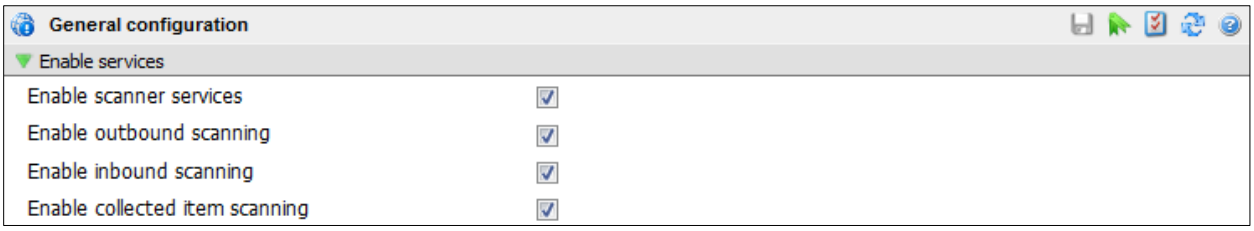


Backtracking is a feature that is normally wanted for the very purpose of falling back to a default scanner, however when you come across a need to stop a specific type of mail from being scanned, backtracking provides that ability.

Scanner Management

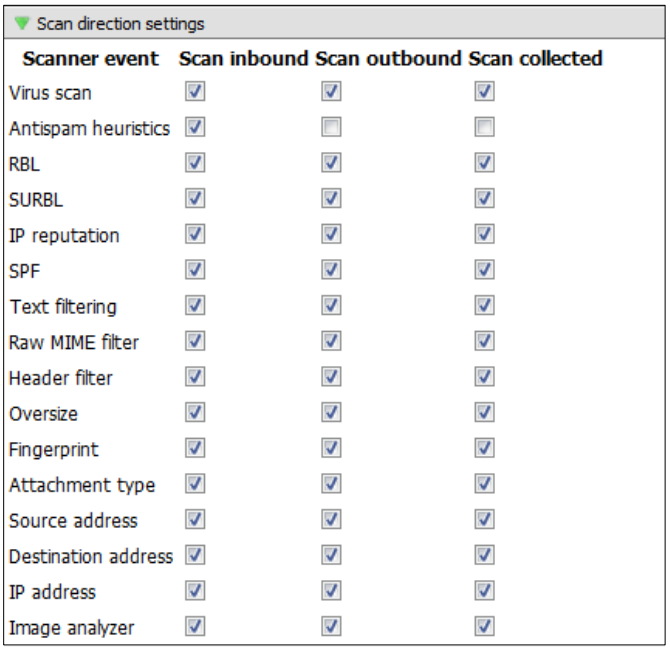
Scanning configuration is organized under each respective policy name, which governs what messages are scanned. Root policies are listed by themselves, while sub policies are nested within the parent configurations.

General Settings

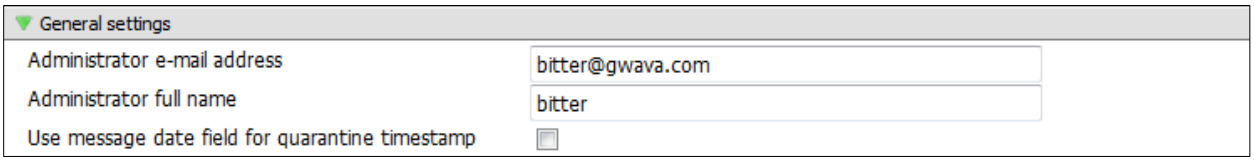


Enable Scanner services: Enables the interface, or places the interface in bypass mode.
Enable outbound scanning: Enables the interface to filter outbound mail.
Enable inbound scanning: Enables the interface to filter inbound mail.
Enable collected item scanning: Enables the POA interface to function if attached.

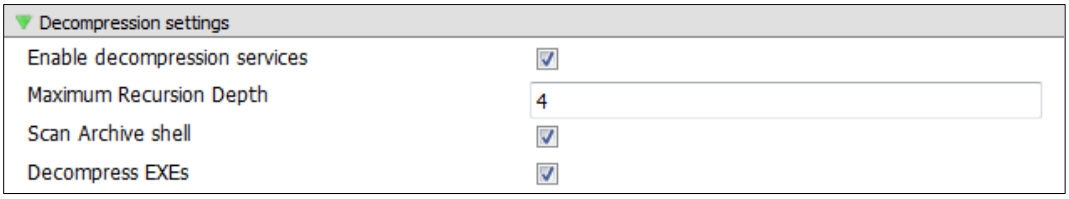
The defaults for the Scan direction settings are shown. The Per event scan direction settings perform the same as the global settings described above, except that it only applies to specific interface events. The default is shown, with all enabled except outbound Anti-spam scanning. In example: if SURBL, RBL, IP reputation or SPF are enabled on the interface, but are not desired for outbound mail, unselect the scan outbound box for those services and click the save changes button to apply them in the interface. The 'Scan Collected' box ONLY applies to scanning a GroupWise Post Office, and will only be useful if the interface being modified is a POA interface.



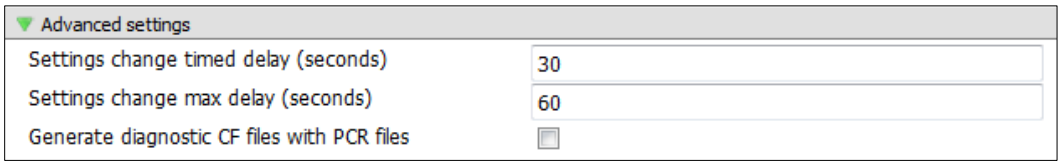
General Settings govern the notification address and settings for the selected interface. The general settings are taken from the system default settings, and do not need to be set or changed unless a different notification address from the default is desired for different interfaces.



The Advanced Decompression Settings dictate how deep a message is scanned. Default recursion is 4, and all options are selected.

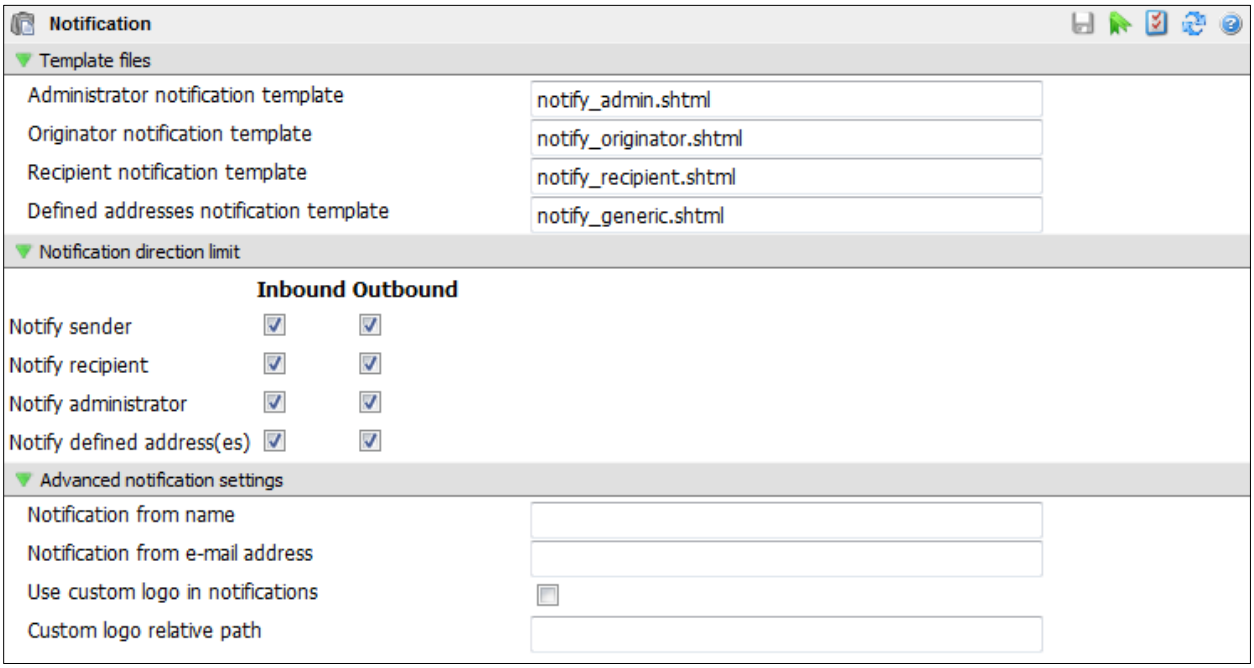


Advanced System Settings provides customization on the timed delay. This delay is the amount of time that GWAVA waits to reload system configuration after a change has been made in the management console. Default is 30 seconds for a change delay, and the max delay is set to 60 seconds.



By default, GWAVA will not generate a diagnostic CF file with the scanning PCR files. These files are temporary files used when troubleshooting the message scanning process. Unless specified by support, there is no need to create a CF file.

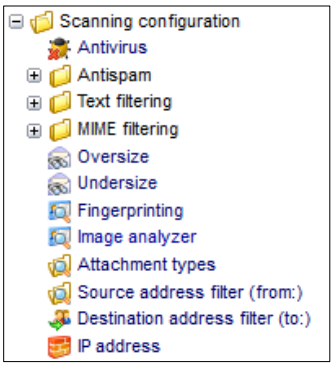
Notification



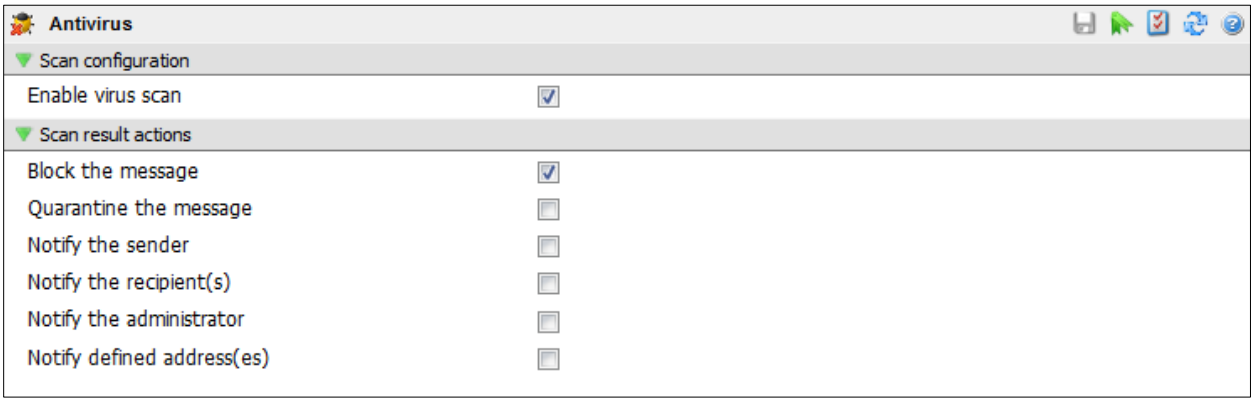
The notification options allow you to specify which templates are used to create the message, the send from address, (the admin address and name are the default used as the 'From:' address), and the events specified for notification. Events specified for notification here still depend on the notification setting to be active in the individual interface events.

Scanning configuration

Antivirus



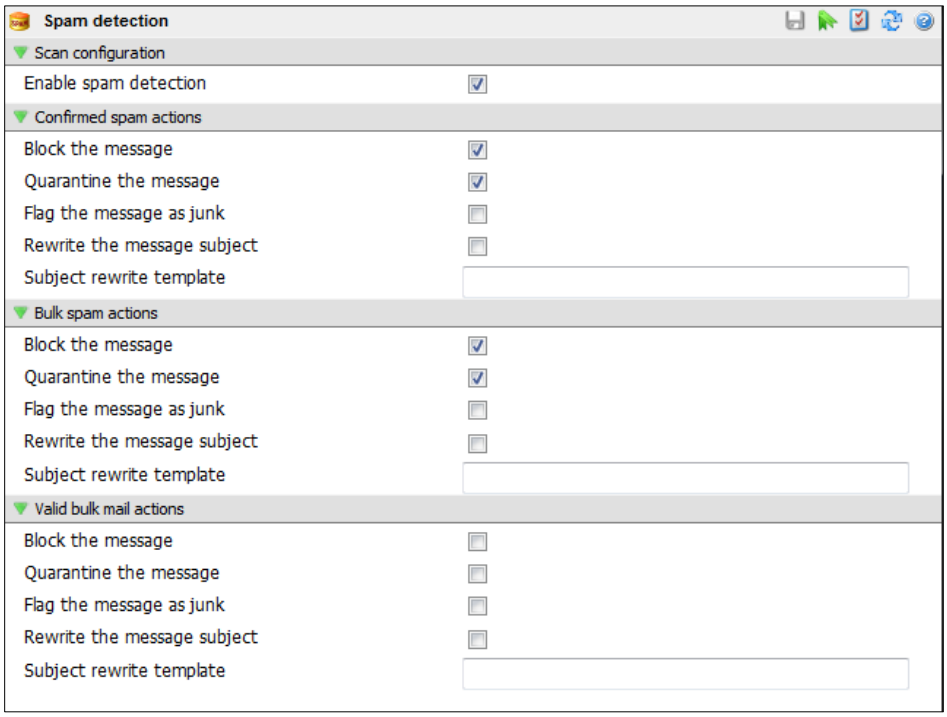
The default antivirus scanning settings are set to scan messages for viruses, and if a virus is found, the message is immediately blocked/deleted, and, regardless of any other setting in the system, never added to the quarantine. See the four-state checkbox section in the appendix for details.



Antispam

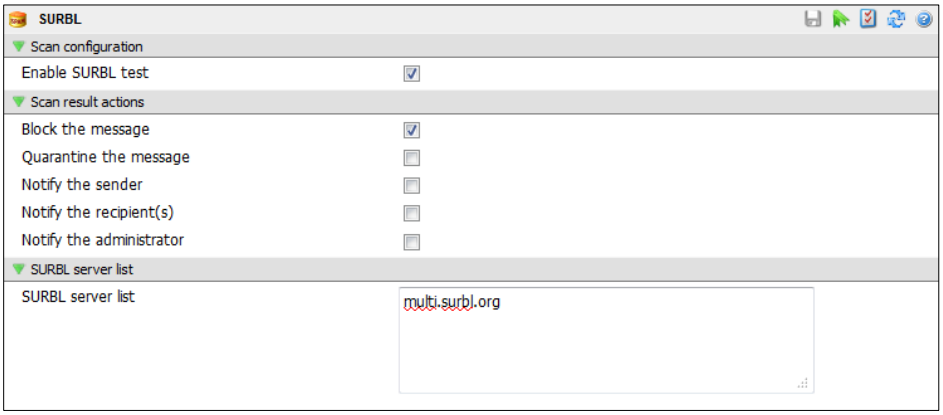
Spam Detection

Spam detection is performed against the signature scanning engine. Messages detected as spam by the system will have the following selected actions performed on them. Spam messages are not required to be blocked or sent to quarantine, they can simply be flagged and sent along, or flagged and have their subject re-written. However, the default action is to block and quarantine to keep mailboxes free.



SURBL

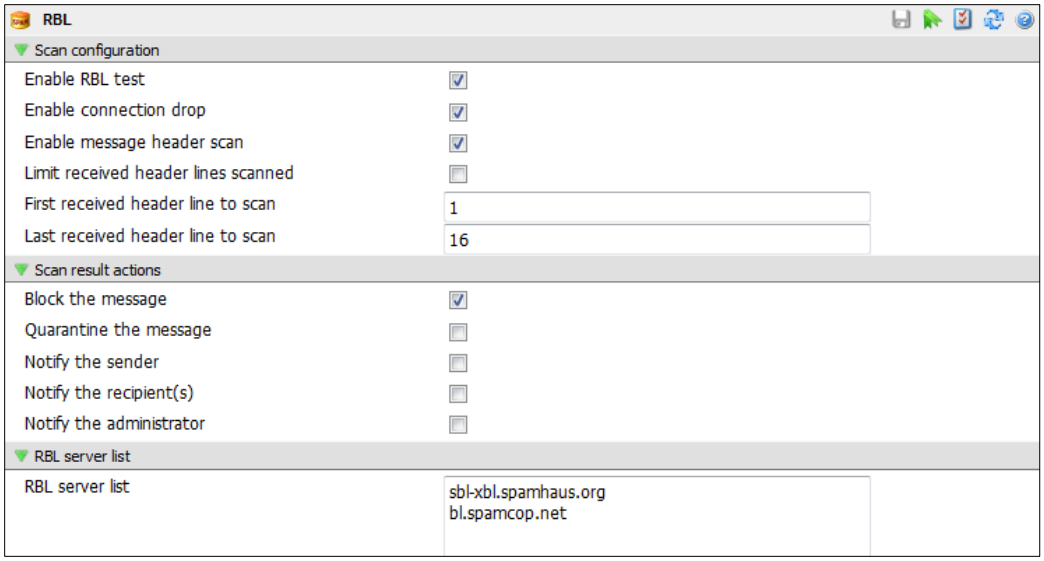
The SURBL event checks each message against the SURBL databases listed in the SURBL servers listed, to see if the sending server is included on the SURBL list. If it is included, the message is blocked. SURBL servers may be added or removed from the active list as desired. (It is not recommended to have more than two SURBL servers active at the same time as it may extend the scanning time with extra lookups.)



RBL

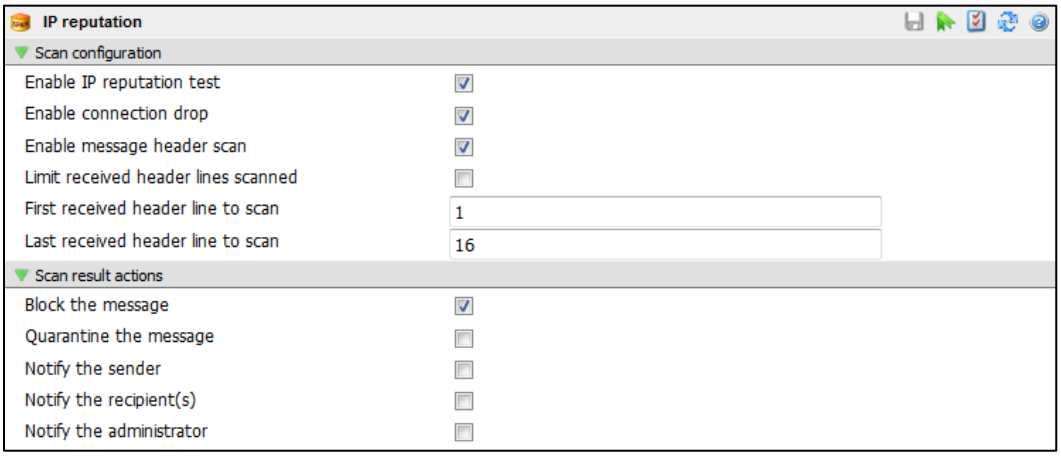
The RBL event functions the same as the SURBL event does. Incoming messages are checked to see if any sending server(s) are included on the list of the RBL servers listed. If a match is found, the service specified will be performed, (block, notify, quarantine).

The RBL event may be limited to certain lines in the message. The default is to scan the entire header of a message. (It is not recommended to have more than two RBL list servers active at the same time as it may extend the scanning time with extra lookups.)



IP Reputation

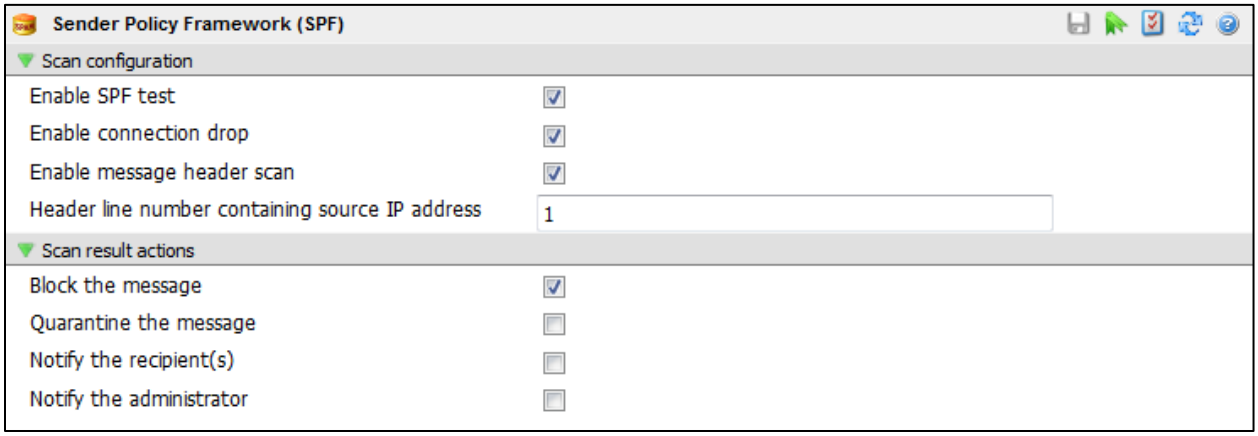
IP Reputation works much like the RBL interface does, in that it uses a black list, but also has a white list for common mail sources. But when used on a SMTP interface and configured for a connection drop, IP Reputation will temporarily fail messages from sources not found on either list. The temporary fail will allow the sending SMTP gateway to retry, and IP Reputation will allow a repeated unknown attempt to pass on to the Antispam filter. As with RBL, the header lines scanned may be limited and specified. (This can be used to skip lines added to the header by a proxy server or other service.)



SPF

Sender Policy Framework can be used with the GWIA and SMTP interfaces. Sender Policy Framework, (SPF) attempts to verify the sender of each email message, which can eliminate spoofed email and most backscatter attacks. For SPF to work correctly, the sending domain must have an updated SPF record set up in DNS. If the sending domain does not have a SPF record set in their DNS, then their mail will not be blocked. Setting up a correct SPF record will block messages from spammers who are pretending to be you, to your system.

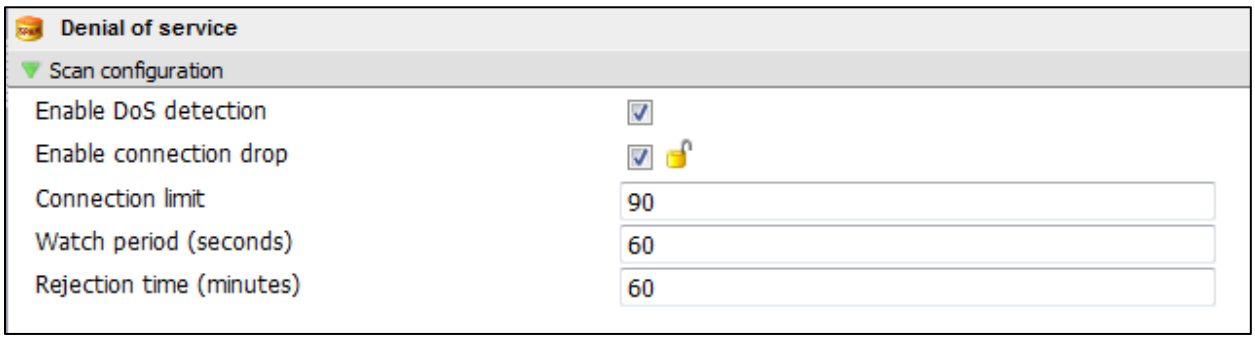
To use SPF on a GWIA interface, you must correctly specify which line in the header of mail messages is to be used. If the mail system is using a relay or proxy which adds a line to the message, then you should set SPF to use the second line (2), otherwise, the line used should be set to one (1), which is the default.



SPF can be configured to perform connection blocks in conjunction with the SMTP interface, which drops the receiving connection of a message before the message transfer is complete, if the sending server fails to be verified by SPF. This saves bandwidth as well as denying the messages from spammers.

Denial of Service

The Denial of Service option, only applicable for SMTP scanners, allows administrators to automatically deny connections to any address which attempts massive amounts of connections over a period of time. GWAVA automatically keeps a constantly updating list of addresses and their connections. Simple configuration and settings allow custom variables for this option.



For Denial of Service to function, it must be enabled along with the connection drop option.

Enable Connection Drop
The connection drop option empowers GWAVA to automatically drop any incoming connection from a banned address. If the Connection Drop option is not enabled, GWAVA will track addresses, but no action will be taken on addresses which qualify for the Denial of Service protection.

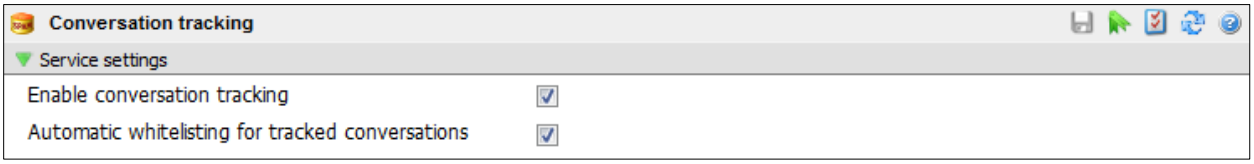
Connection Limit
This is the number of connections from any one address which the system will allow. This limit can be set to anything, but if enabled, this limit will be applied to every address sending mail to the SMTP server. The setting is defined as total allowed connections for the watch period.

Watch Period
The Watch Period is the time to which the connection period applies. This is the setting which decides how long an address is maintained on the watch list. If the number of connections allowed is exceeded in the time specified here, the address will be added to the rejection list, and all incoming connections from that address will be automatically dropped. The setting is defined in seconds.

Rejection Time
The Rejection Time is the amount of time a blacklisted address remains on the rejection list. Any address which is added to the rejection list will be automatically denied any connections to the GWAVA system. Addresses on this list will remain on this list for the specified time, and then be automatically removed from the list and connections will then be allowed again. An address released from this list will still be subject to the same connection limit and watch period which resulted in that address being added to the rejection limit in the first place. This essentially throttles the offending address to the connection limit over the amount of time listed in the rejection time setting; it does not permanently remove all message connections from the offending address. This setting is defined in minutes.

Conversation Tracking

Conversation tracking keeps tabs of continued email correspondence between local users and their outside contacts. These email 'conversations' are, by default, automatically added to a white list as well as copied and added to the advanced learning engine as examples of good mail.

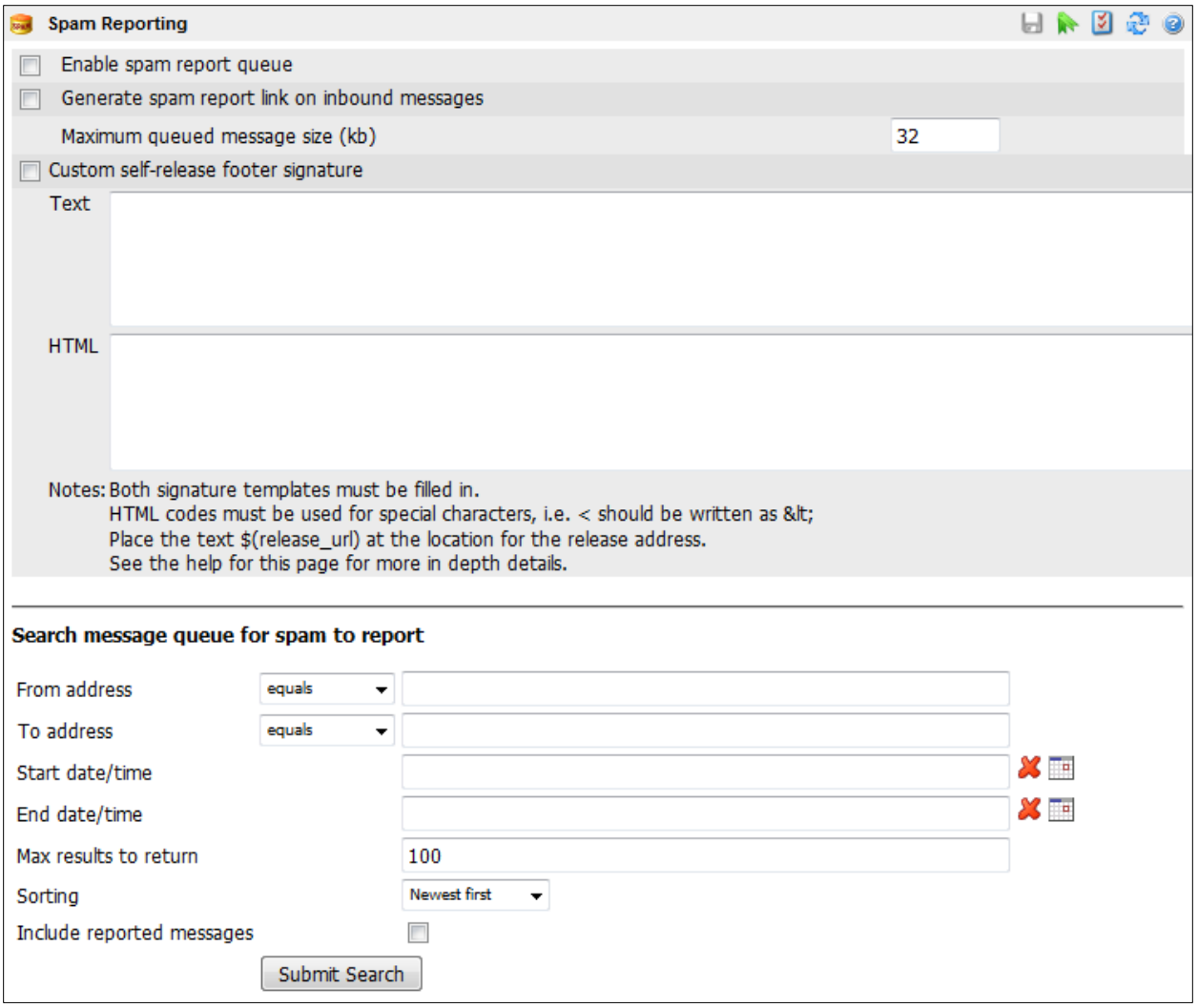


Spam Reporting

The signature spam engine included with GWAVA is extremely accurate, however, it is not perfect and GWAVA still has a way to improve the engine. Spam Reporting is a method by which messages which are flagged as spam can be submitted and reported to the master system.

When turned-on, GWAVA will keep a clean, unaltered copy of all messages that make it through the system for three days. If a message that was scored as 'clean' by the signature engine is discovered to be

spam, it can be searched for and the unaltered copy will be submitted and reported to the GWAVA systems as well as modify the local GWAVA rule set.



To facilitate quick reporting of spam, an automatically generated spam reporting link may be added to the messages which can simply be selected to report the offending message to the GWAVA system. The generated link may be customized in the provided fields, ensure to use proper syntax and fill out BOTH fields for a custom link.

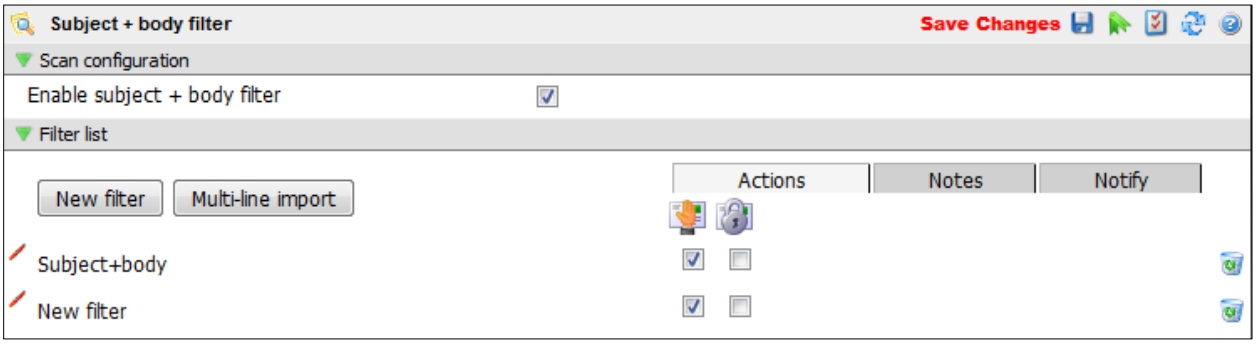
Text filtering

Subject + Body

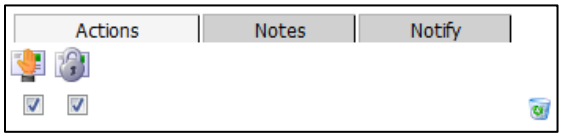
Subject + Body Text filtering searches the subject line and body of the message for a match to any filter specified. Filters must be added manually. GWAVA recognizes all plain text filters as well as standard regular expressions, or RegEx. GWAVA does not recognize RegEx ranges, (values in between { } braces), unless the entire RegEx string is followed by a '/q' at the end.

Subject or Body

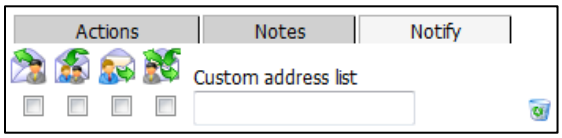
Both the Subject and Body filters work identically to the Subject+Body filter except that the filters added to these sections are restricted to only the subject of the message for the subject filters, and likewise only the body of a message for the Body filters.



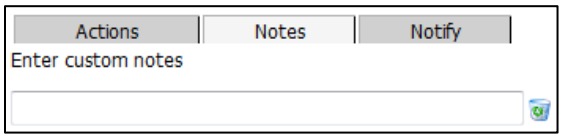
There are six optional actions or services for every interface event or filter that fires on a message: **Block**, **Quarantine, Notify Sender**, **Notify Recipient(s)**, **Notify Administrator**, and **Notify Defined Addresses**.



The action icons instead of the checkbox work as a global toggle.



Selecting the icon globally toggles, activates or deactivates the event for every listed option.



The block and the quarantine options are not the same. If you select to quarantine a message, but do not select the block action, then the message will have a copy placed in the quarantine, but still be allowed to reach the destination mailbox. Blocking a message without selecting quarantine will simply prevent a message from entering the GroupWise system.

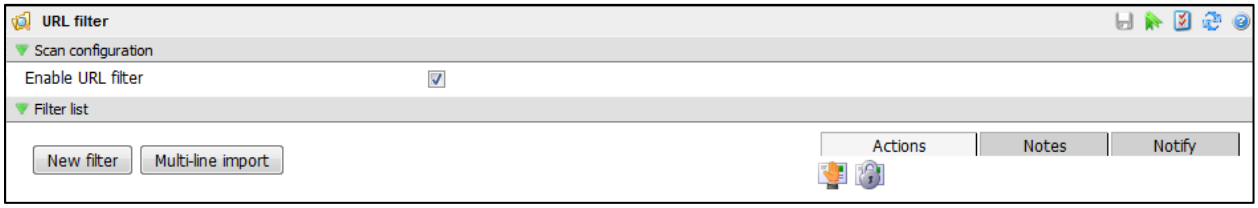
The different notification options are exactly as they are named and are active for every time the event fires. The Notify Defined Addresses sends a notification to the addresses defined in the custom address list. To add addresses, simply enter them into the provided window, separate multiple addresses with a

comma, and save the changes. The custom addresses are only active for the text filter which the addresses are tied to.

In addition to the 'addresses' option, the 'Notes' option allows for any particular notes to be applied to the text filter. Notes does not modify the function of the filter, but is provided for convenience. To modify the notes field, simply enter text into the provided field. Make sure to save the changes before leaving the page to commit the notes to the system.

URL Filtering

URL Filtering is utilized by the Web Interface to block specified URLs from being accessed through the web filter. Any URL which has been specified will be blocked when placed in the URL filter and configured with a block action.



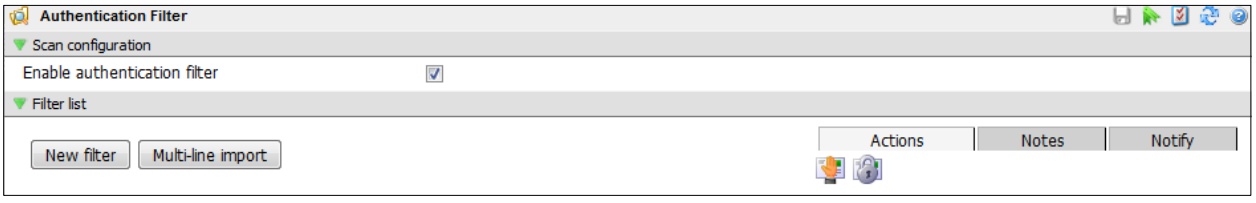
To enter a URL into the list, select the 'new filter' button and specify the URL. The syntax for specifying the URL accepts wildcards, but must match specifically, or the URL will not be detected. For instance, in order to block gwava.com, the URL could be entered in two different ways:

- http://www.gwava.com*
- *gwava.com*

The use of the asterisk is to guarantee that the URL is completely blocked. Though other forms may be utilized to block specific sections or services from sites, these are the recommended forms.

Authentication Filtering

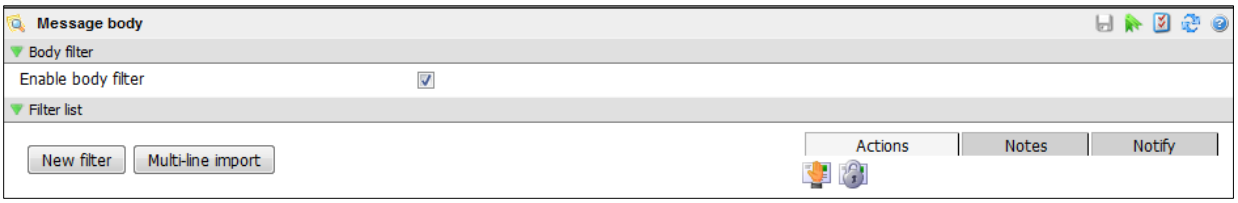
Authentication filtering is the process whereby GWAVA requires the user to authenticate to the proxy to be able to access the internet. Once enabled, all users are required to authenticate to gain access. To deny access or set specific actions to a specific user, add the user to the filter list.



To enter a user in the authentication filter, select the 'New filter' button and enter the user's name. Select the different actions desired for the specified user and save changes.

Body Filter

The body filter used for the Web Interface works the same as the body filter for message scanning, except that the Web Interface scans requested web pages for key words. The end effect is the same in that offending pages are blocked.



To add a keyword or phrase to the body filter, click 'add filter' and enter the text desired. The body filter is not case sensitive. Save changes.

MIME filtering

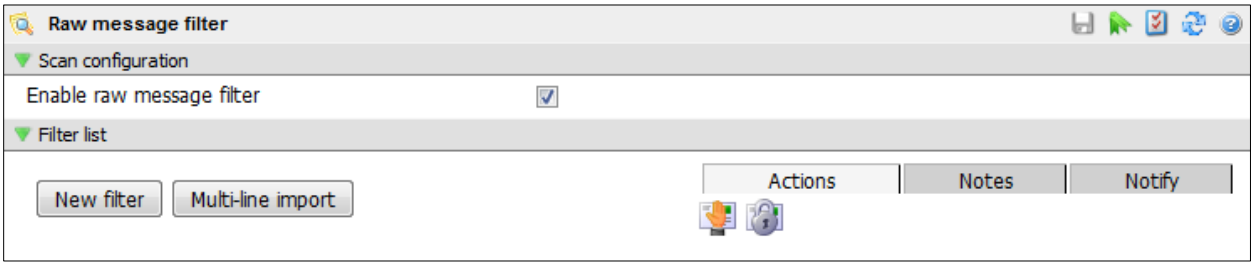
Every internet message passing through the mail system comes through as a MIME file. MIME filtering scans the message in its basic raw form, the MIME file, for patterns matching any filter specified by the Administrator. GWAVA does not come with any raw message filters pre-configured. The MIME filters work in the same way as the text filters do for events and options.

To create an effective MIME filter, the original MIME file for an offending message must be examined to identify a string or variable to create the filter for. Any line or variable in a MIME file may be subject to a filter. Specify the filters in plain text. For instance, to create a filter to block out a specific character set; create a filter looking for '`charset=<desired character set>`'.

For example, '`charset=US-ASCII`'

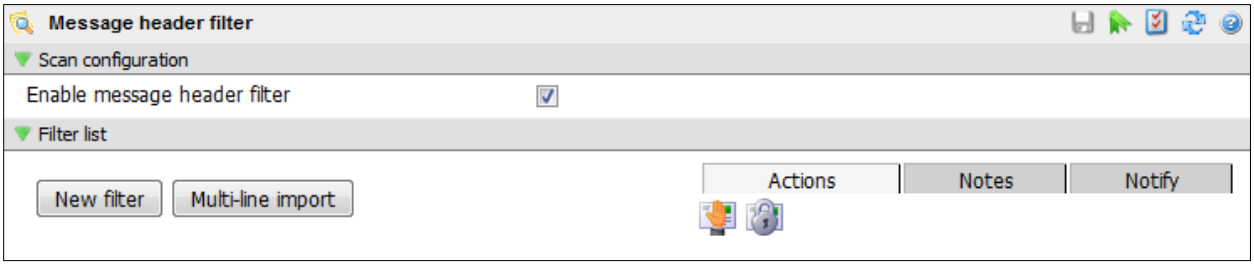
Raw

The Raw message filter searches the message section of the message MIME file. Create filters in this section to target variables in the message section of a MIME file.



Message Header

The Message header filter searches the header of the MIME file. Create filters in this section to target variables in the header of the MIME file.

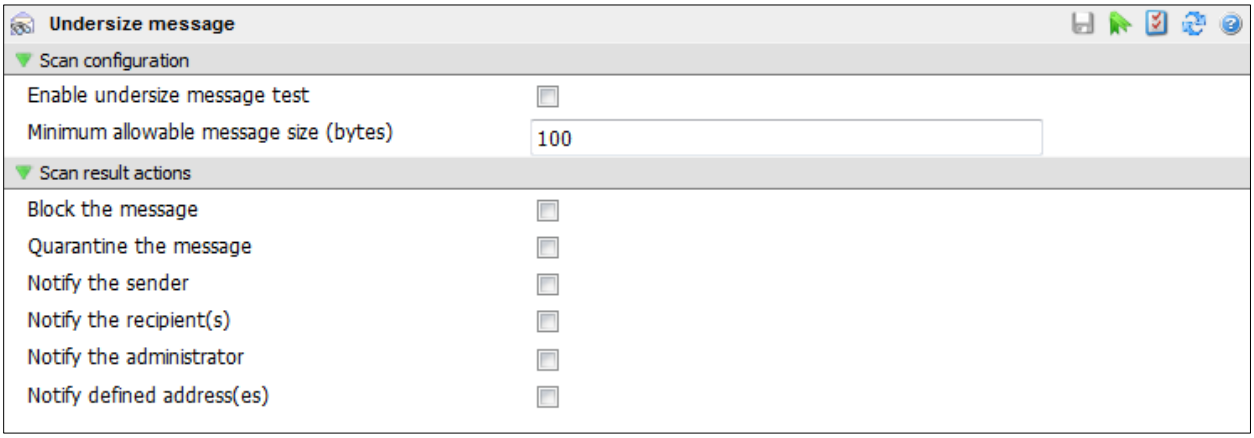


Oversize

The Oversize message event interface targets the total size of a message to make it subject to a block, quarantine, or notification. The maximum message size allowable is specified in kilobytes, enabled with a default of 8.1 MB. If you wish to allow larger messages through the system, increase the allowable size or disable the Oversize event.

Undersize

The Undersize message event is designed to filter incomplete message files or 'blank message spam'. It may also be used to filter all messages below the standard message size in the system. The default size is 100 bytes, and may be tailored to each specific system. This interface is not enabled by default, and must be enabled before it becomes active.



Fingerprinting

The Fingerprinting event interface works like a virus interface does, to identify the patterns of files for specific file types. This allows the fingerprinting interface to identify renamed .exe or other file types, and keep them from advancing through the system. See the Fingerprinting interface for defaults and all included file types. Additional file types cannot be added manually. Default actions for active file types are block and quarantine.

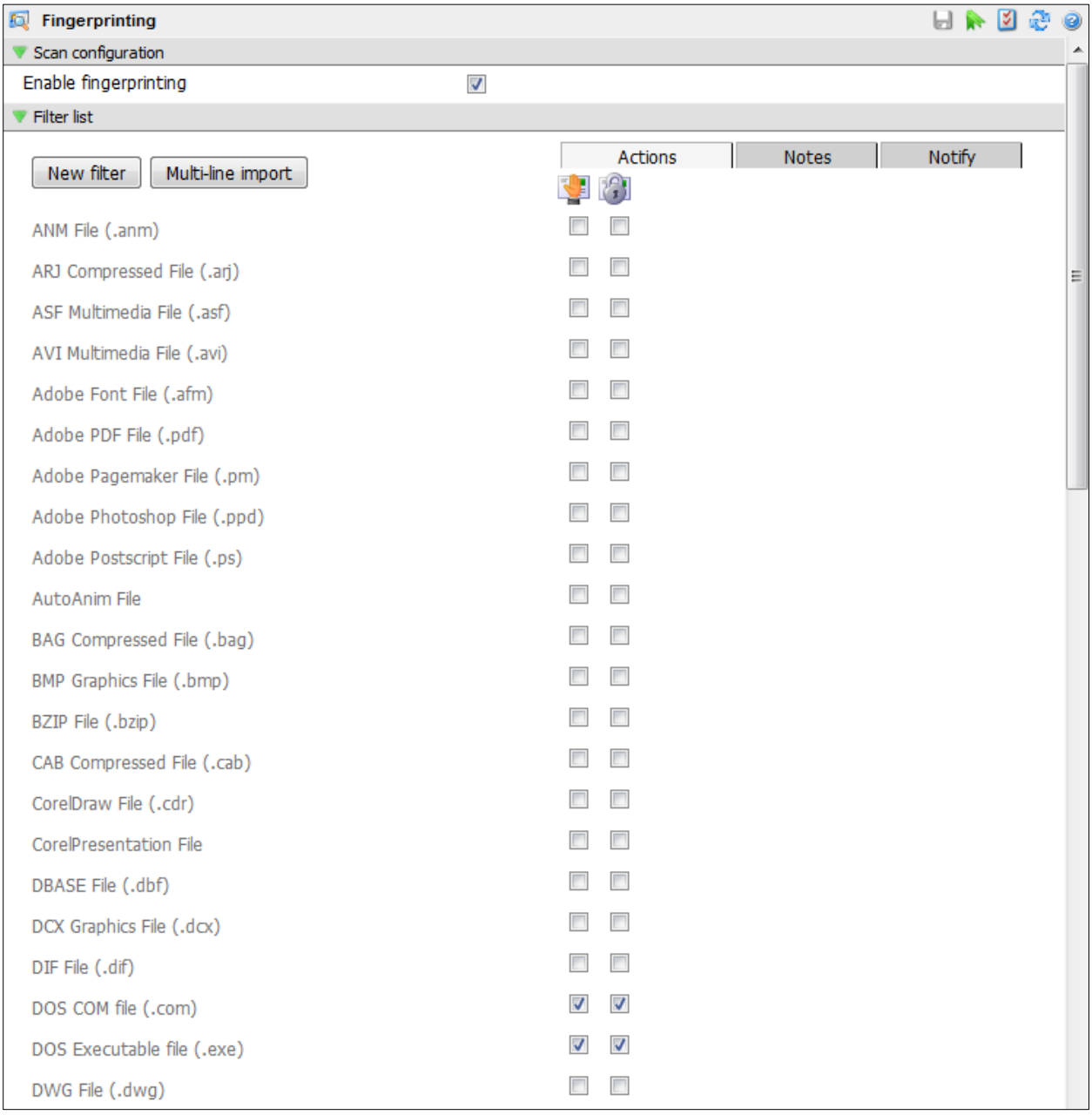
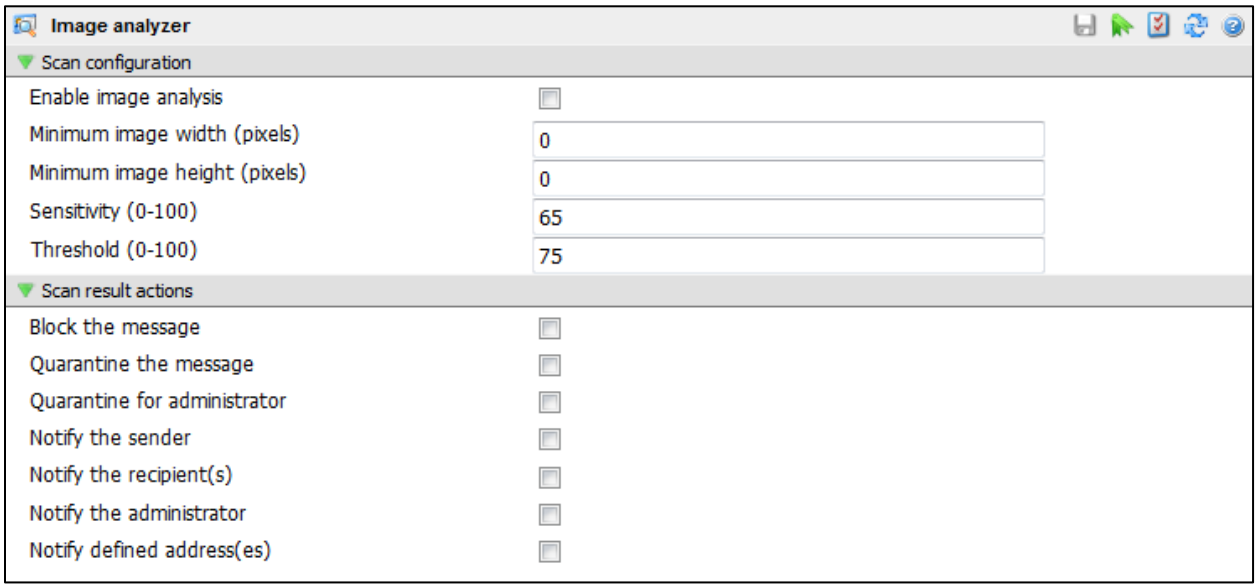


Image Analyzer

The image analyzer scans images in messages for illicit material. The image analyzer can be configured to check images of all different sizes. Default settings are shown. It is not enabled by default. Image Analyzer services are an additional service requiring an additional license to be purchased. Please contact GWAVA sales to acquire the Image Analyzer license.

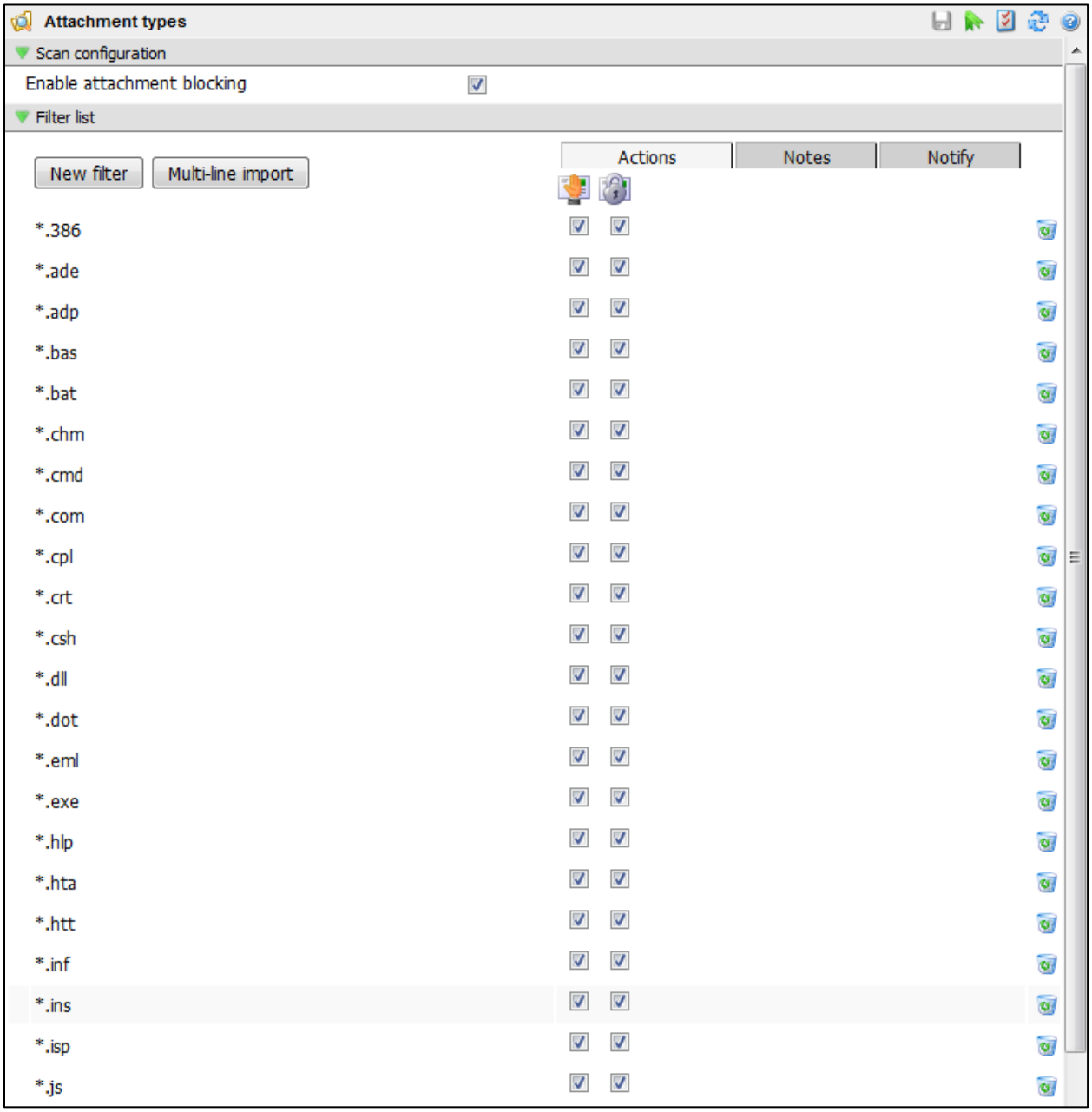


By default, the Image Analyzer is configured to flag any image of any size that matches a score level defined by sensitivity and then violates a threshold. The Image Analyzer scores images based on different criteria including skin tone colors, shapes, etc. all combined to generate the score. The sensitivity determines the detected criteria and therefore the score, while the threshold dictates at what score the message triggers action.

As with the other filters, the image analyzer can be set to block, quarantine, or notify, or all the above.

Attachment types

The Attachment types event interface reads the extension of an attachment and either allows or blocks the file depending on the extension. Because this is not dependent on the file's profile, as the fingerprinting interface does, additional file extensions may be specified as desired. See the Attachment types event page for default attachment types. For all default types active in the system, the default action is to block and quarantine.

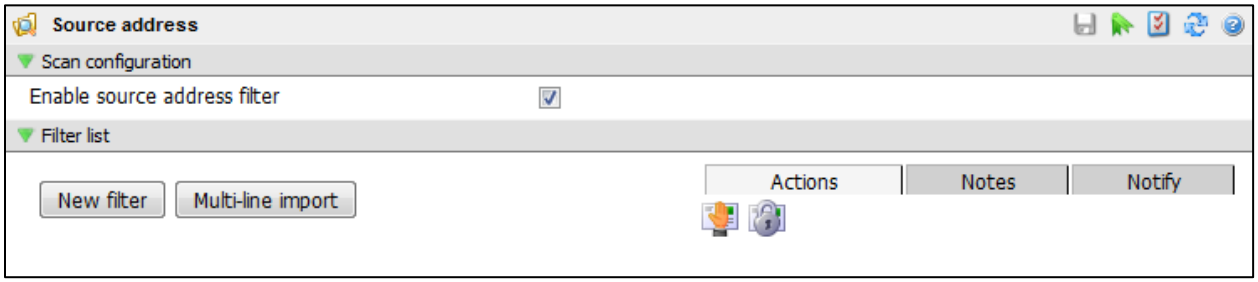


Source address filter (from:)

The Source Address event allows specific addresses to be specified for a block, quarantine, or different notifications. The Source Address filter searches incoming message's 'From:' address for a match with any specified addresses in the list. There are no default addresses in this list.

Wildcards are recognized, though not recommended unless an entire domain is desired to be blocked. For example, to block a single address, add the undesired "**username@domain.com**" as a filter and specify the desired action: block, quarantine, notify.

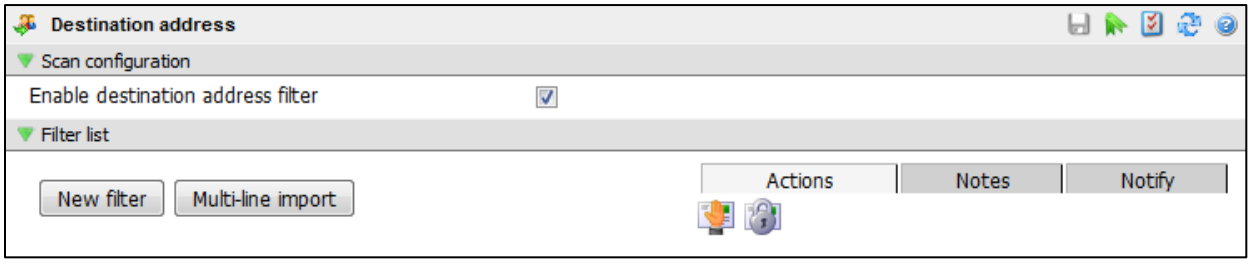
To block an entire domain, enter the undesired "***@domain.com**" as a filter and specify the desired action. A filter that specifies an entire domain, will act on all messages from that domain.



Destination address filter (to:)

The Destination address filter works the same way as the Source address filter, except for the 'To:' address instead of the from address. This can be used to deny specific users messages. Specify the address with standard syntax: "username@domain.com". This is useful for when an account is no longer desired to be used, or when a notification is desired for each time a message comes to a specific user.

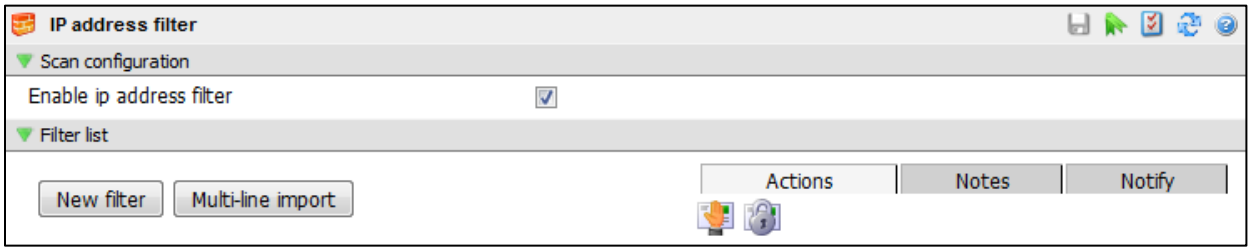
When notifications are set for a specific user, note that each time a message is sent to a specified address then the filter will fire and a notification will be sent, even if the message was blocked as spam. Every message is scanned by every enabled interface, (except for the SPF and IP reputation scans if they are configured for connection drop).



IP Address Filter

The IP Address event searches the message for a match to any specified address in the filter list. There are no default addresses listed. If any IP address contained in the MIME file matches one specified here, the selected event will be processed. Specify filters with the bare IP address desired.

For example, 192.168.56.21

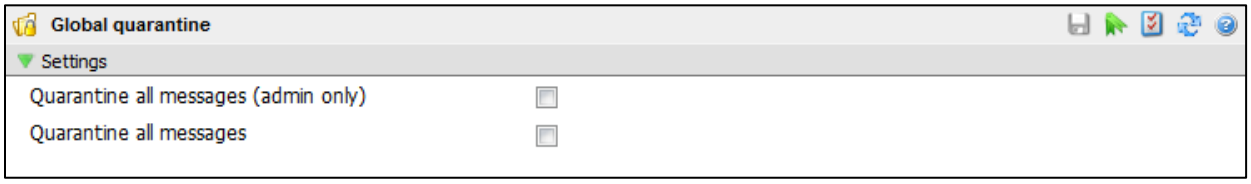


Message services

GWAVA can perform three general services for the entire message system. These services are performed on all messages passing through the system.

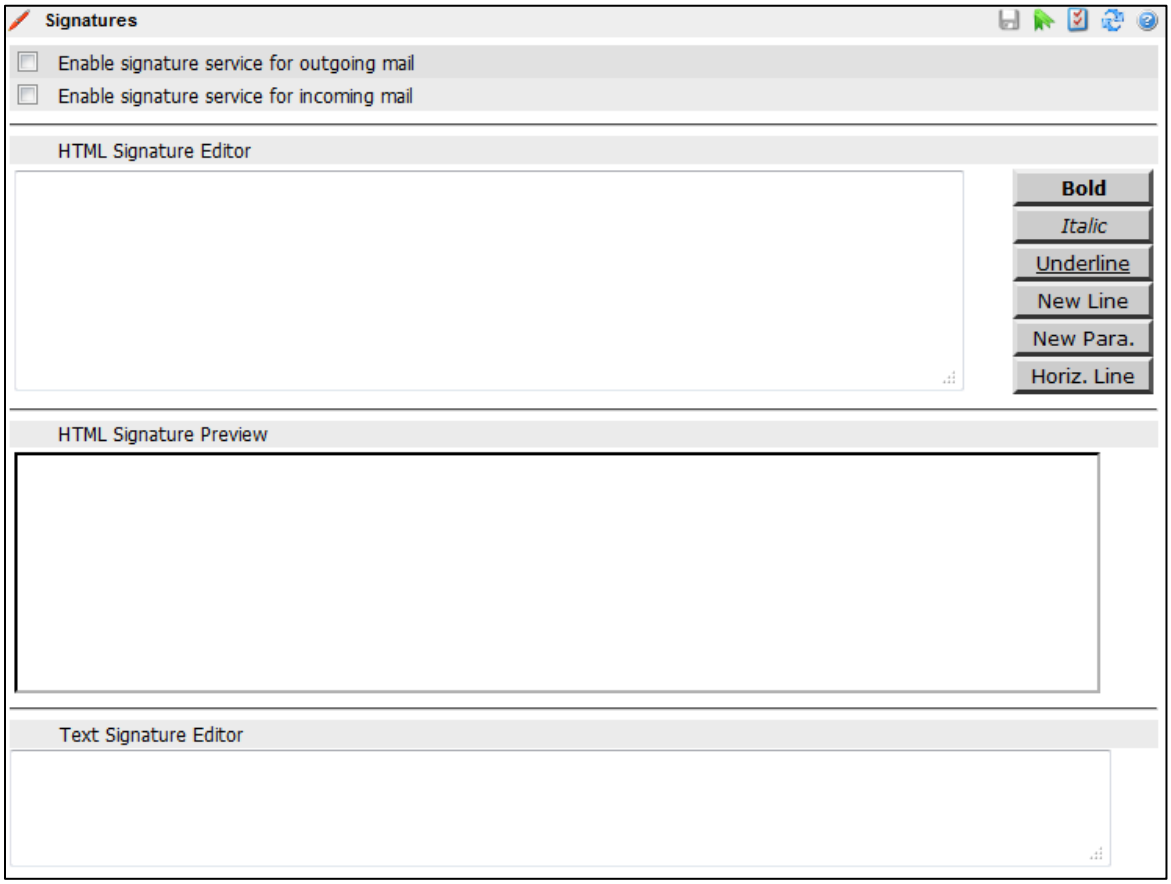
Global quarantine

The Global quarantine message service acts exactly as it sounds; every single message passing through the mail system has a copy placed into the quarantine. This option overrules all other settings in the system, including forced deletion of virus infected messages; a copy will be placed in the quarantine.



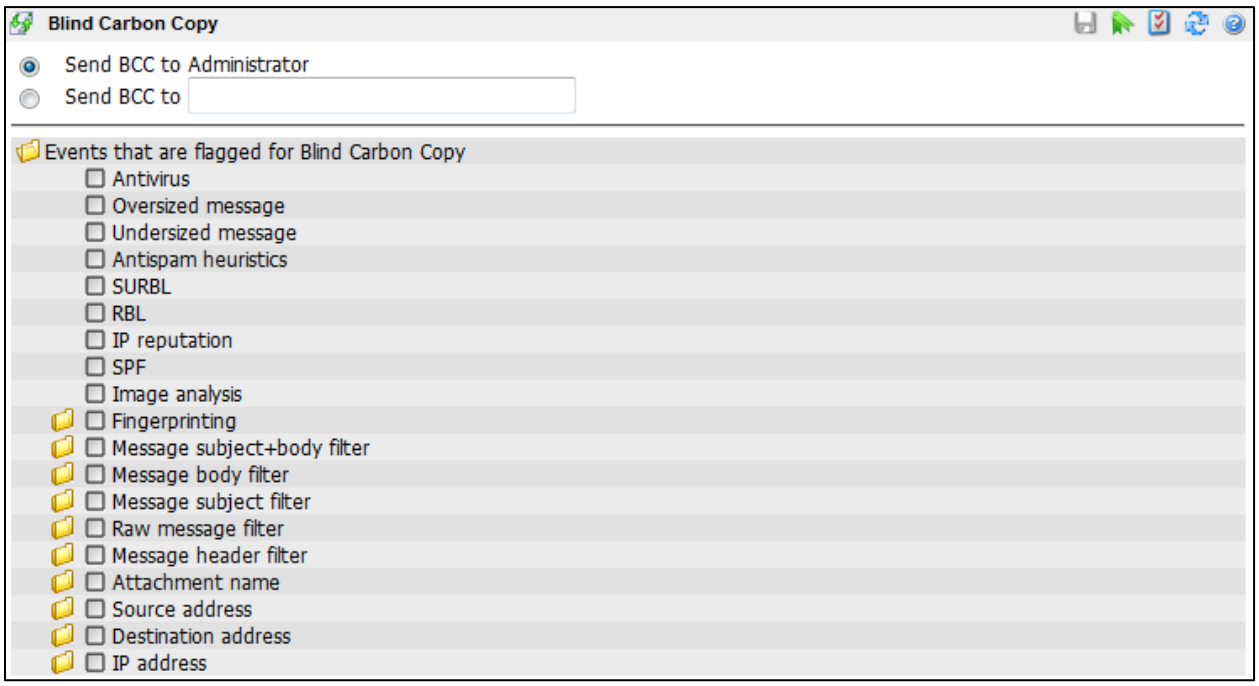
Signatures

The Signatures service instructs GWAVA to add any specified signature to the selected directional mail. Signatures WILL NOT WORK with POA interfaces. If incoming mail is selected, all messages coming into the mail system will have the signature appended to the end of the message. The same applies to outgoing mail messages. If selected, all outgoing mail will have the specified signature added to the end of the message.



Blind Carbon Copy

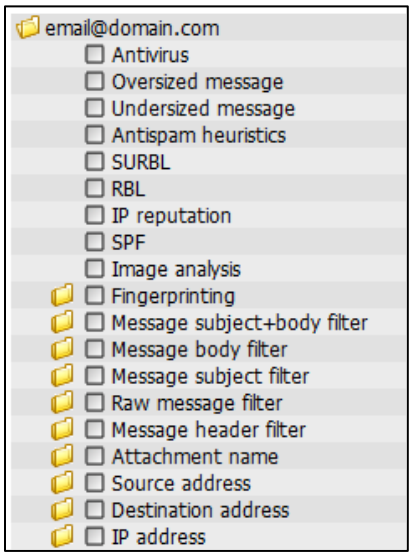
The Blind Carbon Copy event instructs GWAVA to create a BCC message and send it to the specified address. (If you wish to send to multiple addresses, an email group should be created in the email system.) This may be specified by a custom or default event, simply by selecting the event from the list provided. For instance; if an administrator desires to be sent a BCC each time a specific user or address receives a message, they may specify a destination address event, and then select that interface address under this list and specify the BCC address. After saving changes, the BCC will become active in a few moments.



Exceptions

GWAVA is designed to avoid needing exceptions. When using the Signature spam engine, there should be no reason to create exceptions on a regular basis, as caught mail will be due to a setting in one of the other filters. If mail is caught incorrectly by the oversized message, fingerprint, subject or body filters, or etc., the offending engine should be adjusted. Adjust the interface settings if exceptions are created regularly; the exception list should be used sparingly, when no other option applies.

GWAVA provides the option to create exceptions to the event interfaces, to allow specific messages or addresses to pass filters that would otherwise have blocked them. An exception in GWAVA consists of two main parts: the identifying item and the event interface(s) it is exempted from. Until you have specified both, the exception will not be valid and cannot be saved.



The different exception pages are essentially the same, though their function and syntax vary. Make sure you use the appropriate exception for each situation.

The exception menu items which have folders are expandable to allow the selection of specific filters inside each event interface. For example, this allows the creation of an exception from specific file types from the fingerprinting system, instead of the entire event filter, though the entire filter may also be selected.

If an expandable event interface does not have any filters, it will show a “No items found” notification. Since each exception adds time, though negligible, to the scanning process, only add necessary exceptions to the system.

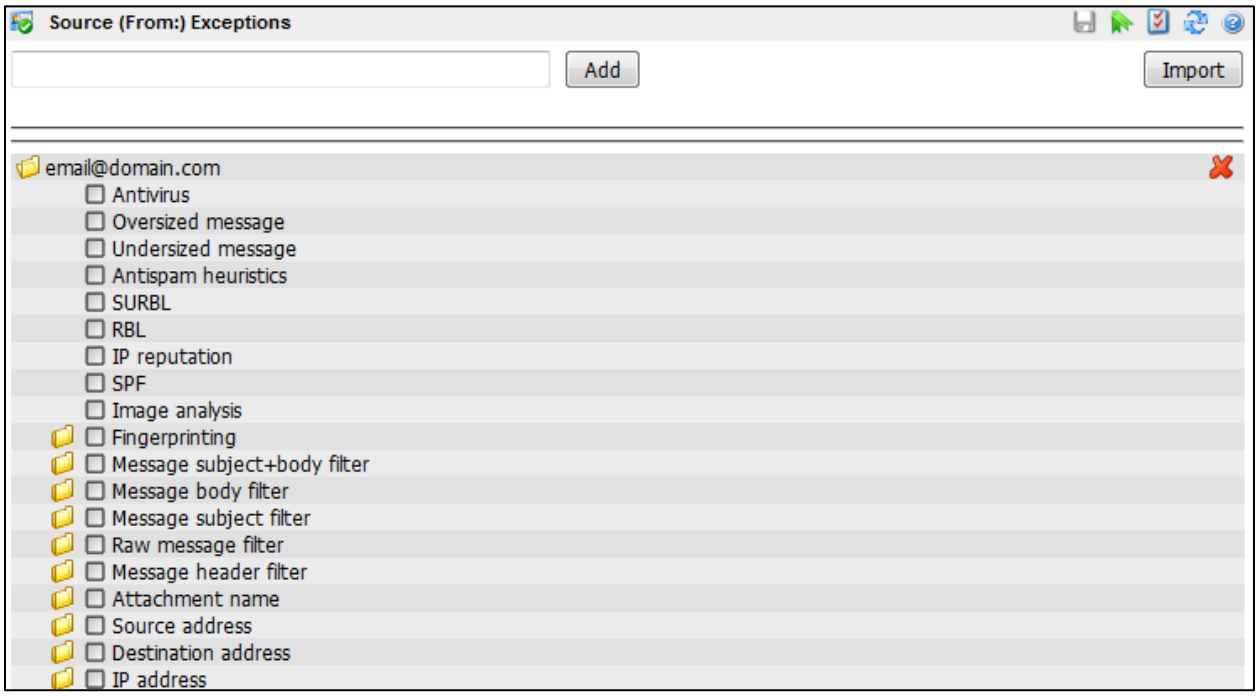
Source address (From:)

The Source (From:) Exceptions are based on the ‘From:’ address listed for the message. The majority of exceptions are created here, as it is the easiest exception to correctly create. Source exceptions are used to allow an outside address to pass by a specific filter or filters. These exceptions are specified in the following syntax:

```
user@domain.com
```

The address exception should exactly match the source address listed on the message. Source Exceptions also recognize wildcards, and, though it is not recommended, entire domains may also be specified. (For example, *@domain.com) However, if a simple wildcard is specified, such as *msn.com, then any message with ‘msn.com’ included in the address will be matched with the exception and will pass the selected interfaces.

After adding the exception, make sure you select an interface to apply the exception to, then save the change by clicking the colored disk to make the exception active.



Destination address (to:)

The Destination address (to:) exception list uses the "to:" address listed on the message to identify messages exempted from specific filters. Destination exceptions are used to allow a specific internal user to receive messages normally blocked by a specific filter or filters. For a destination exception to work, the domain the excepted address belongs to must be managed by GWAVA. DO NOT use wildcards with destination exceptions. Creating a destination exception allows all external mail coming to the specified address to pass the selected filter. If a wildcard and domain is specified here, all external mail to that domain will be exempted from the selected filter and spam will be allowed through. Use the same syntax as the Source Address exceptions. (Fore example, user@domain.com)

Message subject

The Message subject exception uses the subject line of the message file to identify and apply an exception. The Message Subject exception should not be used often, as repeated conversations are better identified by 'Conversation Tracking' (found under the Non-spam auto-learn section). The syntax is specified in plain text.

Message text

Message text exceptions search the text of a MIME file for matches to any specified exception. Regex and plain text are accepted. Specific and exclusive signatures are a good target for message text exceptions.

Message header

Message header exceptions search the MIME header for a match to a listed exception. Header exceptions should be specified with regex or plain text as found in the header of the message.

Message source

This exception searches the entire MIME file for specified text to identify a trusted server or mail source. This is used only when the identifying information is not in a specified place in the MIME file. Any message sent from the specified source will be allowed through to the system.

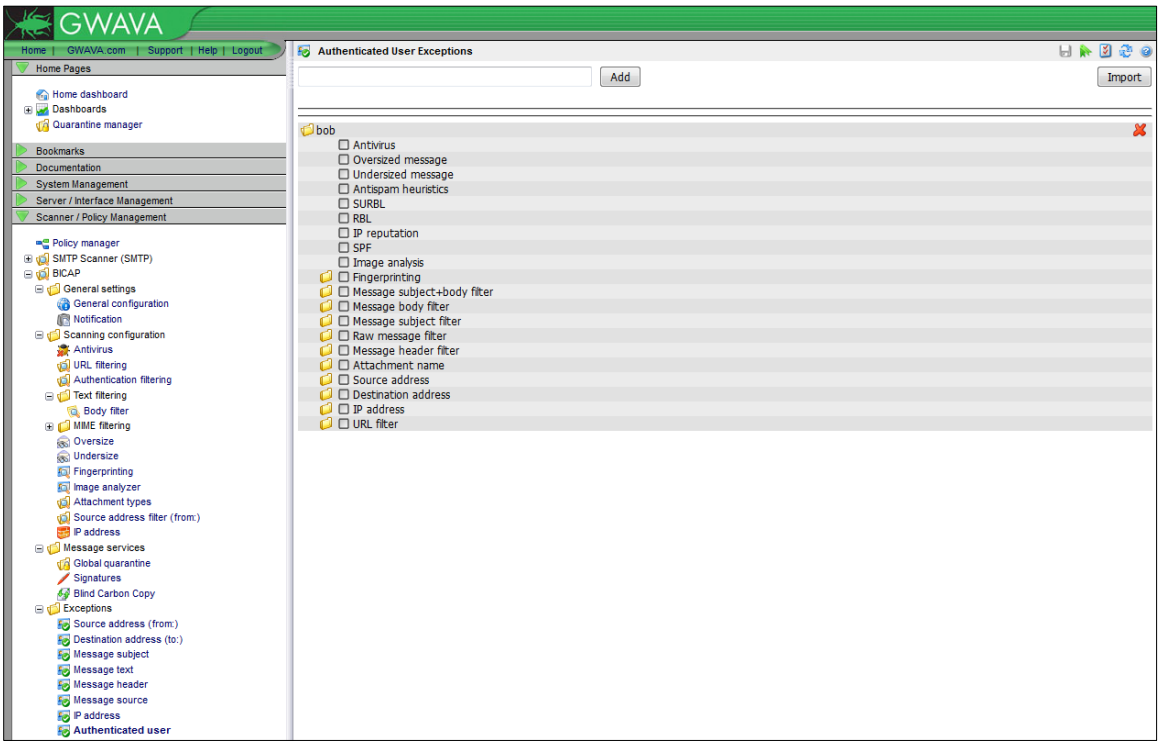
IP Address

The IP Address exception searches for a specified IP address anywhere in the message header. IP addresses specified in this exception list are considered 'trusted', and no messages from these IP addresses will be blocked.

Authenticated User

The Authenticated User exception list offers a chance for administrators to exempt specific users from Web Interface scanning criteria. This exception only applies to Web Interface scanners, as all other applications utilize the full email address. This option will exempt an authenticated user from restrictions placed on the Web interface due to the URL filter.

To add a user to the exception list, enter the user name into the 'Add' window and select the 'add' button. Once the user has been added, the URL exception must be checked and then saved.



GWAVA Quarantine system

The GWAVA Quarantine system has two different control levels for the interface: the general user interface, and the Administrator interface. When login credentials are passed to the Quarantine system, QMS, (Quarantine Management System), contacts the GWAVA management system for administrator accounts, and the GWIA for normal users. QMS uses a simple SMTP authentication to check for a valid user and password against the GWIA, so the same password used by system users is used to login to manage their personal quarantine. Admin users, setup in the GWAVA management console, should only use their username and password to login. Normal system users should use their full email address and GroupWise password to authenticate.
For example,

```
admin
password
```

-or-

```
user@domain.com
password
```

User interface

The User interface is different from the Admin interface in that the options available to normal users is extremely limited. Only the Quarantine and Options tabs are available, and they only contain data related to the logged-in user.

Only the mail sent to the operating user is shown, (unless specified by the administrator, only the mail sent to a user's email address will be shown; Administrators may specify more than one address to be managed by a single user). Users may be granted rights, or have them removed from the administrator.

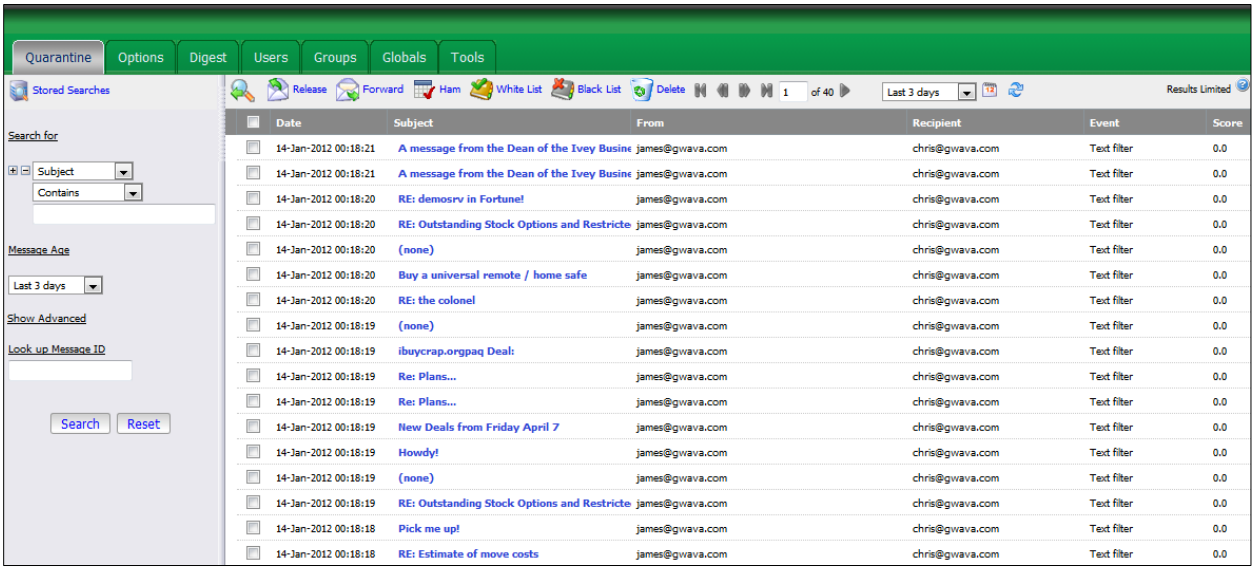
By default, the user's options tab offers specific login, timeout, whitelist, blacklist, and display settings for their specific account. Users do have the ability to whitelist and blacklist addresses; however, this ability only applies to their specific address, and does not affect the rest of the system. Any user's individual whitelist and blacklist is accessible through the administrator interface, and can be modified and managed by the administrator. The individual lists are located at **Options | Whitelist \ Blacklist | <select specific user>.**

Administrator interface

The administrator user created during the initial GWAVA user creation is the default account with administrator rights to the Quarantine system. When the administrator account logs into QMS, the following window is displayed listing all, if any, spam added to the quarantine system in the last three days, by default.

Quarantine

The quarantine tab lists messages and message information. It is important to pay attention to the last two columns: Event and Score. The score is a threshold level for the anti-spam engine, and the event is the interface event, or events, which caused the message to be added to the quarantine. This information is critical to creating effective exceptions and fine tuning the scanning engine. The quarantine tab allows for the selection, white or blacklisting, forwarding, release, and searching of messages in the database.

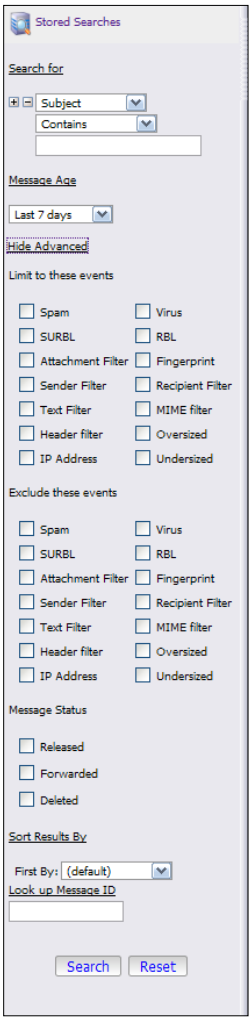


The search function of the quarantine tab provides multiple methods of specifying criteria to search the database. As with any search engine, the more information known about the target object, the more precise the results will be. There are two main ways to search; using key words or terms and browsing by categorical results.

Searching by key words or terms is the faster, more precise way to locate a message, but make sure that any key terms provided are spelled correctly to avoid accidentally excluding the target object from the search engine. To begin a search on specified criteria, select the **Search** button.

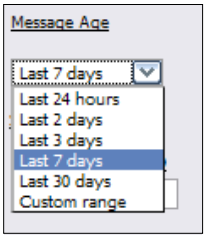
Searching by browsing through categorical results may seem tedious, but there are several categories which may be included or excluded to considerably tighten the search results. As with the key words and terms, ensure that any items excluded from the search results does not contain the target message as well. A combination of both methods may produce the best results on a consistent basis.

Search preferences and settings are specified on the Left side of the quarantine tab window. Expanding the **Advanced** criteria section allows the limiting to events, or exclude events from the search results. For instance, most messages in the quarantine will be caught by multiple event interfaces, which may cause the result list to bloat. Limiting the results to the oversize message event may help find the desired message, but if the RBL and SURBL event filters are excluded, the result list is significantly reduced, as any message caught by the oversize message filter and SURBL or RBL will not be shown.

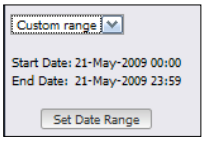


Message Status, (released, forwarded, deleted), are 'include' options which act the same as the 'limit to' events listed above.

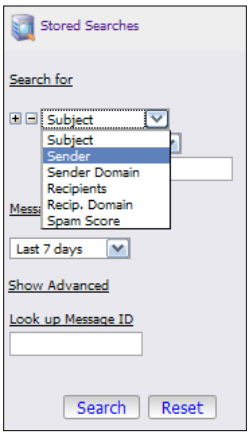
Sort Results by re-orders the results list by the selected option. Default sorting is by date.



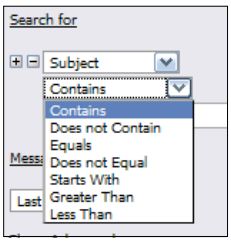
The Message Age is also a very useful criterion, which limits the results to a time frame. The date of any quarantined message in QMS is given as the time stamp set in the message MIME file. To set a custom date range, select the custom date range button and then specify the date range from the subsequent popup window. The window provides miniature calendar selection tools to specify the date range.



If the **Message ID** is known, (for example, from the message digest), the message ID may be used to immediately call up the desired message.



To specify a key word or term to locate the message, select the specific key word category at the top of the search pane. The search engine needs to know both where and what it is looking for. First specify where the search engine is to look in the database. The default search field is the 'sender', or the sender's user name/address. If the 'equals' is selected, ensure exact matching spelling to the desired criteria.



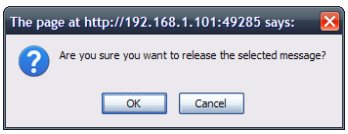
Using the **+** and **–** buttons, multiple search terms may be specified or removed from the active search.

Any search may be saved by selecting the "Stored Searches" icon at the top of the search pane. The **Stored Searches** function spawns a save or load window which prompts the user to either save, delete, or load any previously saved search sessions.

The toolbar across the top of the quarantine tab window provides functions to quickly manage quarantined mail. The magnifying glass exposes and hides the search window, and the other main tools are labeled.

Release

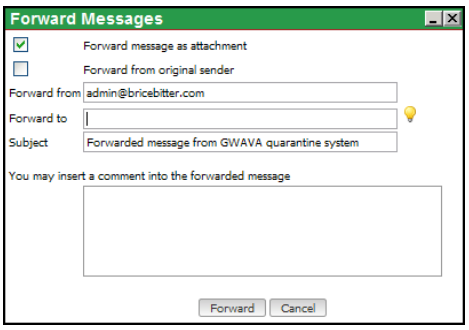
Releasing a message from the quarantine tells GWAVA to return that message back to the mail stream, where it will be delivered to the original recipient, unchanged.



Select a desired message(s) by placing a check in the associated checkbox, and then select the release button from the toolbar. Verify that you wish to release the message.

Forward

Forwarding a message from the quarantine does not automatically send the message to the original destination(s), but allows the admin to send mail to any recipient or recipients he desires.



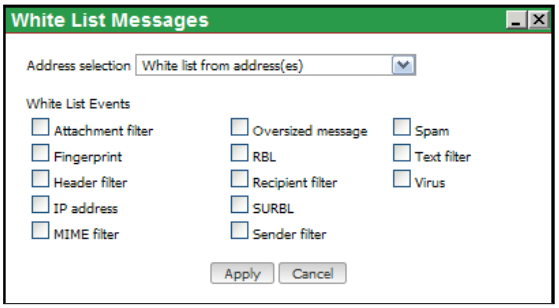
You may forward the message in the message body, or send as an attachment, as well as define the 'From:' field of the message.

Ham

The 'Ham' button reports selected mail as incorrectly identified 'spam' caught in the system. This setting only applies to the Signature spam engine, and will not have an effect on any other filter.

White List

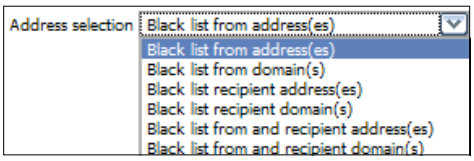
When a message is selected for white listing, the system is actually creating a source exception in the Management database.



As with all exceptions, white listing requires an address, and at least one event to bypass. Be sure to select the event which the message was quarantined for, plus all other desired events.

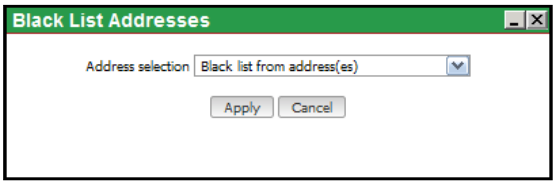
The quarantining event for each message is listed on the message row under the quarantine tab. The event column may hold more than one event per message, if there is more than one event listed, a drop-down menu will be available to display the different events for each message.

Both the white and black list options allow you to select different address options. These options correlate with different exception or black list types or entries. It is up to the Administrator which type of white list exception or black list entry to create.



Black List

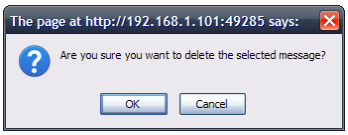
Black listing a message instructs the GWAVA system to always block messages from the Address selection (Source address, source domain, recipient address, recipient domain, or a combination of both the source and the recipient address or domain.)



Blacklisted addresses' or domains' messages are added to the quarantine.

Delete

The Quarantine Management system automatically deletes messages after the specified retention time. (Default is set to retain messages for 30 days – located under the **Globals | Pruning** tab.)



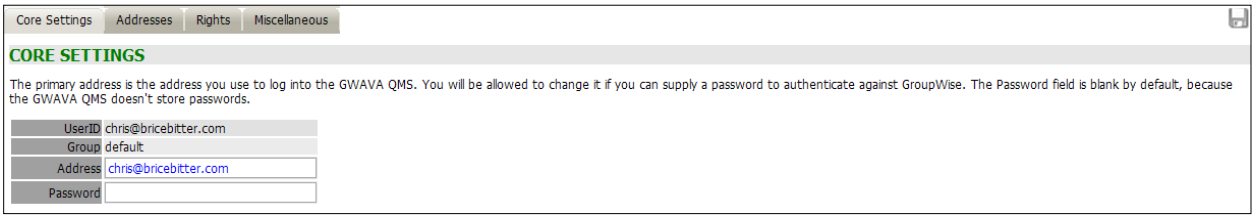
Because the Quarantine is set to automatically manage message age and database size, there is no reason to delete messages from the quarantine. Messages deleted by users will only be completely removed from the system if all destination users have deleted their copy. However, messages deleted by the Administrator will be completely removed from the system.

Options

Users and Administrators have access to the Options tab. User's only have access to options regarding their own address and quarantine settings. Administrators have access to everything by default, and as such, the only tabs in this menu which are useful for Administrators is the **Miscellaneous** tab, which holds account preferences, and the Whitelist and Blacklist tabs – which contain the whitelists and blacklists for individual users. These lists are not global lists, but only apply to the specific user who created it. To modify the user's list, select the user desired and view the list. Users will only show up in the system if they have received mail which has been added into QMS. Addresses may be added or removed from any specified user's list.

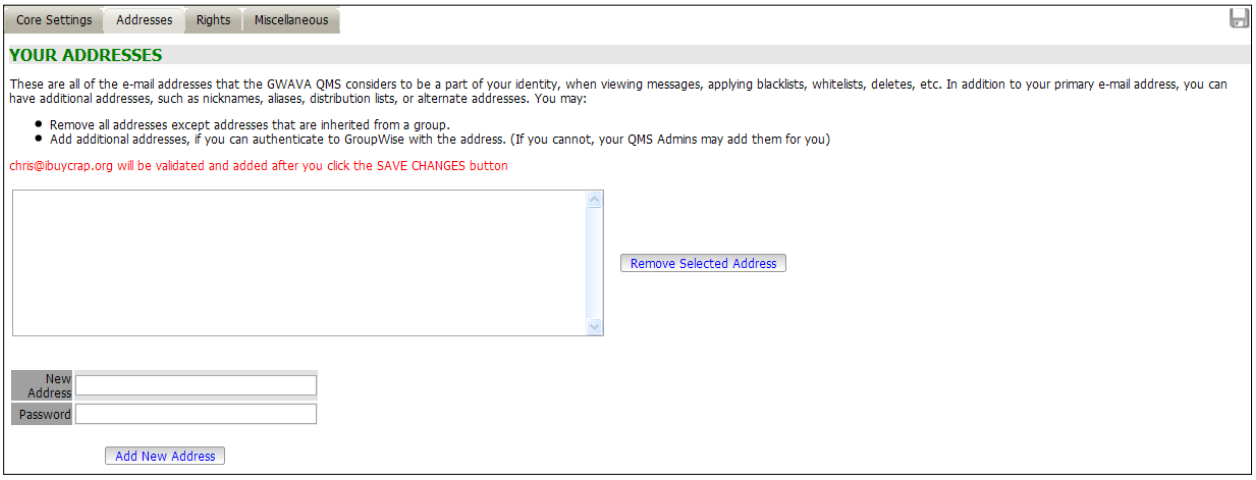
Core settings

The Core settings tab under Options, displays the basic information which categorizes the currently active user. The currently active user, the UserID, Group, and managed address(s), and password. (The password will either be stored in the GWAVA Management console (GWAVAMAN) or authenticated through the GroupWise system.)



Addresses

Users have the option to add a managed address to their account, which will add the managed address' mail to the quarantine results of the user who added the additional address. To add a managed address, a user must provide the desired address, and the GroupWise password for that address. If a user cannot authenticate to the GroupWise system for an additional address, the address will not be added as a managed address. The Administrator may add any address to any other address in the system without needing to authenticate. Administrator added managed addresses are configured under the Users tab.

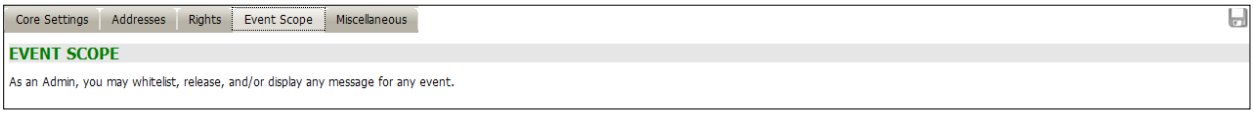


Rights

The Rights tab lists the rights to actions which each user has. Administrators have all rights. Users may be granted specified rights to manage mail by the administrator, or by virtue of group in which they reside.

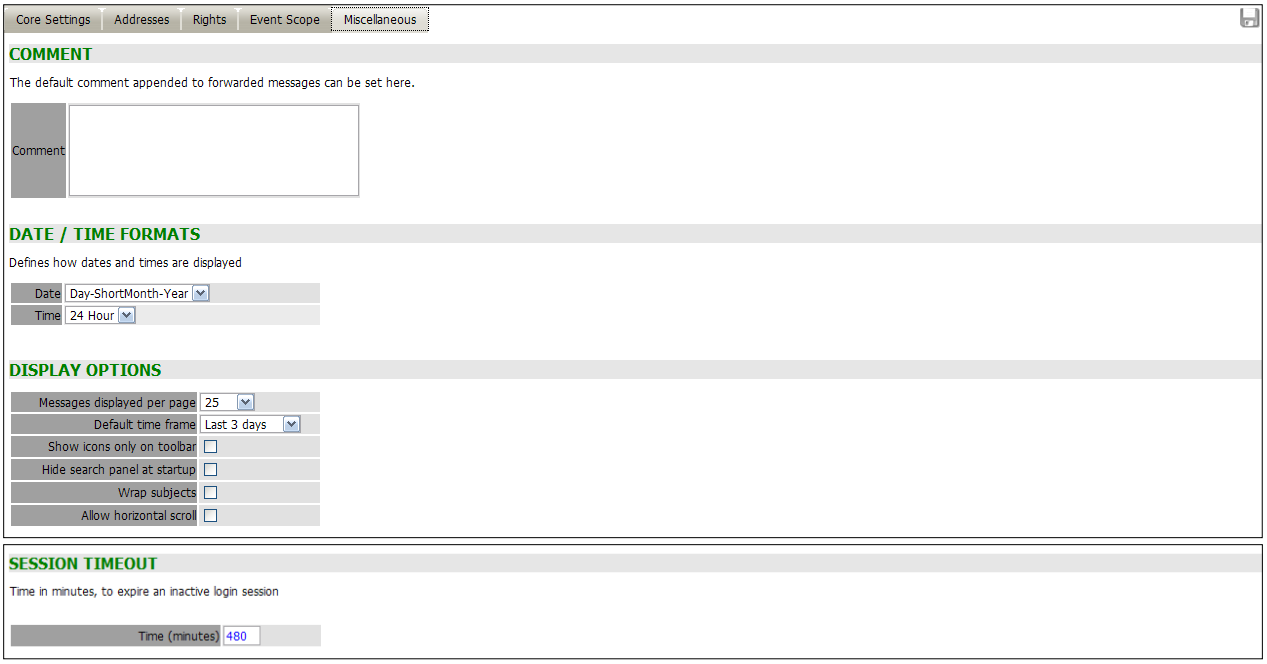
Event Scope

The Event Scope is an administrator level tab; users do not have this tab in their interface. Each user has rights to release mail by default. The Event Scope lists the release rights for the logged-in user. If a user has rights to release a filter type of mail, then any messages quarantined for that event will be available to be released to the receiving user. Admin may release any mail type in the system.



Miscellaneous

Account settings for the logged-in user are kept under the miscellaneous tab. The settings under this section are all available to be modified, as they only apply to the user's account. Forwarded messages may have a comment added to them as a default action, as well general configuration for the quarantine display.

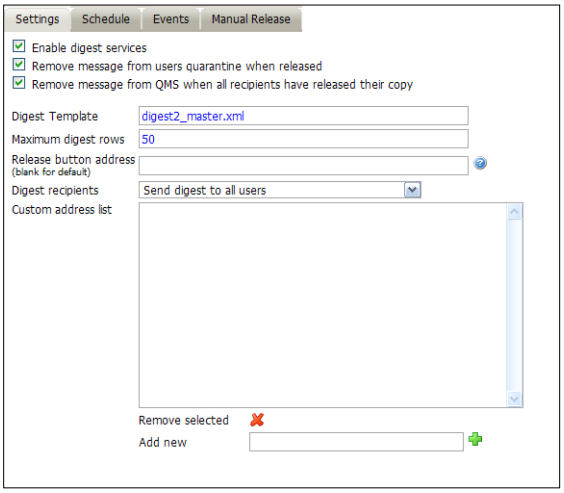


Digest

GWAVA can be setup to send regular reports to users when mail is blocked from a user's address. Messages listed on the GWAVA digest can be released directly from QMS via a web link for each message. A working digest setup requires three things: an enabled user list, schedule, and an event list.

Settings

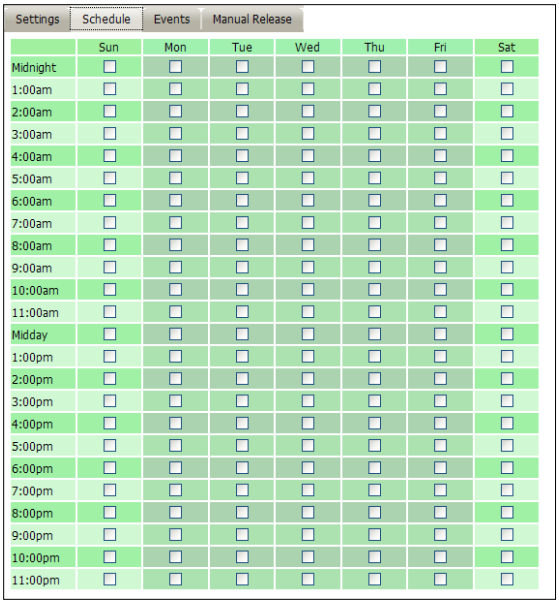
The digest service must be enabled before digests are sent. Message removal settings when a message is released from the digest, are set here. If the message is not removed after release, it is possible to re-release messages, resulting in multiple copies of the same message sent from QMS to the recipient.



By default, the digest service sends digests to all users. If you wish to specify digested addresses, or to exclude addresses from the digest, you may specify them in the custom address list, then select the appropriate digest recipients option from the drop-down menu.

Schedule

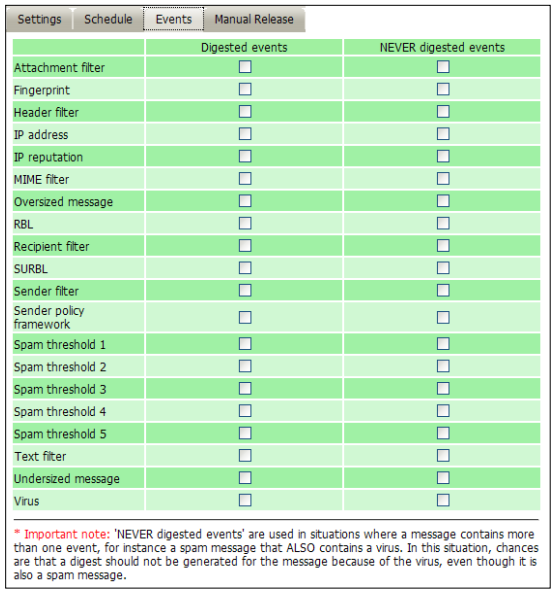
The digest service will be processed and sent to users on the schedule set here. A check mark in the provided boxes notes an active hour time. Only the provided times are available. Clicking on the time or the day, (8:00am, Mon), constitutes a global selection for that time or day.



A recommended setting for different offices and users is impossible, though a reasonable setting for the system would be to send a digest in the morning, after lunch, and finally an hour before users leave, to allow time to catch any missed good mail on the day they are processed. The digest process is not cumulative, and only messages added to the quarantine which have not been previously listed on digest will be on the next digest. So, in the previous schedule, only messages received after the previous day's last digest up to the morning digest will be listed on the morning digest, and only messages from after the morning digest to the after-lunch digest will be listed, &etc.

Events

Like the schedule, the digest must be told which events to list on the digest. Messages caught for an event with a check under the 'Digested events' column will be listed on the digest. **Messages listed on the digest can be released from the digest, even if the user does not have QMS rights to release that event.** If an event is listed on the digest, it is assumed that the administrator wishes to allow the users to release the messages listed.

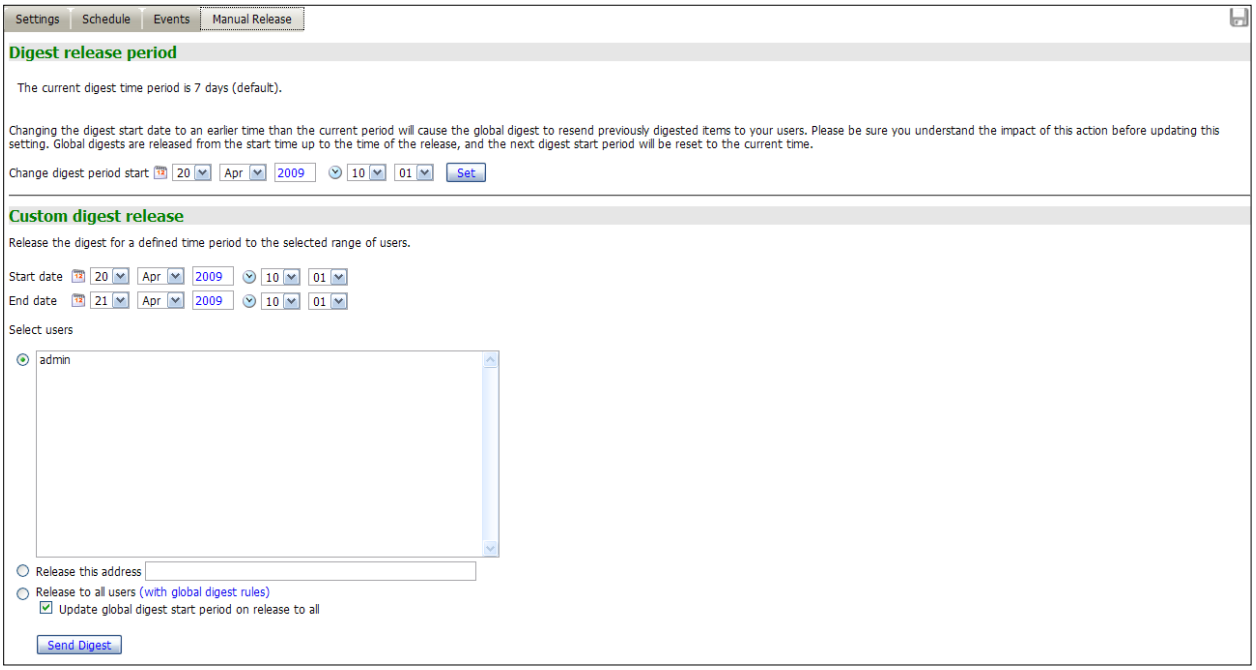


If a check is placed in the 'Never digested events' column, messages caught for that event will never be listed on the digest, even if it is also caught for a digested event. Selecting 'Virus' is an example of use for this section, (if viruses are quarantined), as a message with a detected virus will never be listed on the digest and cannot be released from the quarantine unless the user has QMS rights to release that event.

Manual Release

The digest may also be sent at any given time. The Digest works on a time stamp, which catalogs and lists mail in the quarantine if they are newer than the time stamp and fit the event list. Manual Release allows the admin to release a digest at any given time, by selecting the 'Send Digest' button. Sending a default manual release sets the digest time stamp.

The digest time stamp may also be manually set to affect the mail listed on the next released digest. This may be used to add additional mail to the manual digest. Select the time stamp desired and click 'Set'.



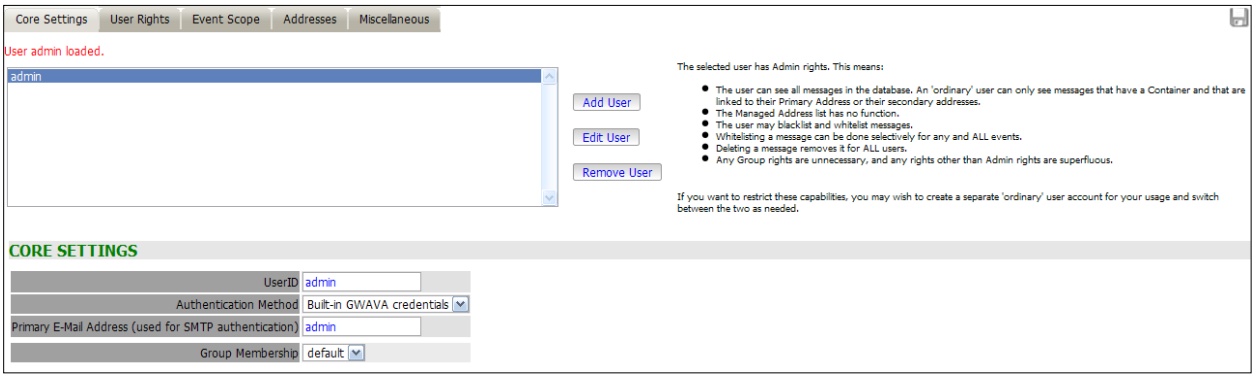
A custom digest may be sent to specific users, or all users, with a specific time frame. This bypasses the usual user list, and does not set the time stamp, unless all users are selected as the release group.

Users

The Users tab allows the configuration of different user accounts, their rights, managed addresses, and miscellaneous settings. Selected users have their settings loaded for each different tab, and are available for management. (Only users who have logged in or have been added by the administrator will be listed. If a desired user is not listed, you may add them by specifying the exact address of the user in the 'UserID' and 'Primary E-Mail Address' sections, then selecting 'Add User' and saving changes. The default setting for authentication is via SMTP. Group membership may be set as desired.)

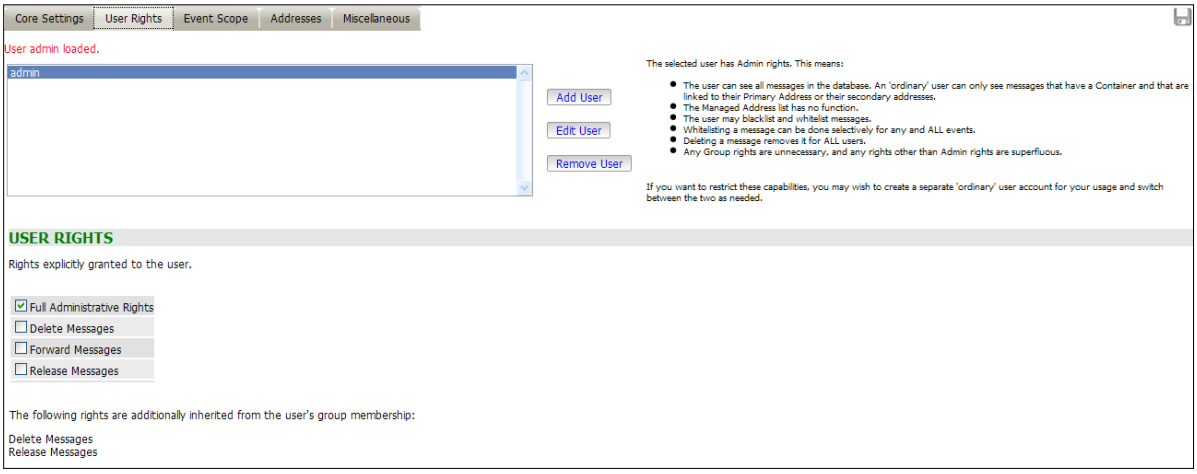
Core settings

The Core settings tab contains the basic settings for each user. The user ID, authentication, email address and group membership are all displayed. The authentication method is important to allow users to log into QMS. By default, the authentication for all users which are not administrators is to use SMTP authentication with the full address as the user name. If the GWIA is not available for SMTP user authentication, then the only authentication method which will work will be built-in GWAVA credentials.



User Rights

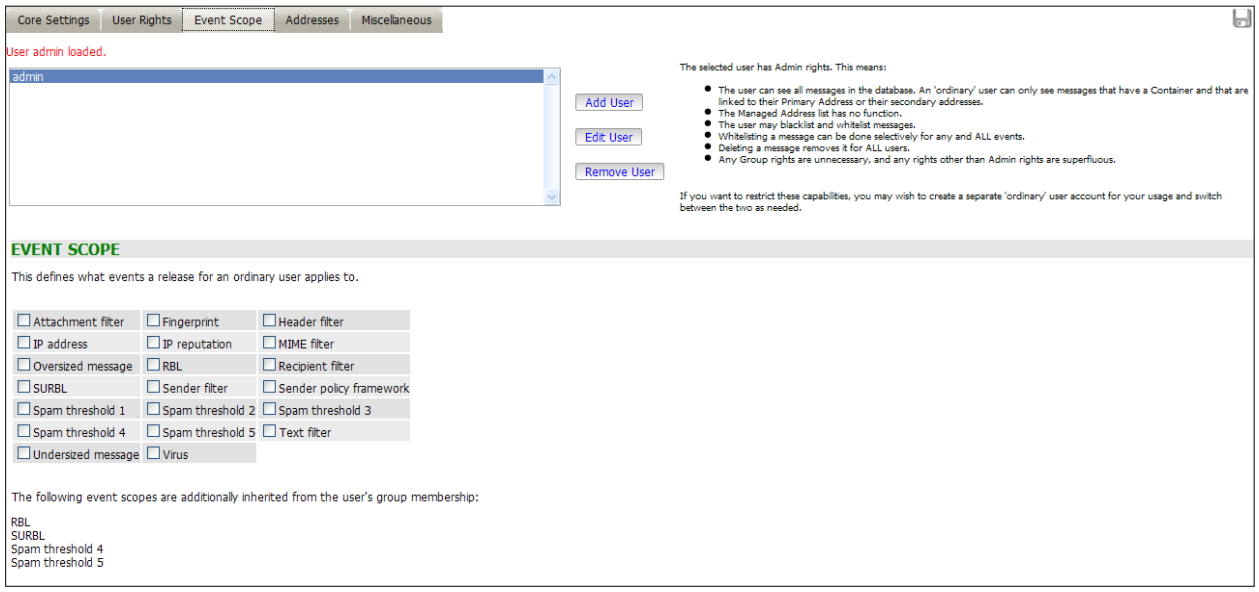
User Rights allows the administrator to modify and set rights for specific users in the system. User Rights provides access to the basic actions of a user in QMS; delete, forward, and releasing messages. Full admin rights can be granted to any user specified.



The selected user's rights are shown. If a user's right to delete or release messages is granted by the user's group membership, the user must be moved to a new group without those rights, or the original group rights must be modified to remove the undesired actions.

Event scope

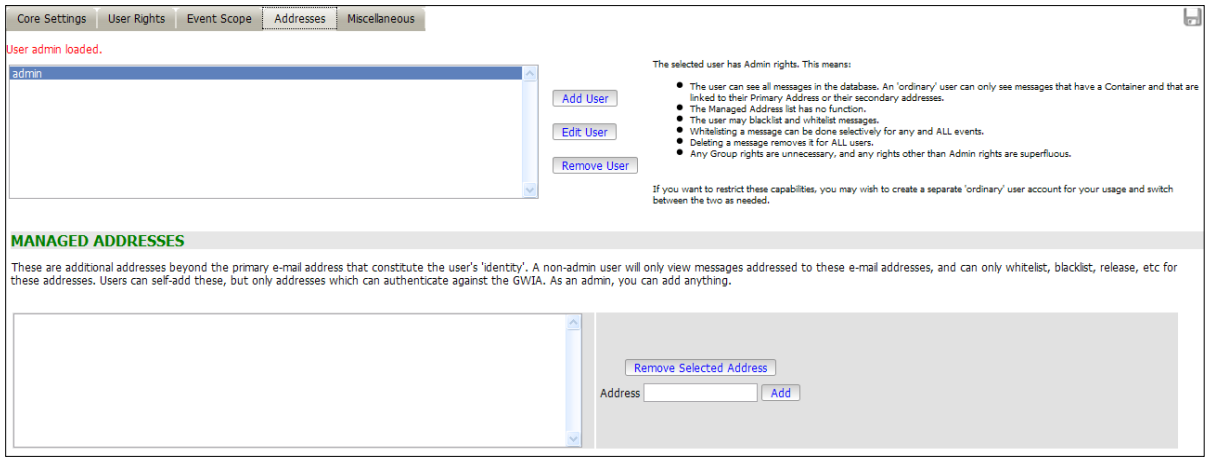
Each user can have specific rights to release messages which have been flagged for specific reasons. If, for example, a specific user may require the right to release messages flagged by the oversize message filter, while that may not be allowed for the rest of the users in the system. If a message has been flagged for multiple events, the user must have rights to release all events flagged on the message or the message will not be released.



Rights granted by group membership are listed at the bottom of the page. See the Groups tab to modify a user's membership to a group, or group rights.

Addresses

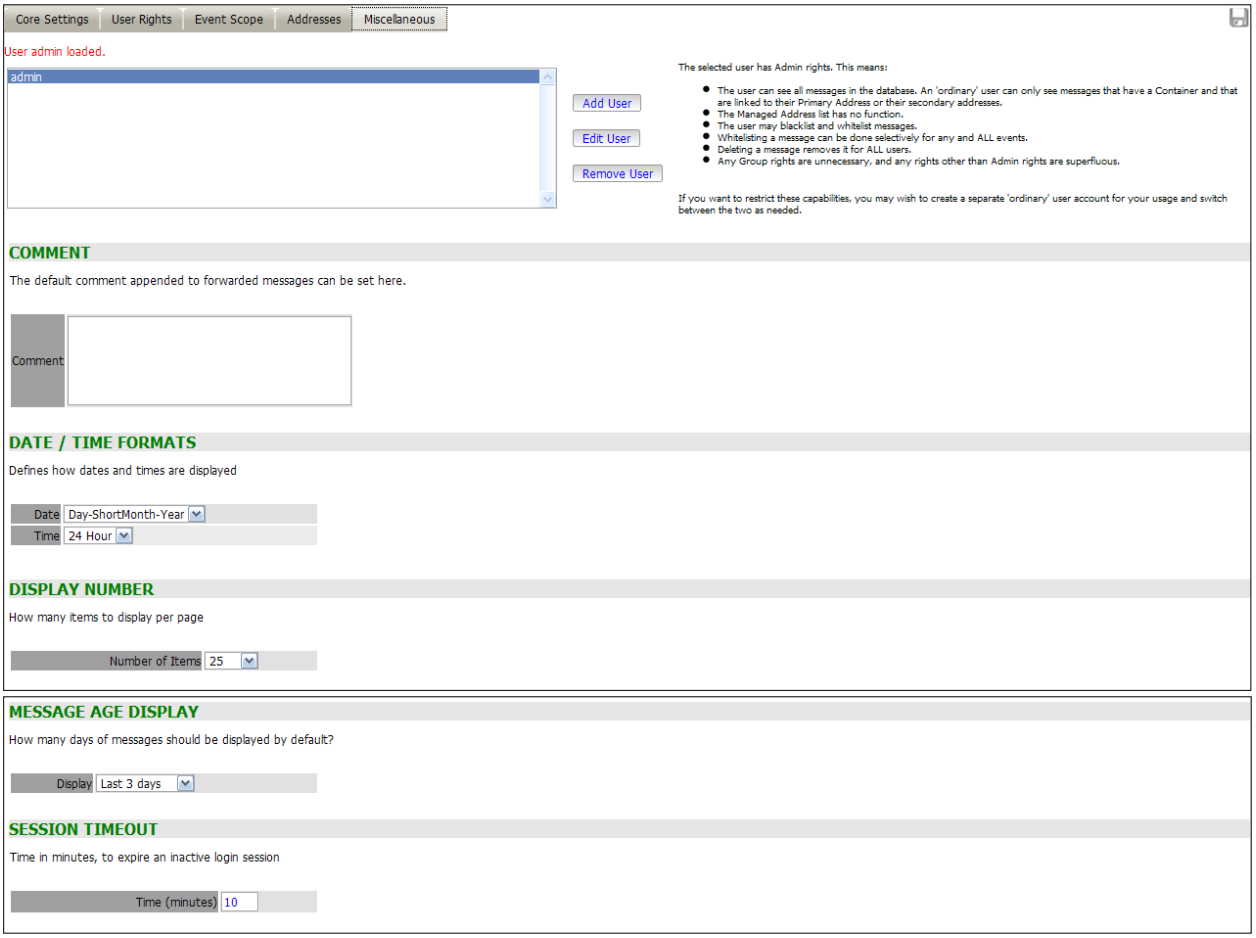
Any email address may be associated with any other user account in the system. This allows any user to modify and manage any quarantined mail for any address entered into the system, as that user would manage their mail.



This is especially useful for GroupWise systems which accept several different variants of a user name or different domains for the same user, allowing that user to manage all mail for their account in one location. As administrator, to add a managed address to a user, simply select the desired user from the user window, then specify the managed address(s) for that user in the managed address window, click ‘add’, then save changes. To remove a user’s managed address, select the desired managed address from the address window, and click ‘Remove Selected Address’ then save changes.

Miscellaneous

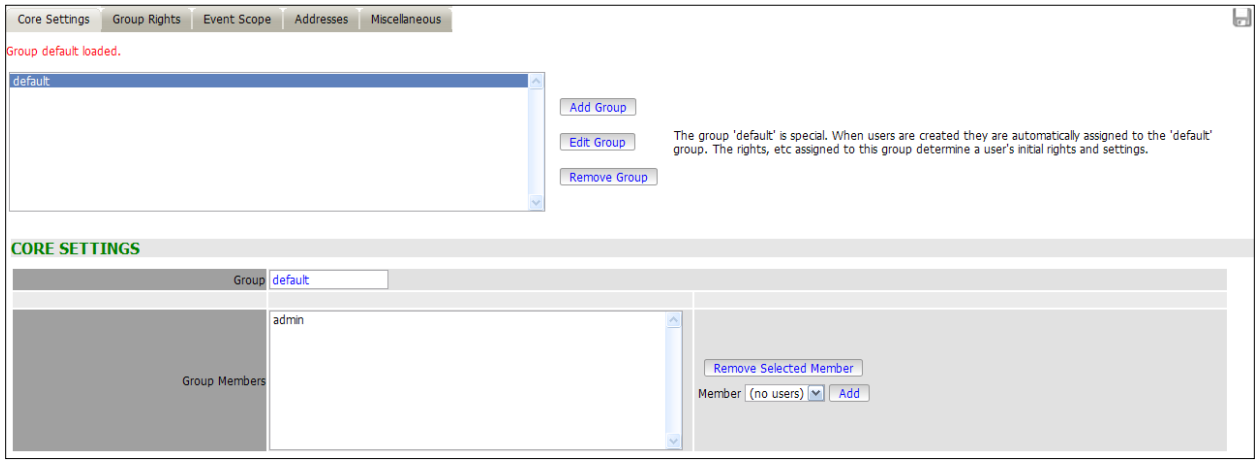
Miscellaneous contains the miscellaneous options for the selected user. These options are the same as those listed under the **Options | Miscellaneous** tab, and are self-explanatory. Any changes made should be saved before browsing to a different window or tab.



Group Rights

The 'Group Rights' tab is essentially identical to the 'User's Rights' section except that it applies to a group of users instead of a single user. By default, there is only one group in the system, to which every new user is added to by default. The default group is named, 'default'. Only users which have logged-in to the QMS system will be displayed in the 'Group Members' window.

To create a new group, specify a new group name in the 'Group' window under 'Core Settings' and select the 'Add Group' button, then save the changes.



User's may be added to any selected group, and must be selected from the drop-down window next to the 'add' button. **Only users which do not currently belong to a group will be listed.** If a user is to be moved from one group to another, they must first be removed from a group before they can be added to a second. A user may only belong to one group at a time.

The Group Rights, Event Scope, Addresses, and Miscellaneous tabs are identical to the 'User Rights' tabs of the same name, except that they modify the entire group, instead of a single user.

It is of note that these sections may be more useful than the individual 'User's Rights' tabs for large systems. Organizing a system into different user groups allows the admin to quickly modify and specify settings for multiple users and simplify the management process.

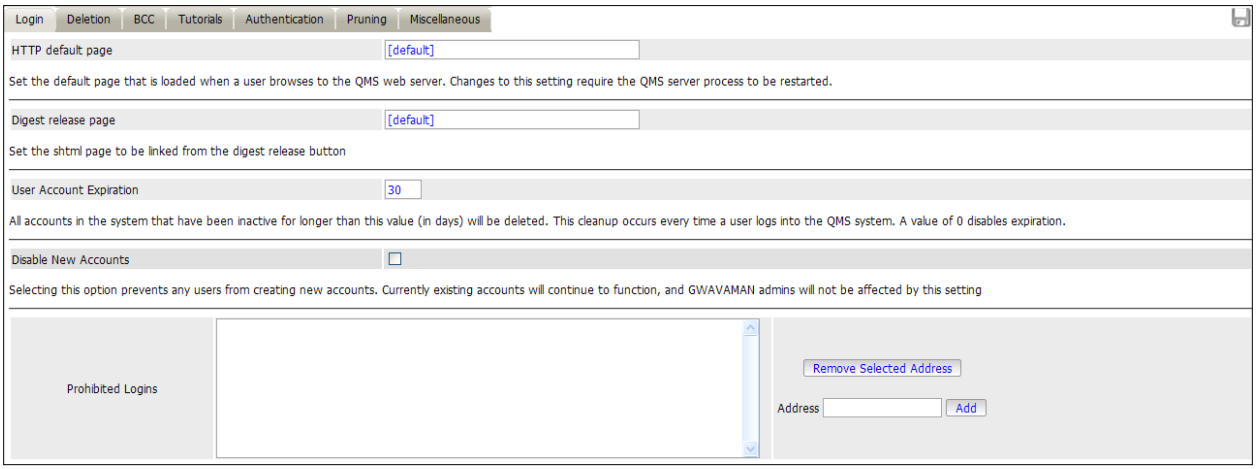
If a group address exists in the system, (for example, sales@domain.com), the admin creates a group for sales, and add the sales@domain.com address to the managed address section of the group. Having the group manage the address causes mail to that address to show up in the quarantine and digest for each user in that group.

Globals

The 'Globals' tab holds settings which affect the entire QMS system. Only administrators have access to the Global settings.

Login

The 'Login' tab allows customization for the QMS interface. If an administrator wishes to modify the HTML of the default pages, (found under …`gwava/services/qms/http`), they may use the original as a template, then specify their modified page as the default page. Modifying the HTTP and Digest release pages is not a supported function, and it is highly recommended to make a copy and archive of the modified page, as updates to the system may copy over any originally named pages present.

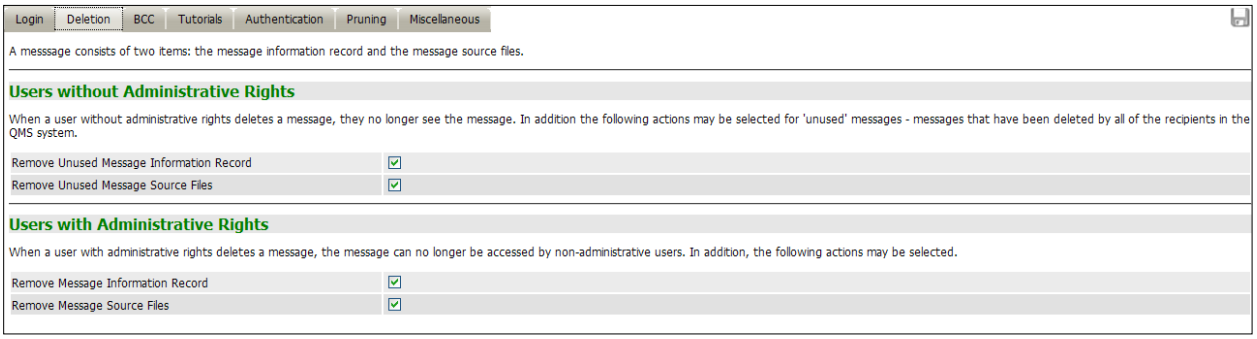


User accounts may also have an account expiration enforced, which will delete accounts which have been inactive for the specified time period.

The administrator also has the ability to restrict the users which have rights to log into QMS. If the 'Disable New Accounts' option is checked, QMS will not allow any users to log in if they are not in the established users list. If an undesired user is in the established list, enabling this option then removing that user from the user list will block that user from logging into QMS.

Deletion

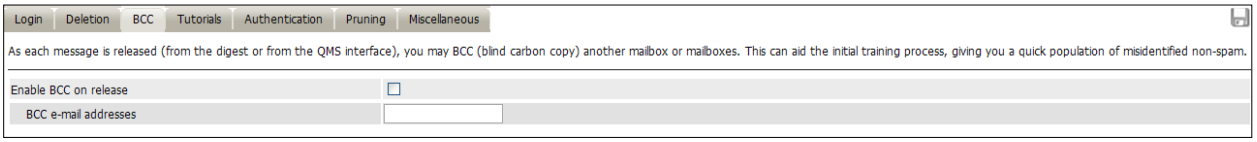
Globally, the ability to delete a message, and what happens to messages that are deleted, can be set here. By default, all options are selected. If an administrator wishes to keep all mail records visible to the administrator account, even after they are 'deleted' from user accounts, then they should uncheck both Remove the informational record, and the source files, so that the message is not removed from the main database. These settings can be for both administrators and non-administrator accounts.



BCC

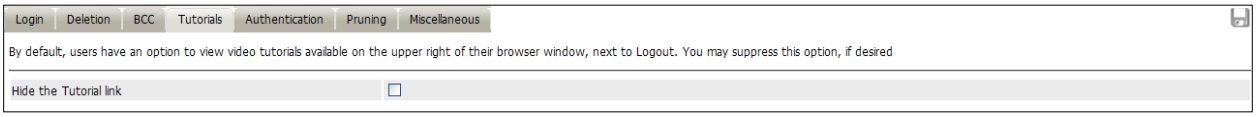
QMS can send a blind carbon copy to any specified address when a message is released. This can be used to monitor what kind of mail is released and for what reason. The 'training' offered by BCC is antiquated and is no longer needed for new systems running the Signature spam engine. Training options and use of BCC is held over for upgraded systems only.

To enable BCC, place a checkmark in the enable BCC box, then specify the desired destination address and save changes.



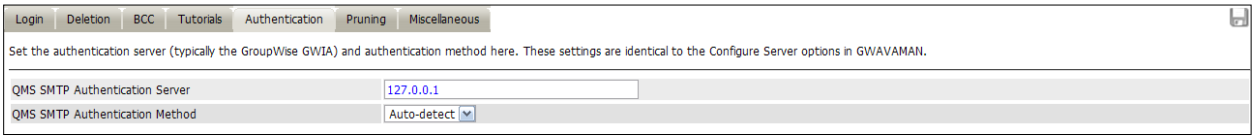
Tutorials

The link to the tutorials on how to use the system may be removed from the quarantine system. Checking the provided box and saving changes will remove this from QMS pages.



Authentication

The SMTP authentication address is specified here. The connection address to the GWIA or SMTP must be correct and open on port 25 for authentication to work correctly. If the SMTP requires a specific authentication method, select it below, otherwise leave the setting as the default 'Auto-detect'.

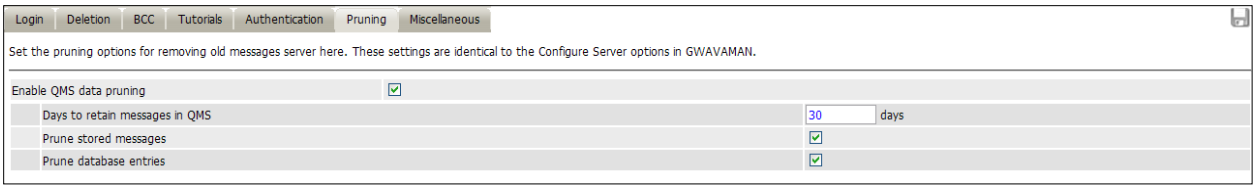


An alternate port for the SMTP may be specified, using a colon then the port number after the IP address, for example, for port 24, specify the address as follows:

```
10.1.1.100:24
```

Pruning

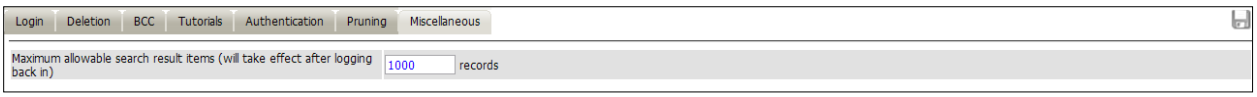
QMS is a light database system meant to service a revolving level of temporarily quarantined mail. The amount of mail kept in quarantine is usually specified by a time frame, in days, instead of size. Since it is assumed that mail sent to quarantine is unwanted, a generous default time frame of 30 days is set to allow users to access and release any wanted mail. All the rest of the unwanted mail will be permanently deleted from the system after it eclipses the age limit.



If messages and database entries are desired not to be removed from the system, uncheck the appropriate options and save the changes. Be warned, since QMS was not designed to be a long-term E-Mail archive, such use of the mail system is unsupported, and the database may become slow and unstable when the database size exceeds design considerations. Normal pruning of the database system will prevent instability.

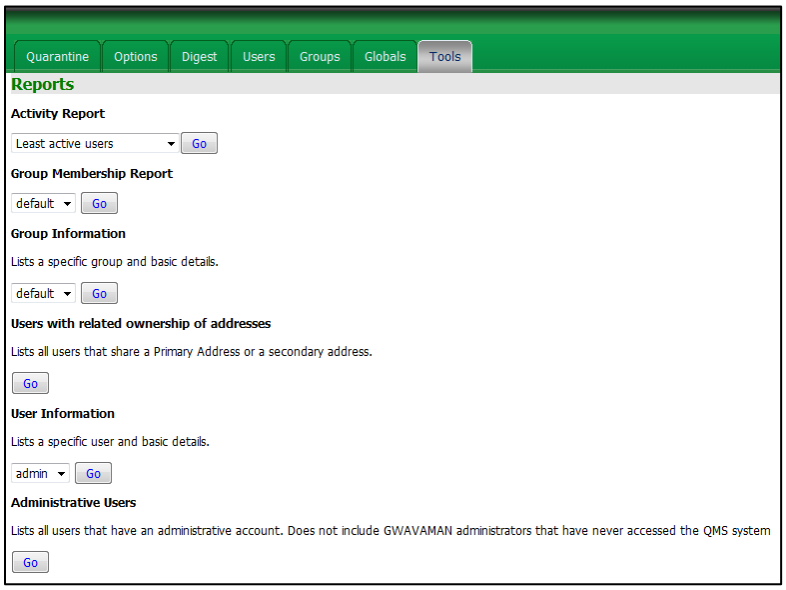
Miscellaneous

To keep the quarantine system from suffering under extensive searches, and to return results quickly, a maximum query number may be specified. No search function will continue after the specified record amount has been reached. The default is 1000. Search results above this number are unmanageable and waste system resources.



Tools

QMS contains tools to help the administrator manage and generate reports on the quarantine system. All tools are located here under the tools tab.



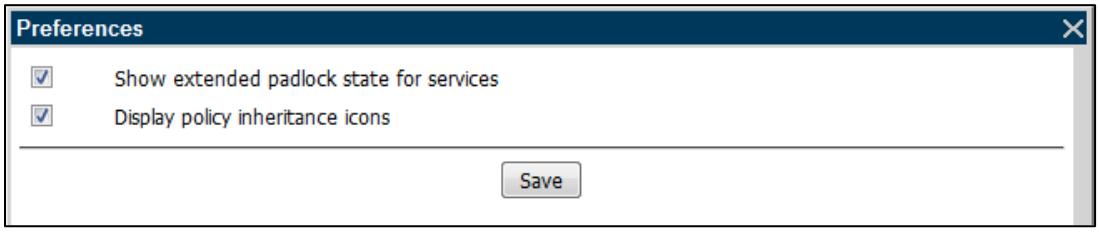
General information about the system can be gathered into a simple report by selecting the desired report type and then clicking ‘Go’.

Appendix

Padlock State Checkboxes

The locks you see next to the options are always visible on the Antivirus scanning settings, but are invisible, and unavailable to configure for the rest of the system, unless you enable the option "**Show Extended Padlock State Checkboxes".**

To Enable the checkboxes and Inheritance, you must have them set to display in the 'Preferences' menu, accessed through the preferences icon close to the save button at the top of the GWAVA Management window.



Select the options desired, select 'Save', then refresh the current page to expose the new options.

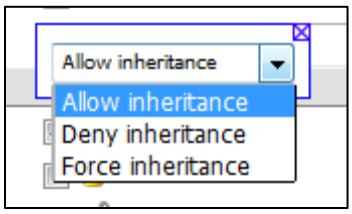
The four-state checkbox allows setting the 'gold locks' on any checkbox in the rest of the system. A closed lock indicates an overriding option. (This overrides any exceptions or settings in the rest of the system.)

Four-state locks are a powerful option and they are not standard in any area except in the Antivirus section. The image shown here is set to always block, but not quarantine, but the block is locked. For the events that these settings are active for, the messages will always be blocked, regardless of exceptions or other actions that are active on that message.

Policy Inheritance

Policies can be set to force their settings to every child policy below them on the policy tree. The Inheritance setting is accessed through the blue policy tree icon.

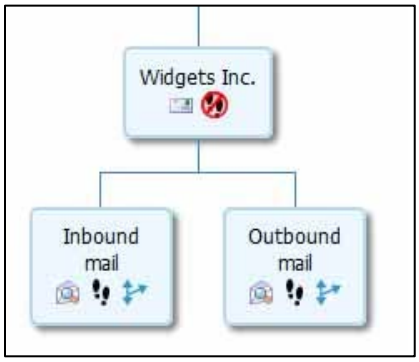
Selecting inheritance offers three different settings: Allow, Deny, and Force. Allowing inheritance replicates parent policy settings to the child, but allows the child policy to change those settings if desired. Forcing inheritance replicates the associated policy setting in the child policy, and child policies cannot change the setting. Denied inheritance does not replicate any settings from parent to any sub policy in the tree.



Scanner Configuration: Hierarchy and Inheritance

The GWAVA policy system includes a strict hierarchal system, complete with inheritance, to help in configuration of mail systems.

Scanning configurations in the policy tree, with sub-policies, parent policies, and root policies, creates an easy way to control message scanning settings for any particular message or group. Using this structure for the policy tree also may add an increased need for configurations in complex systems.

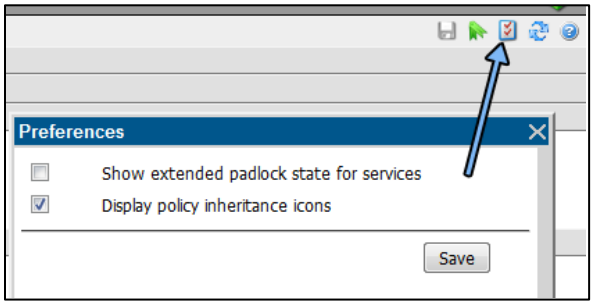


A simple example of this can come when separating inbound and outbound message scanning. In the example, Widgets Inc. has separated their mail scanning into two separate policies to independently scan messages coming into and leaving the mail system.

In the example, the inbound system is using antispam, antivirus and some attachment filters to prevent known and yet to be detected problems from entering the system. Outbound scanning is limited to antivirus and the same set of attachment filters.

The two policies are configured nearly identical, where the only difference is that only inbound mail is scanned for spam.

If, at a future point, a new attachment type must be blocked in both inbound and outbound mail, it must be separately added to the configuration of both the inbound and outbound policies. However, this is where inheritance becomes useful.

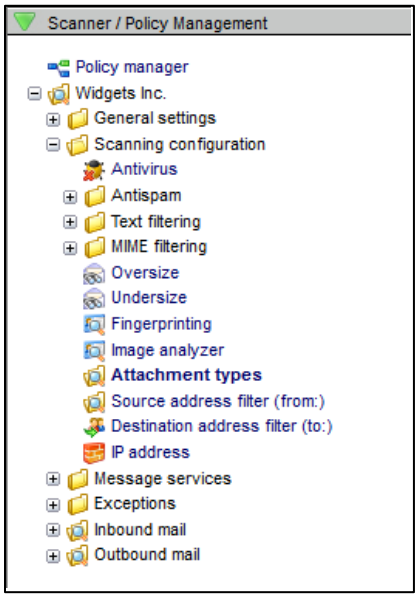


Scanner hierarchy configuration is usually hidden by default, and must be exposed before it can be modified. To access the hierarchy and inheritance settings, select the ‘preferences’ button at the top

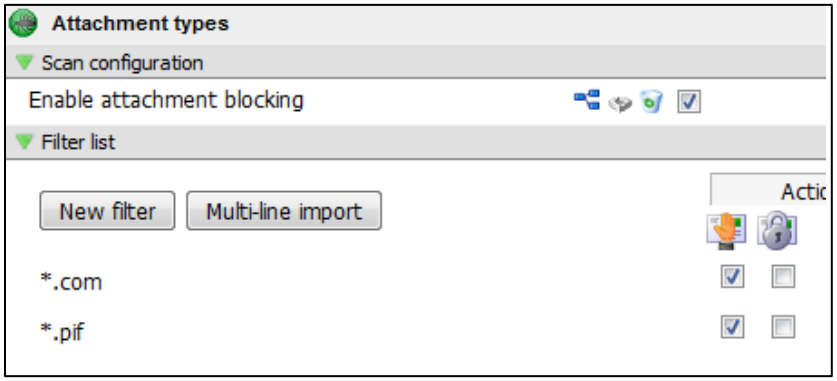
right of the user interface, and check the 'Display policy inheritance icons' box. Save the setting before closing the preferences box.

To apply the desired attachment block to both policies at the same time, the shared configuration components should be moved to the root or parent policy, the 'Widgets Inc.' policy in the example. To do so, the parent policy must have the 'policy contains scanner' option set 'on'. With an active scanner, the parent policy can now contain 'umbrella' settings which will transfer to all sub-policies the parent contains.

In the scanner view, the new attachment type can be added to the block list for the Widgets Inc. policy. These attachments types and items are to be blocked regardless of the message direction. To begin, add the forbidden items to the attachment type list. For this example, *.com and *.pif files are added.



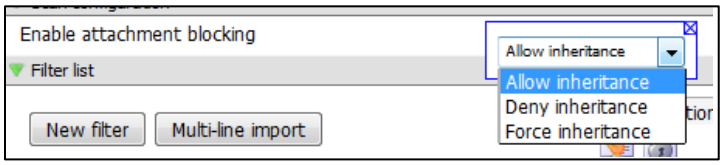
(Note that the subordinate, inbound and outbound policy's scanning configuration is located within the Widgets Inc. parent policy.)



While configuring this service, you will now see new icons which were exposed when the inheritance setting was enabled. The icons, left to right, are:

- Inheritance settings
- Inheritance status, (Not inherited is shown)
- Reset to default
- Enable service checkbox

The inheritance setting has three options.



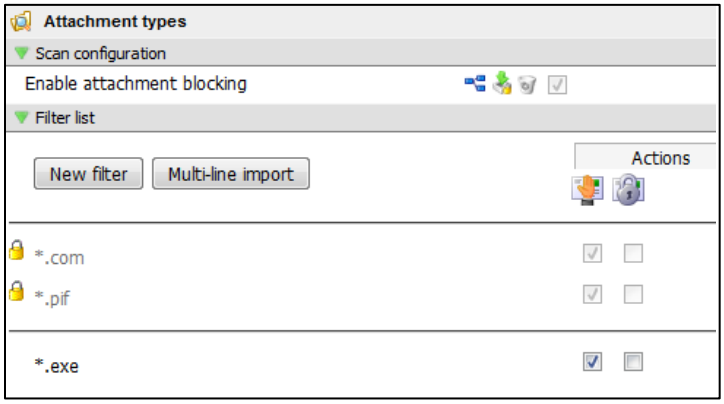
Allow inheritance: This is the default setting for every setting. Simply enabling inheritance causes the same setting to be duplicated through any and all child or sub policies, but still allows the sub-policy to have change this setting independently if required.

Deny inheritance: Denying inheritance causes the parent policy's setting to not affect the settings of any and all child policies.

Force inheritance: Forcing inheritance causes child policies to use the parent's configured policy. This is useful when certain scanning configurations must be followed, or a setting cannot change. All lower policies will be forced to accept and use the parent policy setting.

The example now shows the attachment type scanning enabled and the inheritance forced to prevent accidental disabling of the service later on.

After saving the settings, expand the 'Inbound' scanner and look at the attachment type settings which are in effect.



Because the attachment scanning was set in the parent policy, the same settings are inherited by default in the child policies. The grayed-out settings shown here are the duplicated settings from the parent.

Because the attachment filtering was setup at a higher level, and the setting was configured to 'force inheritance' in the parent policy, enabling or disabling the setting is ‘locked’. This is indicated by the yellow padlock. Because it is grayed-out, these settings cannot be changed or configured at this level. The inheritance icon also includes a green arrow, indicating that this setting was inherited from the parent policy.

All of the grayed-out items are locked and cannot be manipulated here, because they are set in the parent policy. However, simply because the setting is locked does not mean that additional filters cannot be created and enabled. For the inbound filter, an additional file type has been added, the *.exe filter. This filter is only active for the inbound, and is not replicated in the outbound.

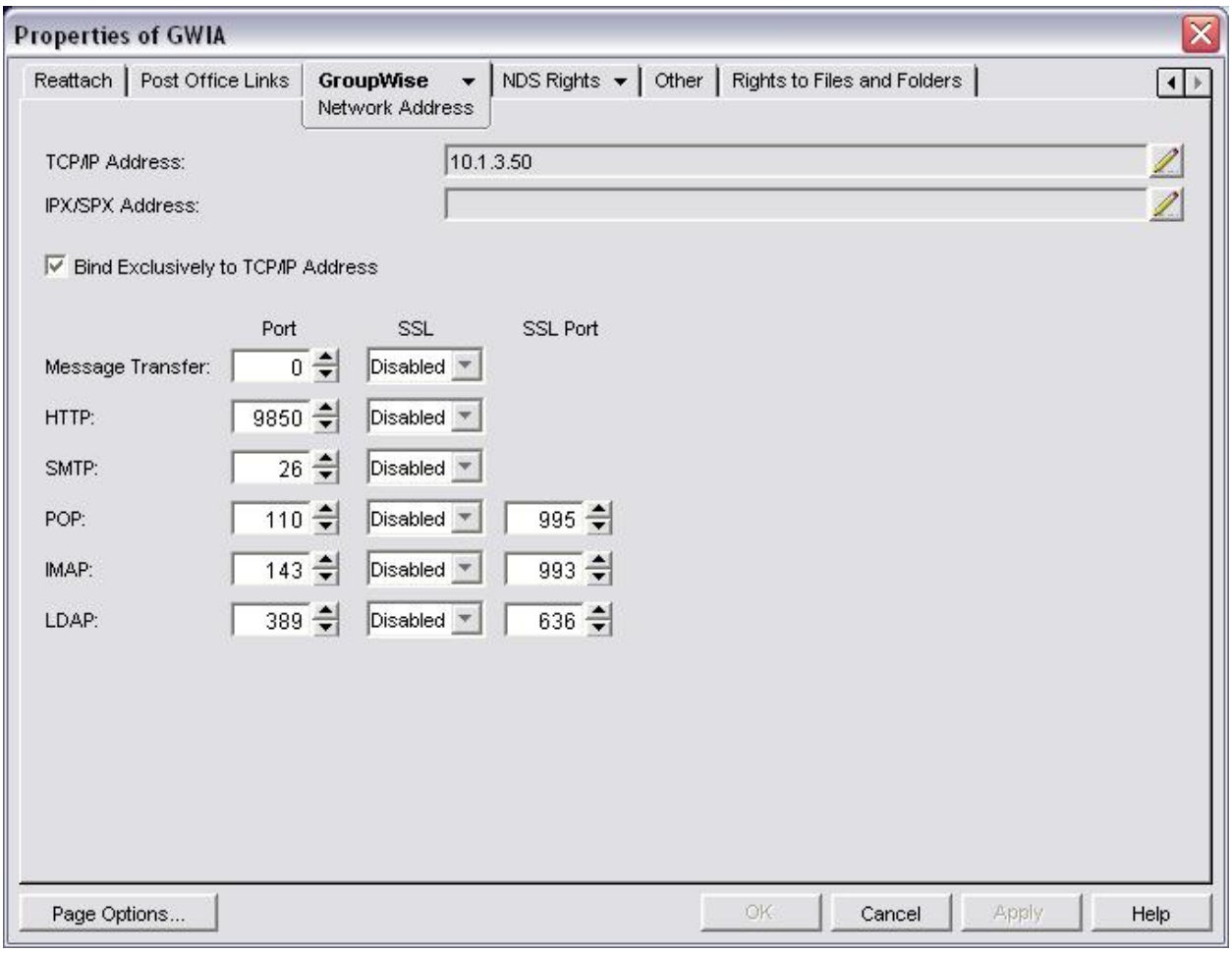
Inheritance can also be used to create independent sub-policies to implement specialized filters for specific messages and addresses defined in a policy qualification. The sub-policies will contain all of the scanner settings from the main policy, but can have additional filters applied which do not affect the parent policy. These filters might include surveillance for particular addresses or additional limits imposed on specific users or groups.

GWIA and SMTP interfaces on the same box

Generally, GWIA is the process that accepts your SMTP traffic over port 25. However, when using a GWAVA 4 SMTP scanner, you want that traffic to go to the scanner first, and then be passed on to the GWIA.

If both processes are running on the same server, then there will be a port conflict. In order to prevent a port conflict between the two processes, the port that GWIA listens on for SMTP traffic must be changed.

Modifying the SMTP port in the GWIA configuration is simple to do. Open ConsoleOne and locate your GWIA, then open its properties. Go to **GroupWise | Network Address**. Change the SMTP port from 25 to an unused port.



SMTP interface ports

If the GWAVA SMTP interface is set behind a firewall, or multiple firewalls, the following ports should be open for mail flow and GWAVA functions or services:

- 80 – TCP Outbound (Updates services for Antivirus, Signature Engine, and GWAVA system.)
- 21 – FTP Outbound (OS updates)
- 53 – UDP (DNS lookups)
- 25 – TCP Inbound (Used for Mail)
- 25 – TCP Outbound (Only if scanning outbound mail)
- 123 – TCP Outbound (Network Time Protocol (NTP))

The following should be open to access the GWAVA appliance from outside the network:

- 49285 – TCP Inbound (QMS message release service)
- 49282 – TCP Inbound (GWAVA Management Console)
- 22 – TCP (SSH access. This can be a security concern, but may be necessary to enable for support access.)

GroupWise paths

Linux

The Linux configuration files are found, by default, in `/opt/novell/groupwise/agents/share`. If the mail system files are not setup according to default, search the system for the correct file name(s) requested in the interface setup wizard. (For example, on Linux, search for 'gwia.cfg'. Search in the likely GroupWise file structure to shorten the search time.)

Squid configuration file changes

There are ten lines which need to be added to the squid configuration file for GWAVA to function with the ICAP connection. Add the following:

```
#icap_log /var/log/squid/icap.log

icap_enable on

icap_send_client_username on

icap_client_username_encode off


icap_service service_req reqmod_precache bypass=0 icap://IP Address of GWAVA
server):1344/request

adaptation_access service_req allow all


icap_service service_resp respmod_precache bypass=0 icap://<IP Address of GWAVA
server>:1344/response

adaptation_access service_resp allow all


#turn off persistent connections to increase speed

server_persistent_connections off
```

For specific file and further information, see http://www.squid-cache.org/Doc/config/ and the GWAVA knowledgebase found at http://support.gwava.com for configuration options and explanations.