# General Administration Guide

GWAVA 4.51

http://www.gwava.com

# Table of Contents

# How GWAVA works

GWAVA is an anti-malware and content management solution for Novell GroupWise, which provides complete protection for your mail system through real time scanners. GWAVA's new anti-spam scanner has an adaptive learning filter, which, when trained correctly, will fit any situation with a custom set of rules to protect and block unwanted items and messages from the GroupWise mail system.

GWAVA allows this scanner to be fit into several applications, integrating with the GroupWise agents and processes to protect the mail system from attack. GWAVA's scanner can integrate with your current setup in the following scanner interfaces:

- GWIA scanner
- MTA scanner
- POA scanner
- SMTP scanner
- WASP (WebAccess) scanner

# How the different scanners work

The different scanner interfaces offered by GWAVA all utilize the same 'scanner' in the base of the GWAVA system, but each is configured separately to integrate to the different components they are named for. For this reason, each different interface is referred to as a 'scanner', and will be briefly explained below.

## SMTP Scanner

The SMTP scanners are the most recent options to the GWAVA system, and allow the 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 scanner adds a scanning layer between the GWIA, or any other mail system's SMTP sending 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 scanner which then sends the filtered mail to the GWIA or SMTP. This scanner allows GWAVA to act independently of your mail system. If used behind a firewall, see the appendix on suggested open ports.

## GWIA Scanner

The GroupWise Internet Agent scanner, or GWIA scanner, 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 scanner does not directly receive mail or send mail, and has no connection to the internet whatsoever. GWAVA's GWIA scanner 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 scanner 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 scanner 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 scanner. Once GWAVA is started, the queued mail will be processed and sent to the internet or the MTA as normal.

## MTA Scanner

The Message Transfer Agent scanner integrates into the process of the actual GroupWise agent, adding an 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 scanner 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 scanner. 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 scanner is, first to start GWAVA, and then start the MTA. To shutdown the MTA and GWAVA, first stop the MTA, then shutdown GWAVA. It is also recommended that on NetWare, the MTA be placed in its own protected memory space; to safely deal with hung processes should the start and stop order ever be ignored.

## POA Scanner

The Post Office Agent scanner is the only scanner in the GWAVA suite which is not a real time scanner. There is no API or process that allows the Post Office to be scanned in real time, so GWAVA has created a scheduled scanner 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 scanner enters and scans each user's post office and messages individually. The POA scanner 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 scanner requires the POA to be running in order to operate, but has no start or stop order associated with the operation.

## WASP Scanner

The GroupWise WebAccess scanner integrates into the WebAccess interface 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 scanner 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 can be operated remotely to the GWAVA server, to run on a separate, dedicated WebAccess server if desired, though there must be a quick and reliable network connection between the WebAccess machine and the machine running GWAVA.

## Choosing a scanner for your system

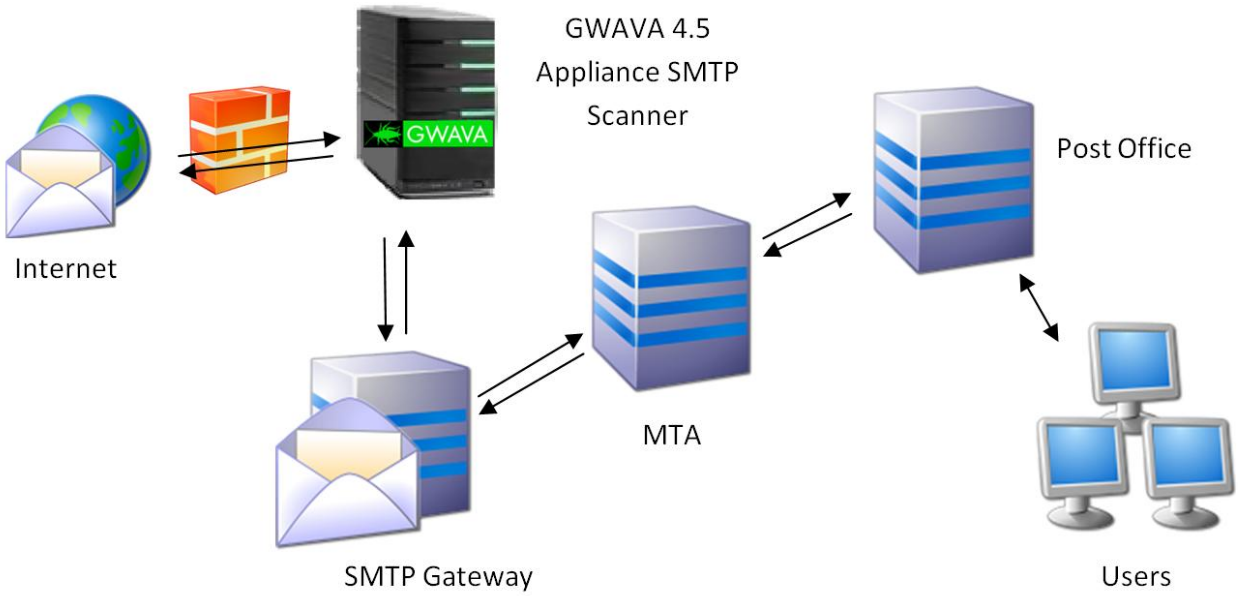
The most recommended scanner for any GroupWise system is the SMTP scanner, which has the highest performance and least intrusion to a mail system as well as providing a few services that are not available to the MTA and POA scanners.  But the SMTP scanner may not be the best fit for your system.

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

The GWIA scanner sorts all mail passing through the GWIA, which protects the GroupWise system from all external mail threats. The GWIA scanner provides all options available, 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 scanner other than the GWIA or SMTP scanner.

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

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

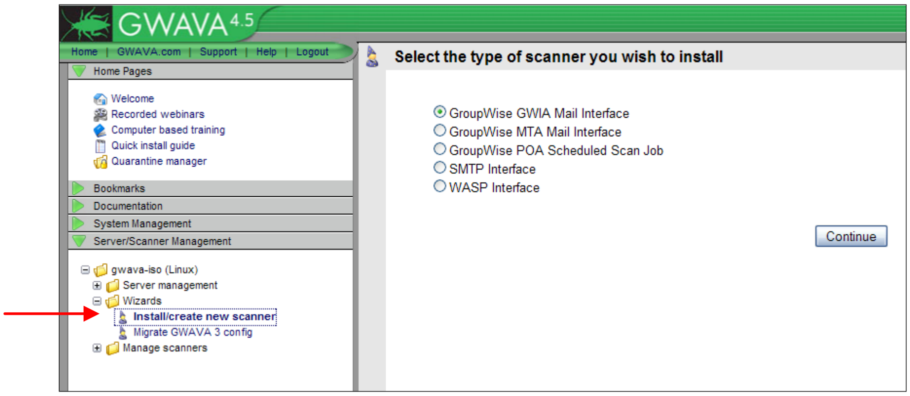


The SMTP scanner and GWAVA appliance are meant to be placed in front of the current GWIA or SMTP Gateway for the mail system. Incoming email sent to your domain will first go to the GWAVA appliance, which scans then sends clean email to the GWIA or SMTP Gateway.  Mail sent from your domain will pass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

Contact the sales representative for your area if you wish to implement the GWAVA 4.5 Appliance and SMTP scanner for your system.

## Creating a Scanner

The Scanner creation wizards, (found under Server/Scanner Management | <Server name>| Wizards | Install/create new scanner), walk through the steps and information required to install the different scanners for your system. Select the desired scanner and follow the instructions to install the scanner.



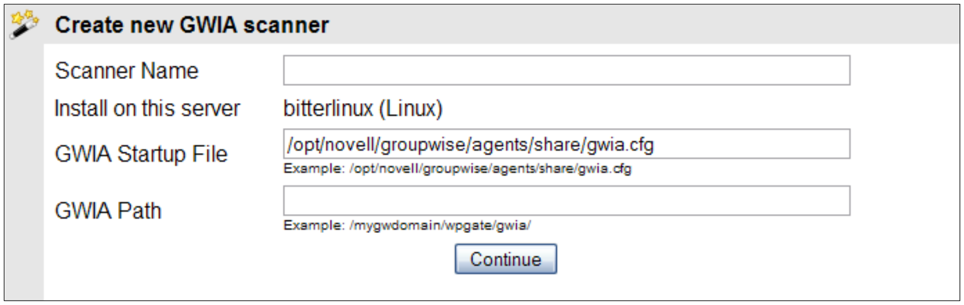
Select the type of scanner you wish to install

● GroupWise GWIA Mail Interface
○ GroupWise MTA Mail Interface
○ GroupWise POA Scheduled Scan Job
○ SMTP Interface
○ WASP Interface

### GWIA scanner

To install a GWIA scanner, you must tell the wizard where the active GWIA directory and the GWIA configuration file are located. The GWIA scanner 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.

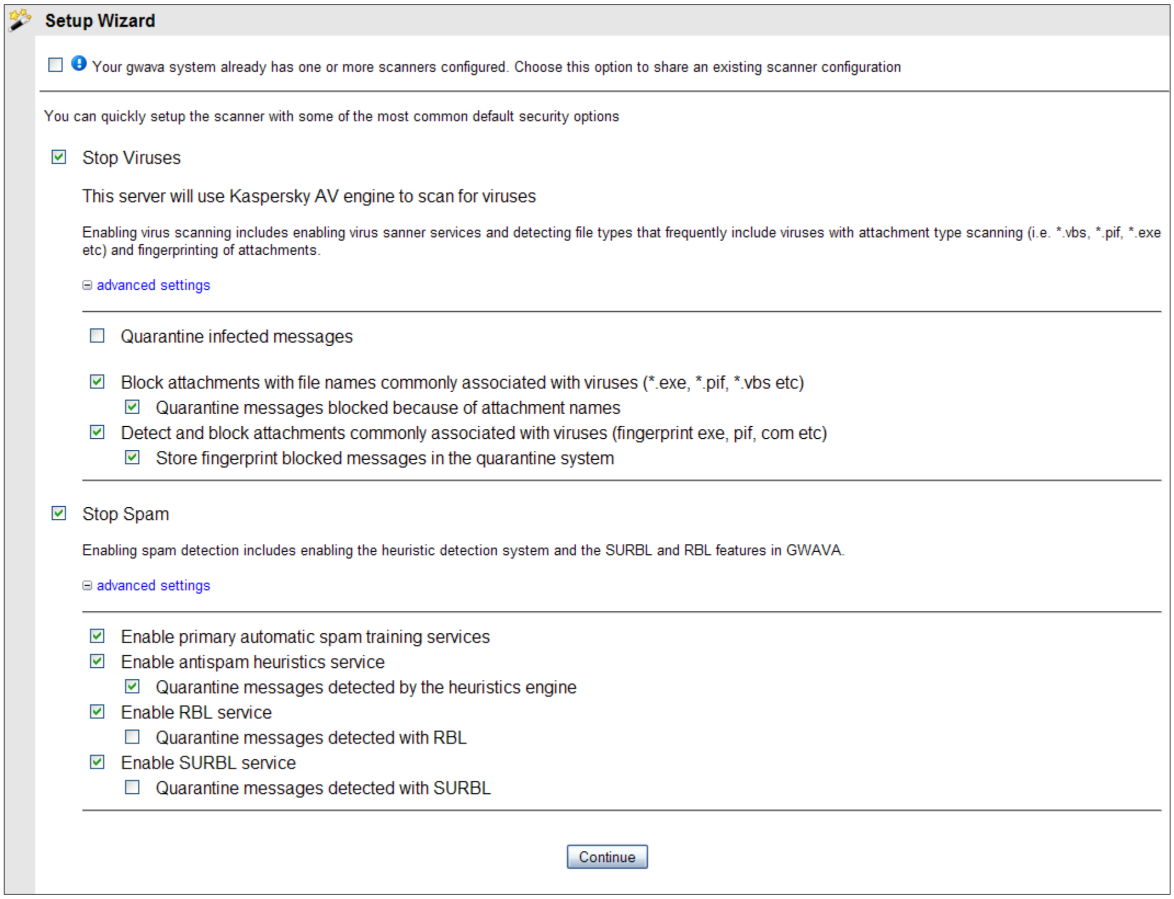
Name the scanner and provide the locations to the directory and file required. Use the example paths as your guide, though they are only examples and will differ from your actual paths. Always double-check your paths to ensure that the scanner will install correctly. If the directory path is incorrect, your mail will not flow after the GWIA has been restarted to enact the changes.



Create new GWIA scanner

| | |
|---|---|
| Scanner Name | |
| Install on this server | bitterlinux (Linux) |
| GWIA Startup File | /opt/novell/groupwise/agents/share/gwia.cfg<br>Example: /opt/novell/groupwise/agents/share/gwia.cfg |
| GWIA Path | <br>Example: /mygwdomain/wpgate/gwia/ |

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 scanner setup is complete. There are many other options to fine-tune the scanner which are only available after the scanner has been created. Select the basic setup options you wish to use as default and click continue.  The default configuration is shown.



**Setup Wizard**

□ Your gwava system already has one or more scanners configured. Choose this option to share an existing scanner configuration

You can quickly setup the scanner with some of the most common default security options

☑ Stop Viruses

This server will use Kaspersky AV engine to scan for viruses

Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.

⊟ advanced settings

□ Quarantine infected messages

☑ Block attachments with file names commonly associated with viruses (*.exe, *.pif, *.vbs etc)
- ☑ Quarantine messages blocked because of attachment names

☑ Detect and block attachments commonly associated with viruses (fingerprint exe, pif, com etc)
- ☑ Store fingerprint blocked messages in the quarantine system

☑ Stop Spam

Enabling spam detection includes enabling the heuristic detection system and the SURBL and RBL features in GWAVA.

⊟ advanced settings

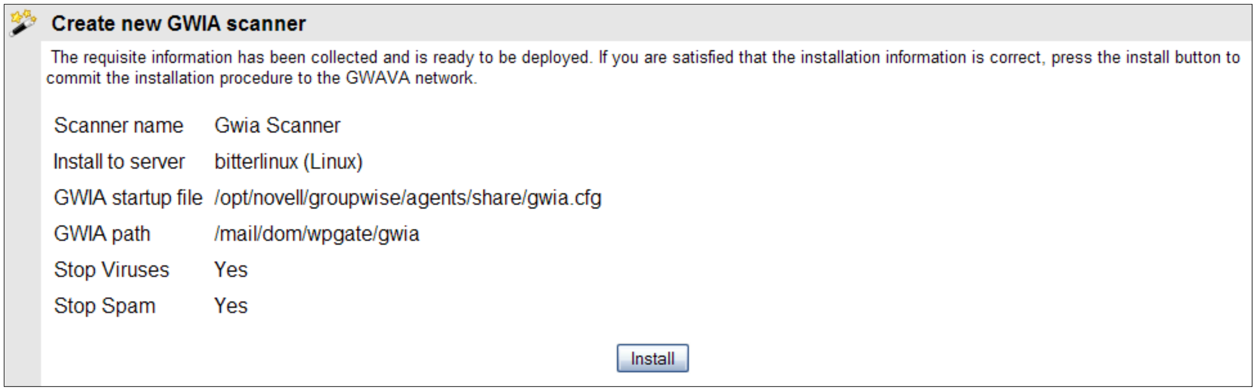
☑ Enable primary automatic spam training services

☑ Enable antispam heuristics service
- ☑ Quarantine messages detected by the heuristics engine

☑ Enable RBL service
- □ Quarantine messages detected with RBL

☑ Enable SURBL service
- □ Quarantine messages detected with SURBL

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



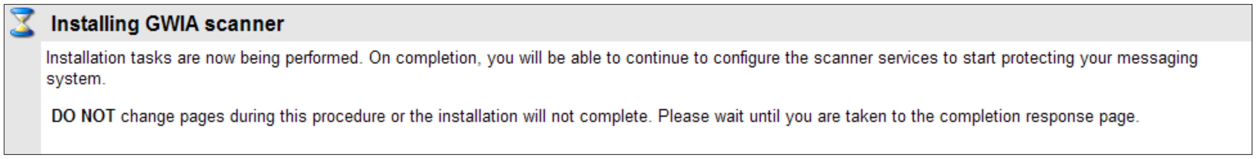
**Create new GWIA scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Scanner name | Gwia Scanner |
| Install to server | bitterlinux (Linux) |
| GWIA startup file | /opt/novell/groupwise/agents/share/gwia.cfg |
| GWIA path | /mail/dom/wpgate/gwia |
| Stop Viruses | Yes |
| Stop Spam | Yes |

Select the install button when you have verified the information.

The wizard will display this page while it is working.

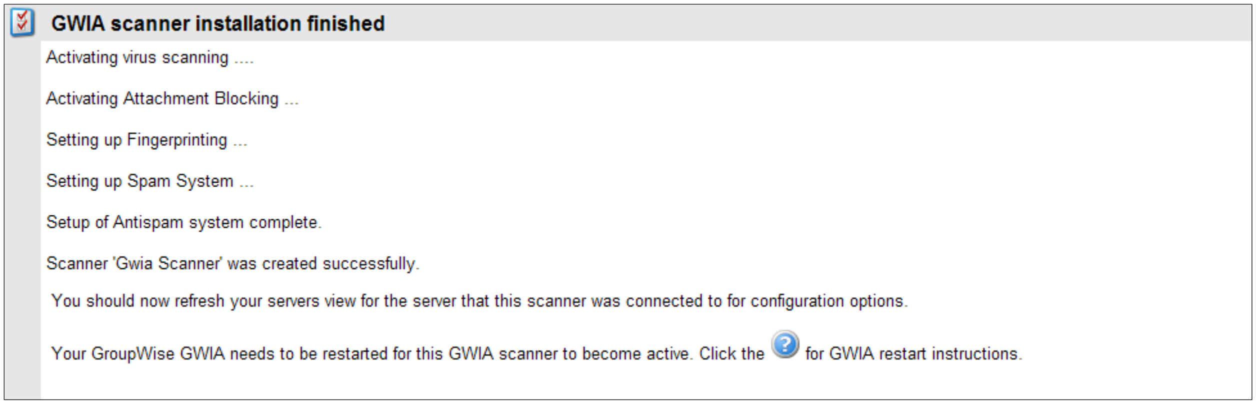


**Installing GWIA scanner**

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

**DO NOT** change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

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.



**GWIA scanner installation finished**

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Setting up Spam System ...

Setup of Antispam system complete.

Scanner 'Gwia Scanner' was created successfully.

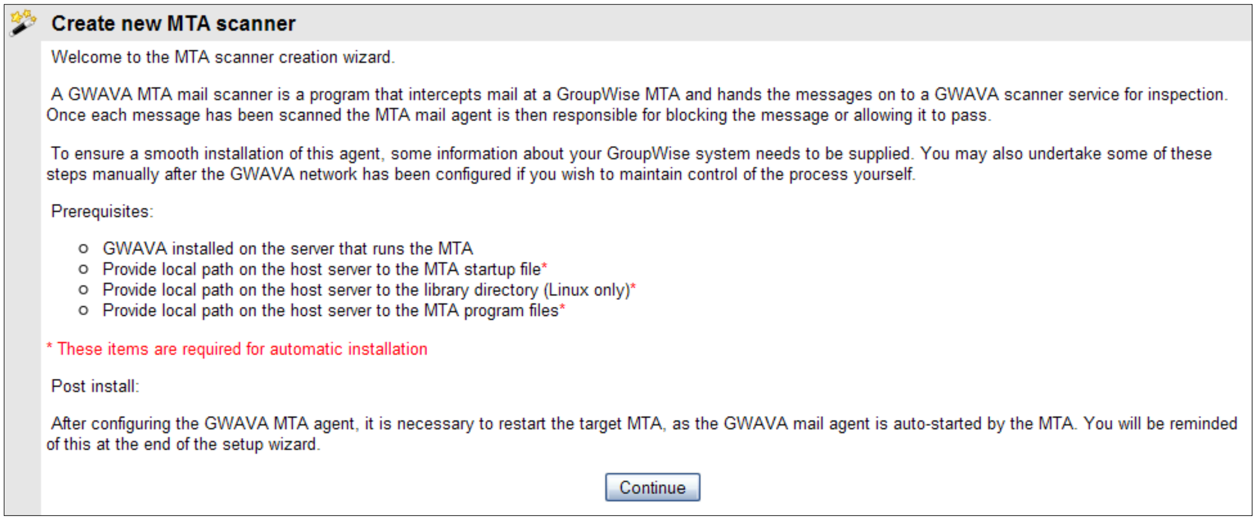
You should now refresh your servers view for the server that this scanner was connected to for configuration options.

Your GroupWise GWIA needs to be restarted for this GWIA scanner to become active. Click the ? for GWIA restart instructions.

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

## MTA Scanner

To create an MTA scanner, select the MTA scanner interface from the wizard and click next.



**Create new MTA scanner**

Welcome to the MTA scanner creation wizard.

A GWAVA MTA mail scanner is a program that intercepts mail at a GroupWise MTA and hands the messages on to a GWAVA scanner service for inspection. Once each message has been scanned the MTA mail agent is then responsible for blocking the message or allowing it to pass.

To ensure a smooth installation of this agent, some information about your GroupWise system needs to be supplied. You may also undertake some of these steps manually after the GWAVA network has been configured if you wish to maintain control of the process yourself.

Prerequisites:

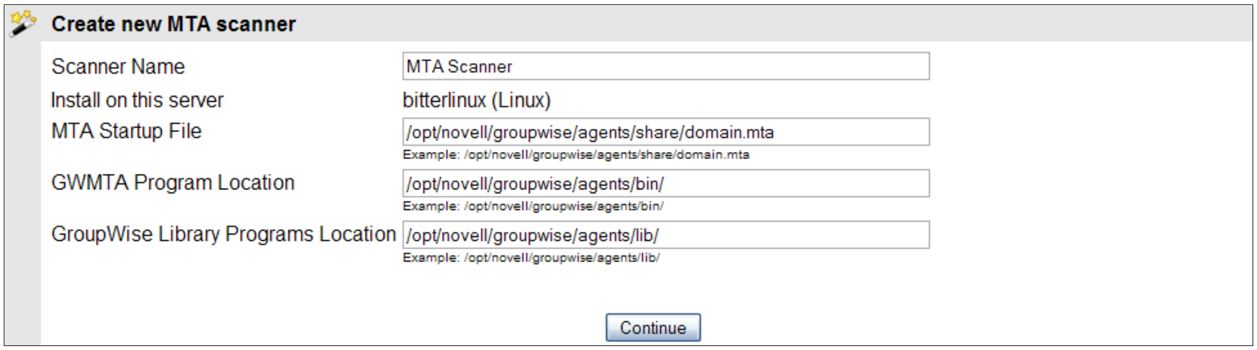
- GWAVA installed on the server that runs the MTA
- Provide local path on the host server to the MTA startup file*
- Provide local path on the host server to the library directory (Linux only)*
- Provide local path on the host server to the MTA program files*

* These items are required for automatic installation

Post install:

After configuring the GWAVA MTA agent, it is necessary to restart the target MTA, as the GWAVA mail agent is auto-started by the MTA. You will be reminded of this at the end of the setup wizard.

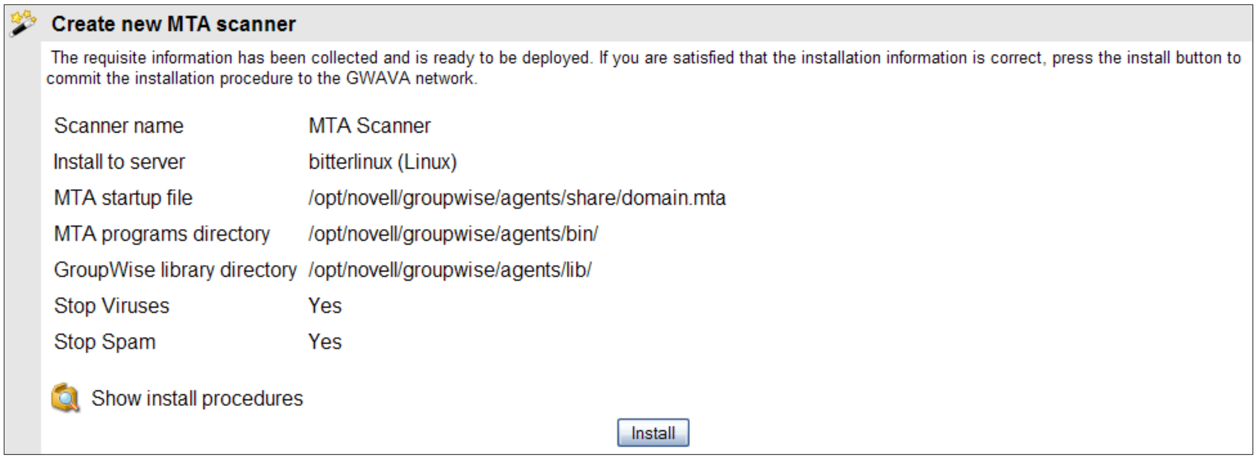
MTA scanner creation lists the information that is required. The paths to the MTA startup file and MTA program files are required on all platforms. Installing the MTA scanner on Linux systems also requires the path to the library directory.



**Create new MTA scanner**

| | |
|---|---|
| Scanner Name | MTA Scanner |
| Install on this server | bitterlinux (Linux) |
| MTA Startup File | /opt/novell/groupwise/agents/share/domain.mta<br>Example: /opt/novell/groupwise/agents/share/domain.mta |
| GWMTA Program Location | /opt/novell/groupwise/agents/bin/<br>Example: /opt/novell/groupwise/agents/bin/ |
| GroupWise Library Programs Location | /opt/novell/groupwise/agents/lib/<br>Example: /opt/novell/groupwise/agents/lib/ |

Provide a scanner name and the paths listed. Use the example paths as a guide, but know that the paths will differ from system to system.

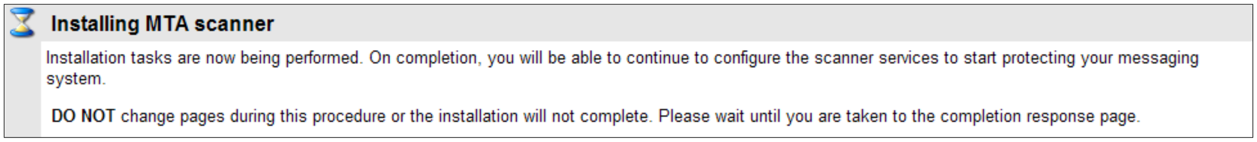


**Create new MTA scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Scanner name | MTA Scanner |
| Install to server | bitterlinux (Linux) |
| MTA startup file | /opt/novell/groupwise/agents/share/domain.mta |
| MTA programs directory | /opt/novell/groupwise/agents/bin/ |
| GroupWise library directory | /opt/novell/groupwise/agents/lib/ |
| Stop Viruses | Yes |
| Stop Spam | Yes |

Double check and confirm the information provided. Once the information has been confirmed, select install.

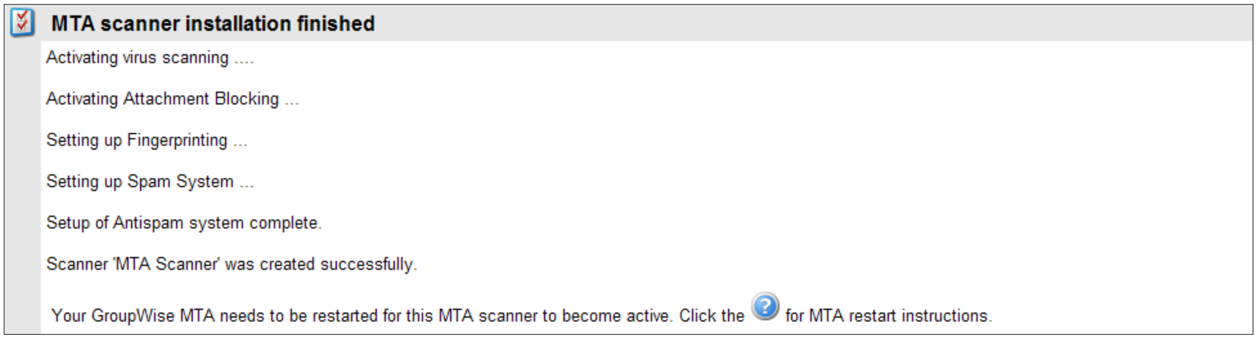


**Installing MTA scanner**

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

**DO NOT** change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

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



**MTA scanner installation finished**

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Setting up Spam System ...

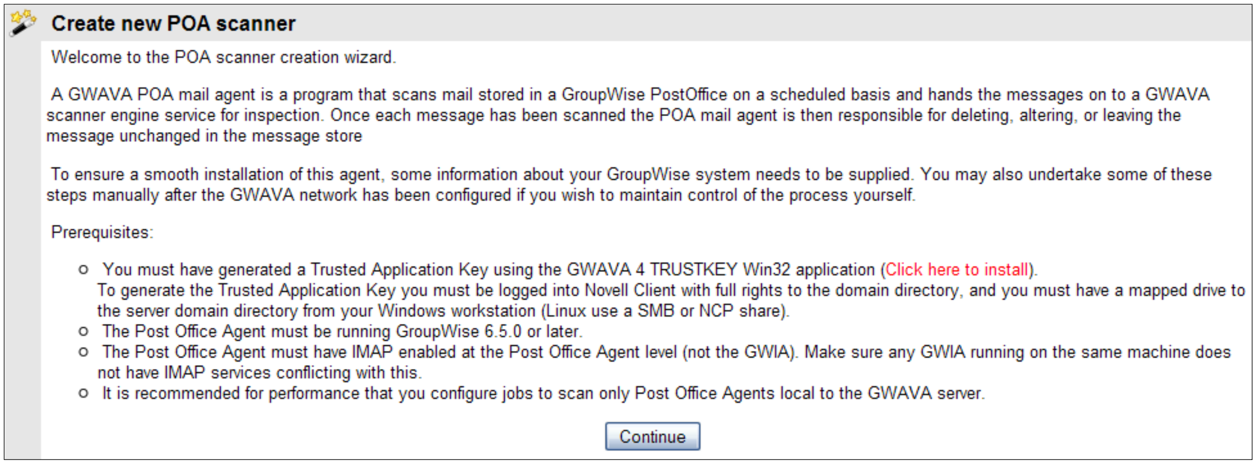
Setup of Antispam system complete.

Scanner 'MTA Scanner' was created successfully.

Your GroupWise MTA needs to be restarted for this MTA scanner to become active. Click the ? for MTA restart instructions.

## POA Scanner

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



**Create new POA scanner**

Welcome to the POA scanner creation wizard.

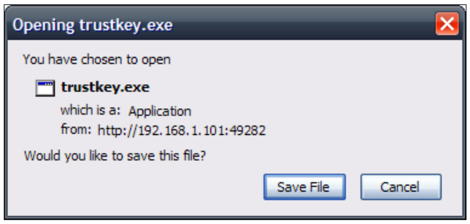
A GWAVA POA mail agent is a program that scans mail stored in a GroupWise PostOffice on a scheduled basis and hands the messages on to a GWAVA scanner engine service for inspection. Once each message has been scanned the POA mail agent is then responsible for deleting, altering, or leaving the message unchanged in the message store

To ensure a smooth installation of this agent, some information about your GroupWise system needs to be supplied. You may also undertake some of these steps manually after the GWAVA network has been configured if you wish to maintain control of the process yourself.

Prerequisites:

- You must have generated a Trusted Application Key using the GWAVA 4 TRUSTKEY Win32 application (Click here to install).
  To generate the Trusted Application Key you must be logged into Novell Client with full rights to the domain directory, and you must have a mapped drive to the server domain directory from your Windows workstation (Linux use a SMB or NCP share).
- The Post Office Agent must be running GroupWise 6.5.0 or later.
- The Post Office Agent must have IMAP enabled at the Post Office Agent level (not the GWIA). Make sure any GWIA running on the same machine does not have IMAP services conflicting with this.
- It is recommended for performance that you configure jobs to scan only Post Office Agents local to the GWAVA server.

The POA scanner 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.



**Opening trustkey.exe**

You have chosen to open

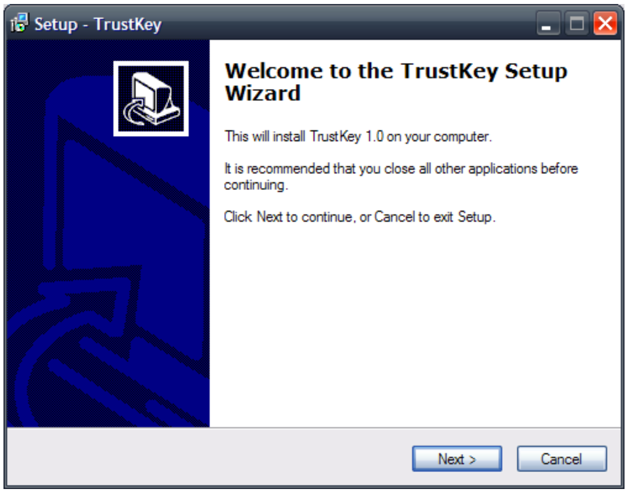
**trustkey.exe**

which is a: Application

from: http://192.168.1.101:49282

Would you like to save this file?

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



Setup - TrustKey

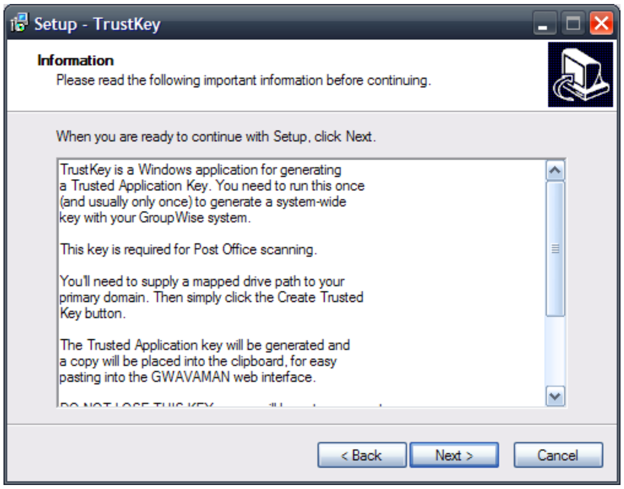
**Welcome to the TrustKey Setup Wizard**

This will install TrustKey 1.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Click ‘Next’ and read the information provided before continuing.



Setup - TrustKey

**Information**

Please read the following important information before continuing.

When you are ready to continue with Setup, click Next.

TrustKey is a Windows application for generating a Trusted Application Key. You need to run this once (and usually only once) to generate a system-wide key with your GroupWise system.

This key is required for Post Office scanning.

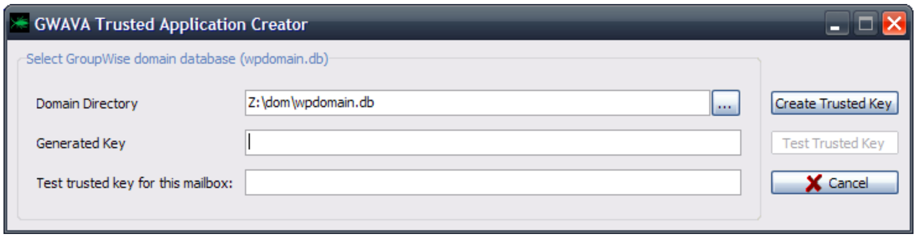
You'll need to supply a mapped drive path to your primary domain. Then simply click the Create Trusted Key button.

The Trusted Application key will be generated and a copy will be placed into the clipboard, for easy pasting into the GWAVAMAN web interface.

DO NOT LOSE THIS KEY [illegible]

The Trustkey application will create a trusted application key for GWAVA 4.5 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.


GWAVA Trusted Application Creator
Select GroupWise domain database (wpdomain.db)
...
Create Trusted Key
Test Trusted Key
Cancel

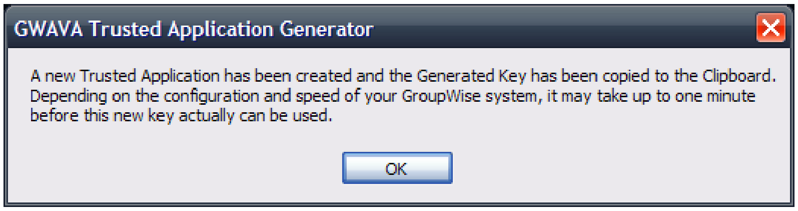
Domain Directory: Z:\dom\wpdomain.db

Generated Key:

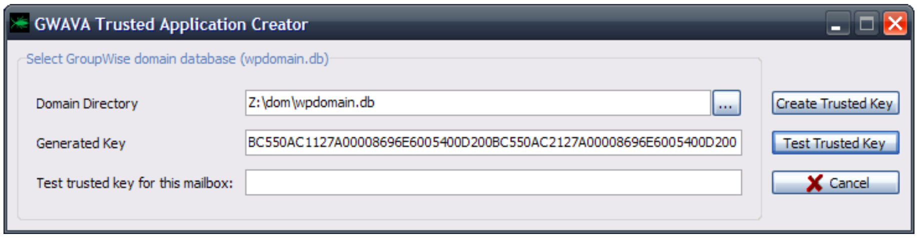
Test trusted key for this mailbox:

Browse to the domain directory containing the active wpdomain.db. This directory must be accessible from the Win32 workstation where the TrustKey application is running. The Win32 box also must be logged into the GroupWise system via the NetWare 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.



A new Trusted Application has been created and the Generated Key has been copied to the Clipboard. Depending on the configuration and speed of your GroupWise system, it may take up to one minute before this new key actually can be used.

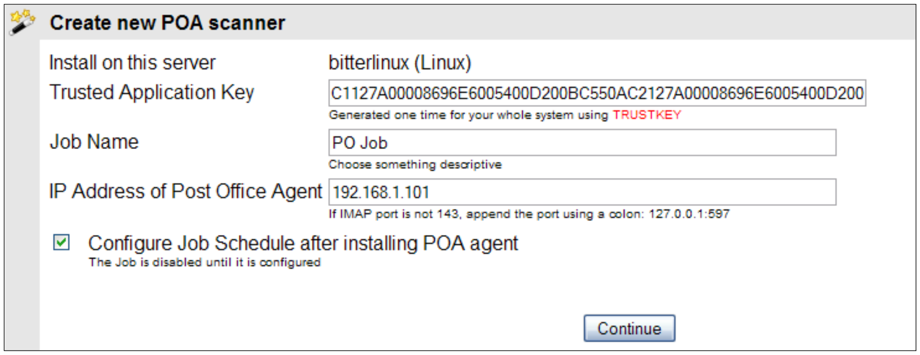

GWAVA Trusted Application Creator
Select GroupWise domain database (wpdomain.db)
...
Create Trusted Key
Test Trusted Key
Cancel

Domain Directory: Z:\dom\wpdomain.db

Generated Key: BC550AC1127A00008696E6005400D200BC550AC2127A00008696E6005400D200

Test trusted key for this mailbox:

Paste the copied trusted application key into the POA scanner 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) See the following link for details on how to enable or change the IMAP port: http://support.gwava.com/kb/?View=entry&EntryID=1099
Make sure ‘Configure Job…’ is checked. If the POA Job is not configured after creation, it will not run until it is configured.



Install on this server: bitterlinux (Linux)

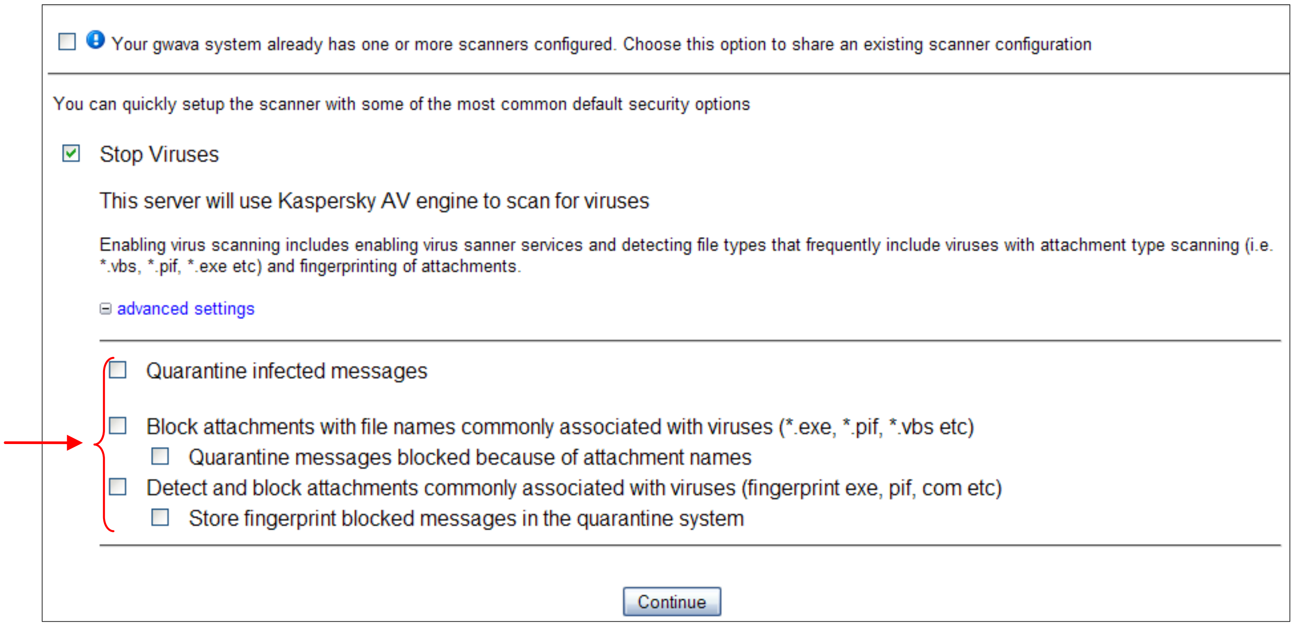
Trusted Application Key: C1127A00008696E6005400D200BC550AC2127A00008696E6005400D200
Generated one time for your whole system using TRUSTKEY

Job Name: PO Job
Choose something descriptive

IP Address of Post Office Agent: 192.168.1.101
If IMAP port is not 143, append the port using a colon: 127.0.0.1:597

☑ Configure Job Schedule after installing POA agent
The Job is disabled until it is configured

**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 scanner 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.



□ Your gwava system already has one or more scanners configured. Choose this option to share an existing scanner configuration

You can quickly setup the scanner with some of the most common default security options

☑ Stop Viruses

This server will use Kaspersky AV engine to scan for viruses

Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.

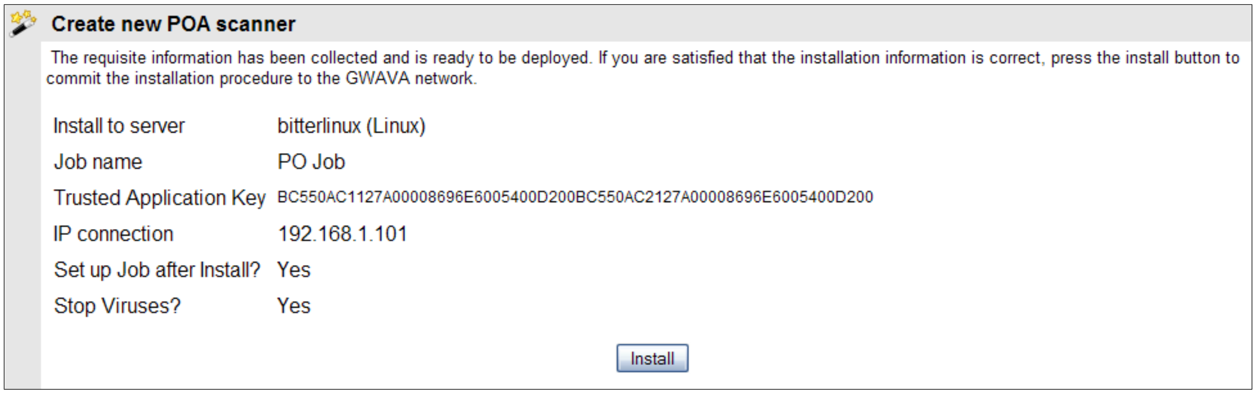
⊟ advanced settings

□ Quarantine infected messages

□ Block attachments with file names commonly associated with viruses (*.exe, *.pif, *.vbs etc)
- □ Quarantine messages blocked because of attachment names

□ Detect and block attachments commonly associated with viruses (fingerprint exe, pif, com etc)
- □ Store fingerprint blocked messages in the quarantine system

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

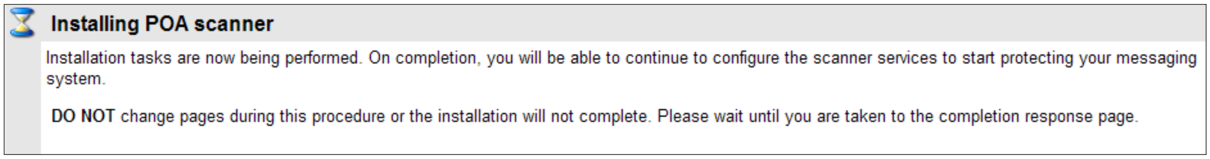


**Create new POA scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Install to server | bitterlinux (Linux) |
| Job name | PO Job |
| Trusted Application Key | BC550AC1127A00008696E6005400D200BC550AC2127A00008696E6005400D200 |
| IP connection | 192.168.1.101 |
| Set up Job after Install? | Yes |
| Stop Viruses? | Yes |

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

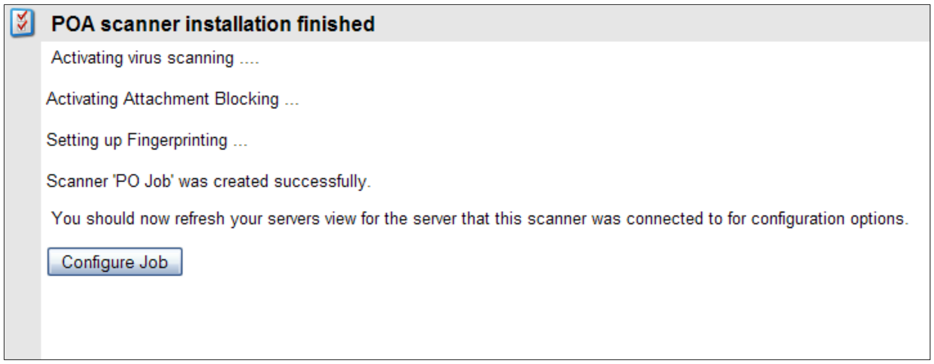


**Installing POA scanner**

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

DO NOT change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

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


**POA scanner installation finished**

Activating virus scanning ....

Activating Attachment Blocking ...

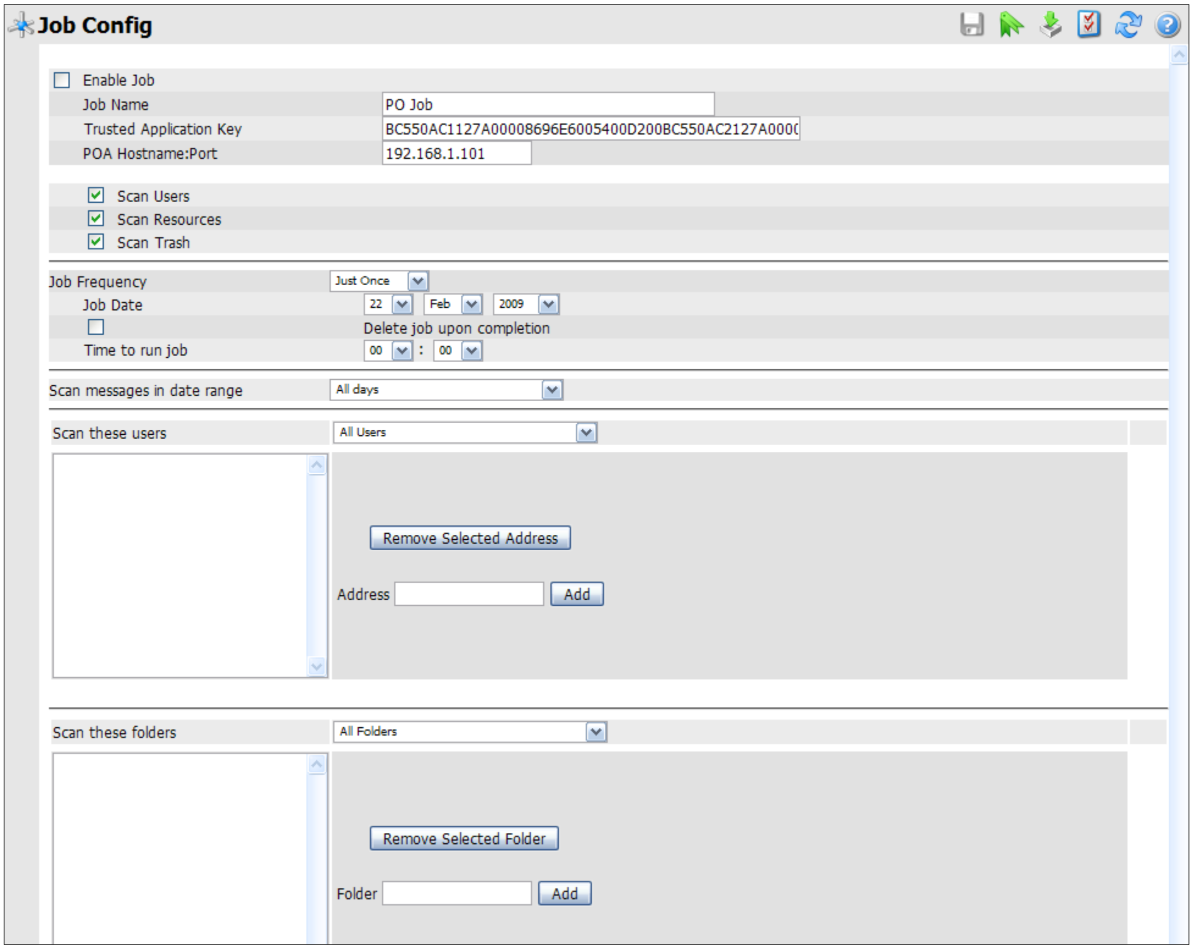
Setting up Fingerprinting ...

Scanner 'PO Job' was created successfully.

You should now refresh your servers view for the server that this scanner was connected to for configuration options.

Once the installation has completed, select the ‘Configure Job’ button to be taken to the configuration page.

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.


**Job Config**

□ Enable Job

| | |
|---|---|
| Job Name | PO Job |
| Trusted Application Key | BC550AC1127A00008696E6005400D200BC550AC2127A000 |
| POA Hostname:Port | 192.168.1.101 |

☑ Scan Users

☑ Scan Resources

☑ Scan Trash

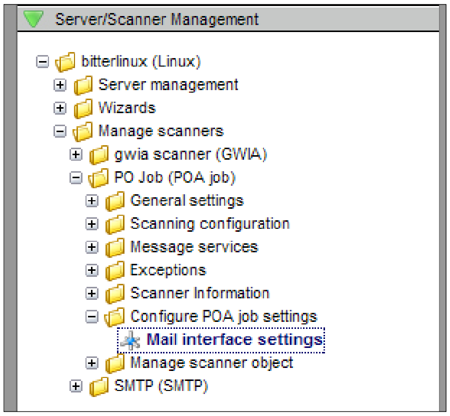
| | |
|---|---|
| Job Frequency | Just Once |
| Job Date | 22 Feb 2009 |
| □ | Delete job upon completion |
| Time to run job | 00 : 00 |
| Scan messages in date range | All days |
| Scan these users | All Users |

Scan these folders: All Folders

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 4.5 system and will become active within a couple of minutes.

To access the POA Job settings page just described, expand the POA scanner and select the 'Mail interface settings' object under the 'Configure POA job settings' folder, as shown.



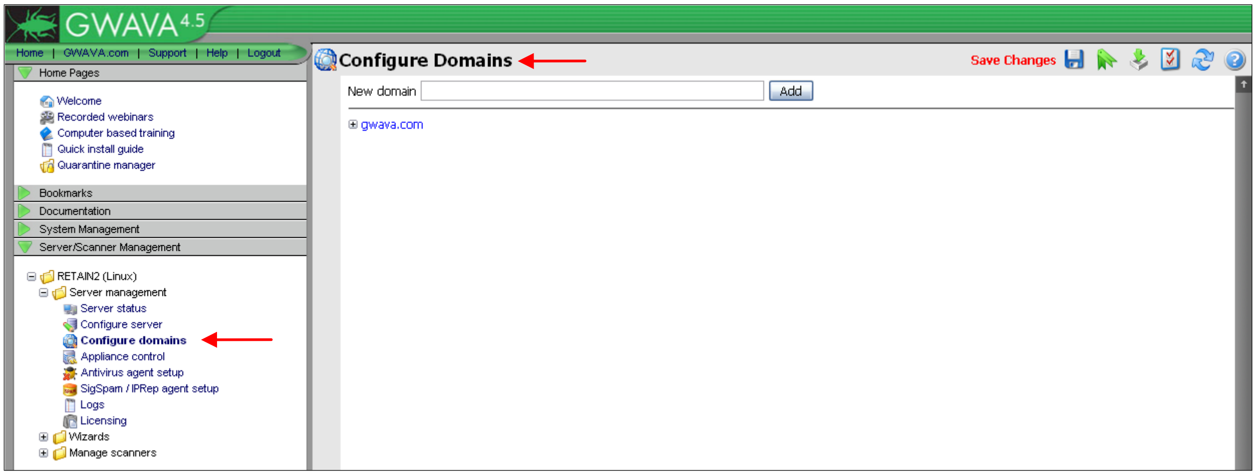
## SMTP Scanner

The SMTP scanners are the most recent options to the GWAVA system, and allow the 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 mail system resources open to function with greater performance and security.

The SMTP interfaces add 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 scanner, which then sends the filtered and clean mail to your mail system, unaltered.  These scanners allow GWAVA to act independently of your mail system.

The SMTP scanner 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/Scanner Management | <Server Name> |Server Management | Configure domains.

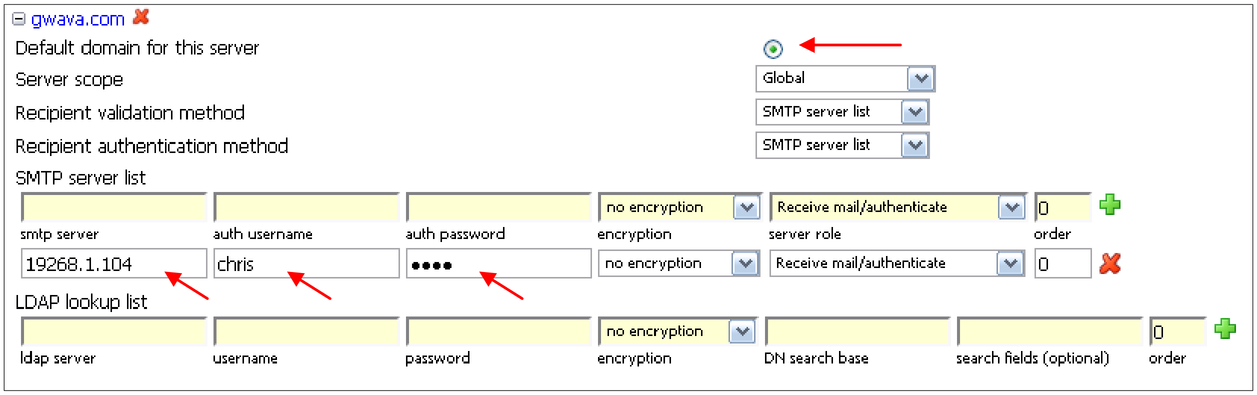


The default domain specified during Server Activation will be specified.  Additional domains may be added through the new domain addition field along the top of the screen. As always, make sure you save all desired changes made to the page before browsing to a different section of the management console.

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.com

Default domain for this server ◉

Server scope: Global

Recipient validation method: SMTP server list

Recipient authentication method: SMTP server list

SMTP server list

| smtp server | auth username | auth password | encryption | server role | order |
|---|---|---|---|---|---|
| | | | no encryption | Receive mail/authenticate | 0 |
| 19268.1.104 | chris | •••• | no encryption | Receive mail/authenticate | 0 |

LDAP lookup list

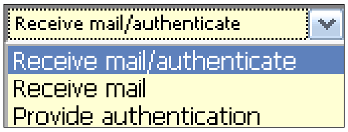
| ldap server | username | password | encryption | DN search base | search fields (optional) | order |
|---|---|---|---|---|---|---|
| | | | no encryption | | | 0 |

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.

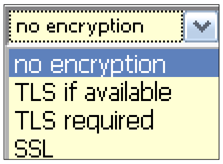
Multiple SMTP or LDAP servers are supported for failover purposes. If a SMTP server is unavailable GWAVA will send messages to the next available SMTP server listed according to the ‘order’ value. The ‘order’ values lowest numbers first, usually with the default SMTP listed as ‘0’, second as ‘1’, and 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 has been specifically configured to only accept authorized connections.

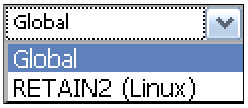
GWAVA shares the user list for each domain between the GWAVA modules, and specific SMTP servers can be selected to serve in different roles for each system, such as using one to receive mail, digests, and notifications, while another is used by QMS to authenticate users. Default settings allows SMTP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



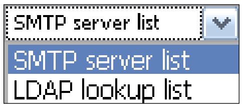
If the SMTP server requires encryption such as TLS or SSL, the setting must be correct.



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.

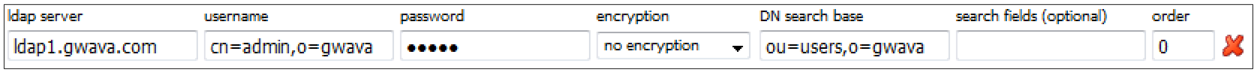


**LDAP** (optional)



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.



| ldap server | username | password | encryption | DN search base | search fields (optional) | order |
|---|---|---|---|---|---|---|
| ldap1.gwava.com | cn=admin,o=gwava | ●●●●● | no encryption | ou=users,o=gwava | | 0 |

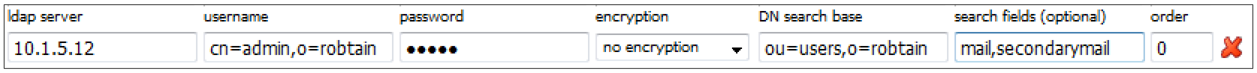
For the LDAP server connection address, place DNS name or IP address of the server

The username and password needs 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.

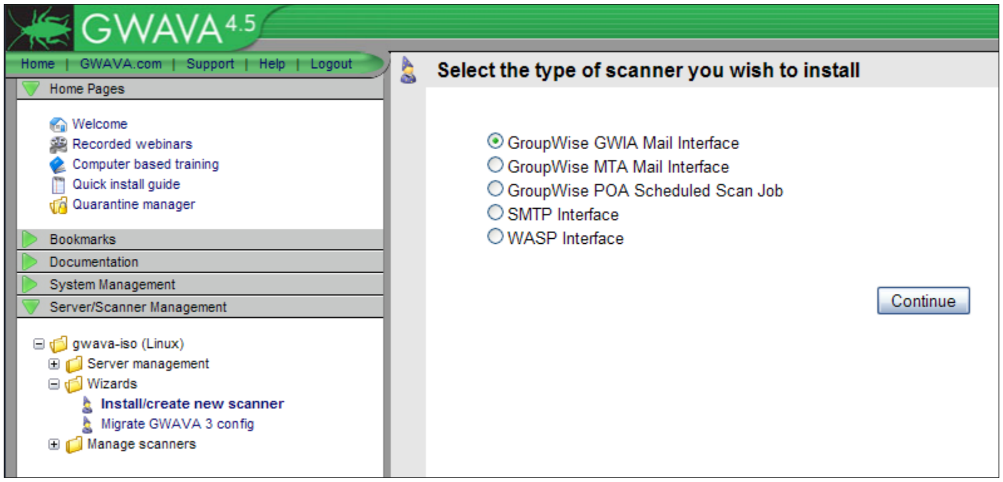
In the example below the LDAP server is set to search for the attributes ‘mail’ and ‘secondarymail’.



| ldap server | username | password | encryption | DN search base | search fields (optional) | order |
|---|---|---|---|---|---|---|
| 10.1.5.12 | cn=admin,o=robtain | ●●●●● | no encryption | ou=users,o=robtain | mail,secondarymail | 0 |

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

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

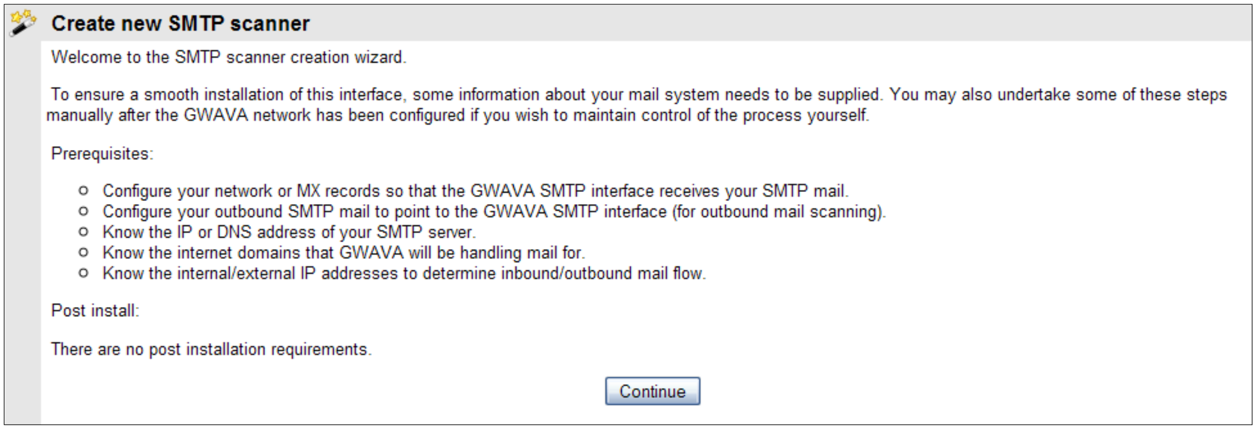


Select the type of scanner you wish to install

● GroupWise GWIA Mail Interface
○ GroupWise MTA Mail Interface
○ GroupWise POA Scheduled Scan Job
○ SMTP Interface
○ WASP Interface

To install a SMTP scanner, select the SMTP scanner option from the wizard and click next.

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



Create new SMTP scanner

Welcome to the SMTP scanner creation wizard.

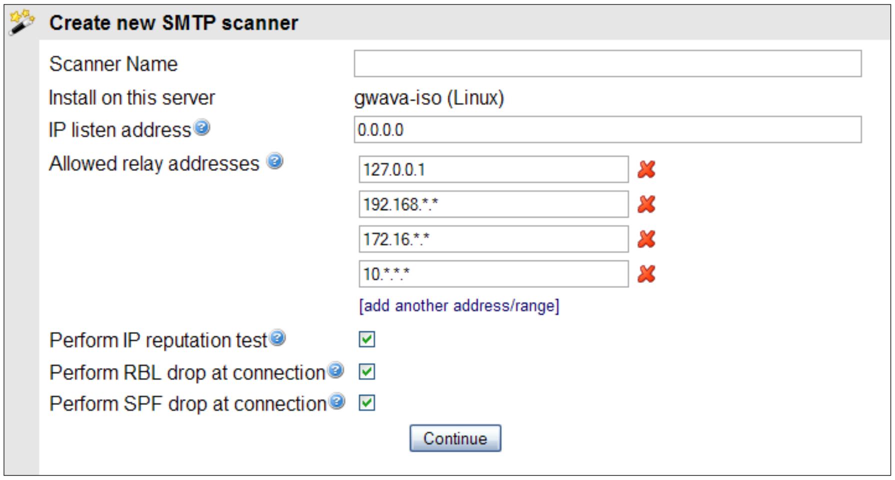
To ensure a smooth installation of this interface, some information about your mail system needs to be supplied. You may also undertake some of these steps manually after the GWAVA network has been configured if you wish to maintain control of the process yourself.

Prerequisites:

- Configure your network or MX records so that the GWAVA SMTP interface receives your SMTP mail.
- Configure your outbound SMTP mail to point to the GWAVA SMTP interface (for outbound mail scanning).
- Know the IP or DNS address of your SMTP server.
- Know the internet domains that GWAVA will be handling mail for.
- Know the internal/external IP addresses to determine inbound/outbound mail flow.

Post install:

There are no post installation requirements.



**Create new SMTP scanner**

Scanner Name:

Install on this server: gwava-iso (Linux)

IP listen address: 0.0.0.0

Allowed relay addresses:
127.0.0.1
192.168.*.*
172.16.*.*
10.*.*.*

[add another address/range]

Perform IP reputation test ☑
Perform RBL drop at connection ☑
Perform SPF drop at connection ☑

The **Scanner Name** is whatever you wish the scanner to be named in the GWAVA server.

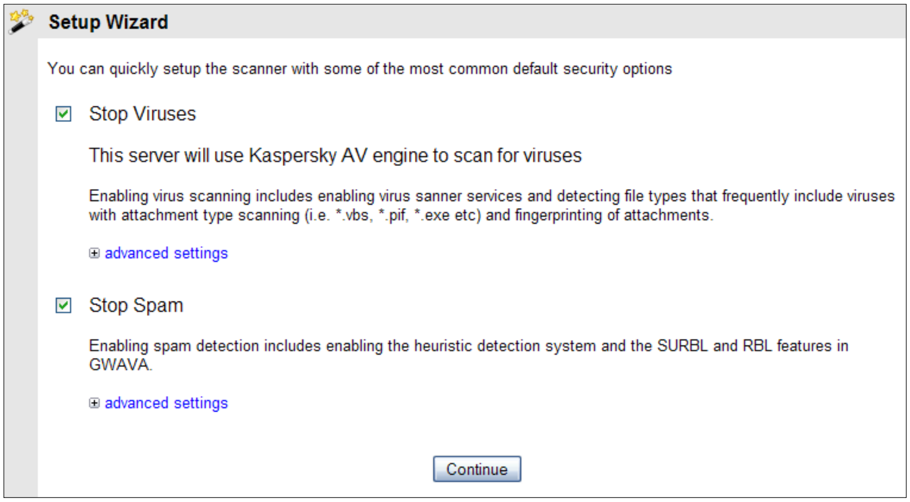
The **IP listen address** is the address that the SMTP scanner will bind to and listen on. It should be the address of the GWAVA server. This should also be listed on the MX record for your domain. (If the SMTP scanner resides on the same machine as the GWIA, then the GWIA must be changed to listen on a port other than 25, as the SMTP scanner 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. (10.1.1.10:25) See http://support2.gwava.com/kb/?View=entry&EntryID=1215 for more details.

**Allowed relay addresses** are the source addresses which are allowed to send mail through the GWAVA SMTP scanner. 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 'Continue'.



**Setup Wizard**

You can quickly setup the scanner with some of the most common default security options

☑ Stop Viruses

This server will use Kaspersky AV engine to scan for viruses

Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.

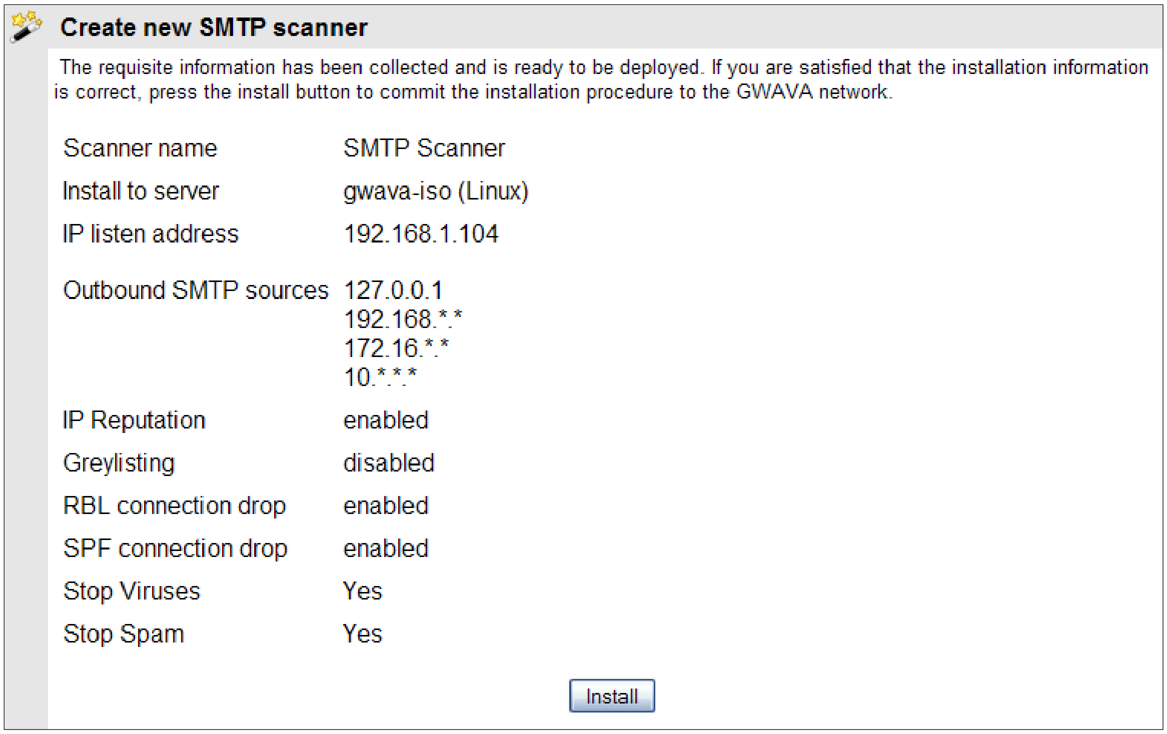
☑ Stop Spam

Enabling spam detection includes enabling the heuristic detection system and the SURBL and RBL features in GWAVA.

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

Click 'Continue'.

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

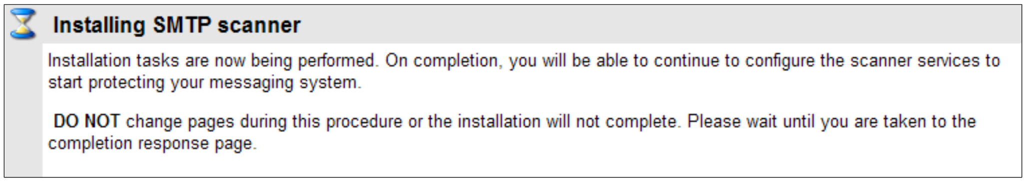


**Create new SMTP scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Scanner name | SMTP Scanner |
| Install to server | gwava-iso (Linux) |
| IP listen address | 192.168.1.104 |
| Outbound SMTP sources | 127.0.0.1<br>192.168.*.*<br>172.16.*.*<br>10.*.*.* |
| IP Reputation | enabled |
| Greylisting | disabled |
| RBL connection drop | enabled |
| SPF connection drop | enabled |
| Stop Viruses | Yes |
| Stop Spam | Yes |

Click ‘**Install**’ to continue.

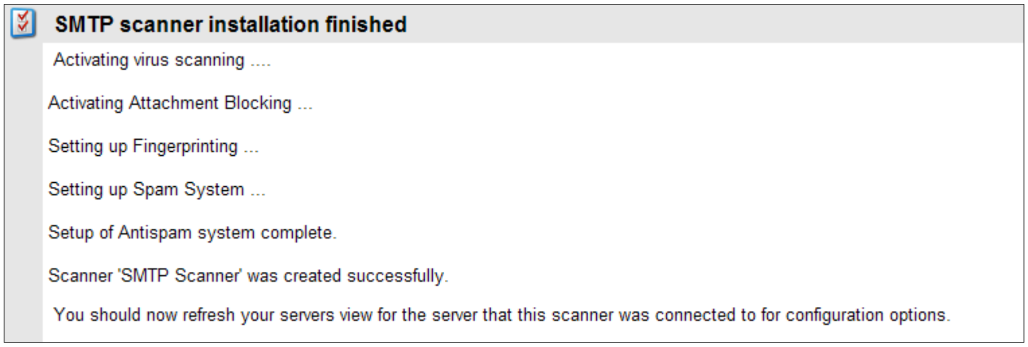


**Installing SMTP scanner**

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

DO NOT change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

Wait while the installation completes.



**SMTP scanner installation finished**

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Setting up Spam System ...

Setup of Antispam system complete.

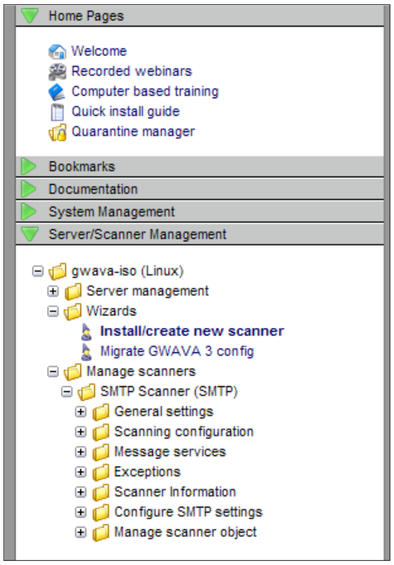
Scanner 'SMTP Scanner' was created successfully.

You should now refresh your servers view for the server that this scanner was connected to for configuration options.

Once installation is complete, refresh the Server/Scanner Management | <Server Name> | Manage scanners  folder to view your new SMTP scanner.

Your SMTP scanner is now created and ready to configure.

As soon as the MX record pointing to the GWAVA SMTP is active, the SMTP scanner will begin filtering mail.



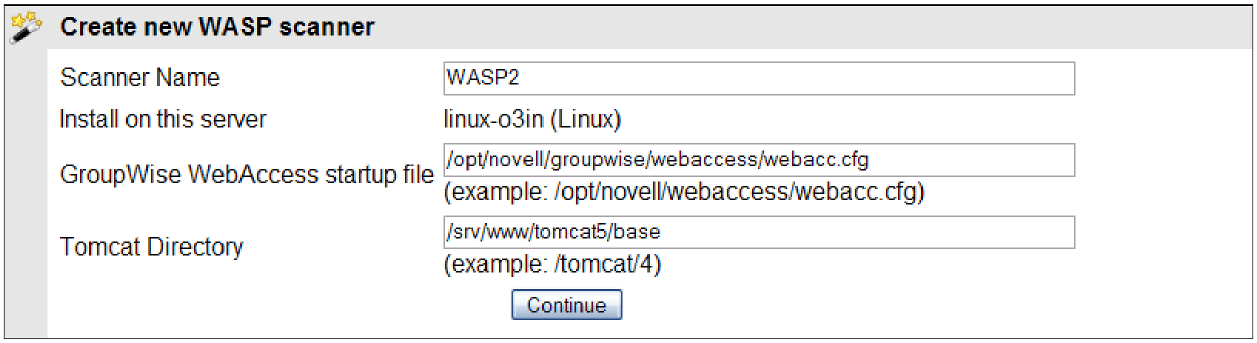
## WASP Local Scanner

To create a scanner you must know the correct information for the location of the Web Access directory and the active Tomcat directory.  Click **Continue.**

(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.



**Create new WASP scanner**

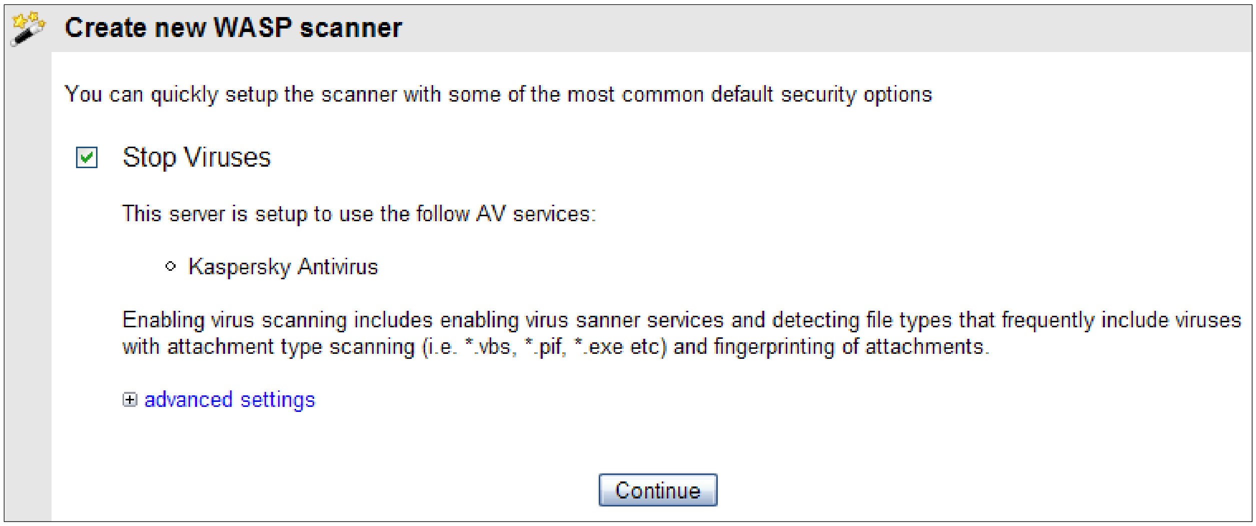
Scanner Name: WASP2

Install on this server: linux-o3in (Linux)

GroupWise WebAccess startup file: /opt/novell/groupwise/webaccess/webacc.cfg
(example: /opt/novell/webaccess/webacc.cfg)

Tomcat Directory: /srv/www/tomcat5/base
(example: /tomcat/4)

Enter the correct information and click **Continue**.



**Create new WASP scanner**

You can quickly setup the scanner with some of the most common default security options

☑ Stop Viruses

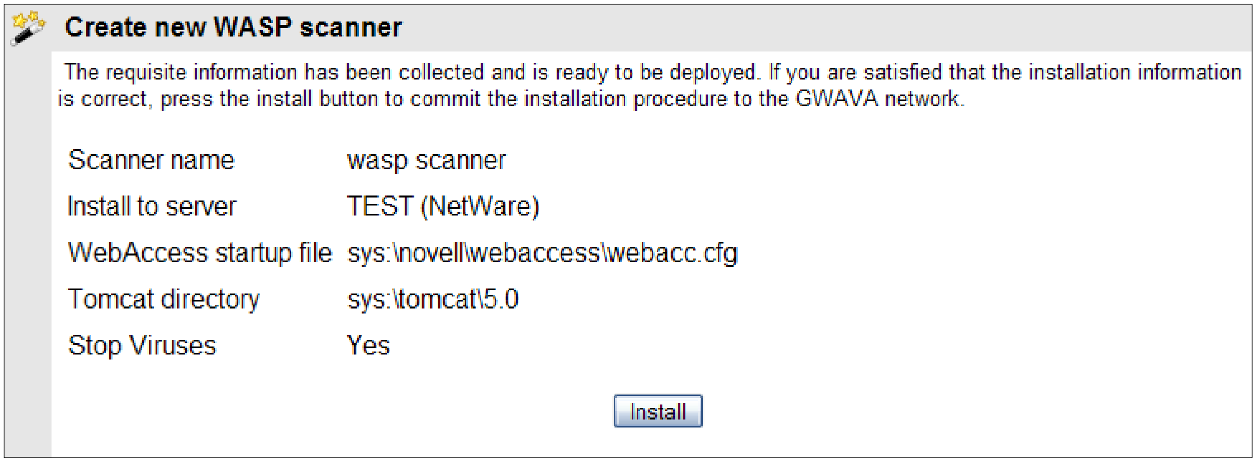
This server is setup to use the follow AV services:

- Kaspersky Antivirus

Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.

To enable protection from viruses, select an anti-virus engine. On Linux, the Kaspersky engine will be selected for you. On NetWare, you may have other engines to choose from in addition to the Kaspersky engine.

Click **Continue**.

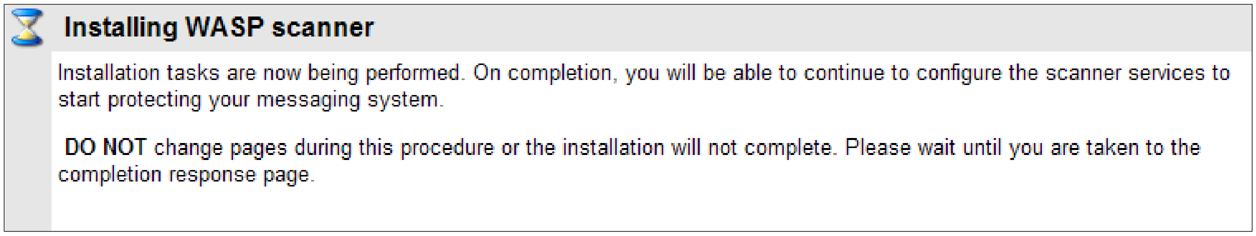


**Create new WASP scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Scanner name | wasp scanner |
| Install to server | TEST (NetWare) |
| WebAccess startup file | sys:\novell\webaccess\webacc.cfg |
| Tomcat directory | sys:\tomcat\5.0 |
| Stop Viruses | Yes |

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

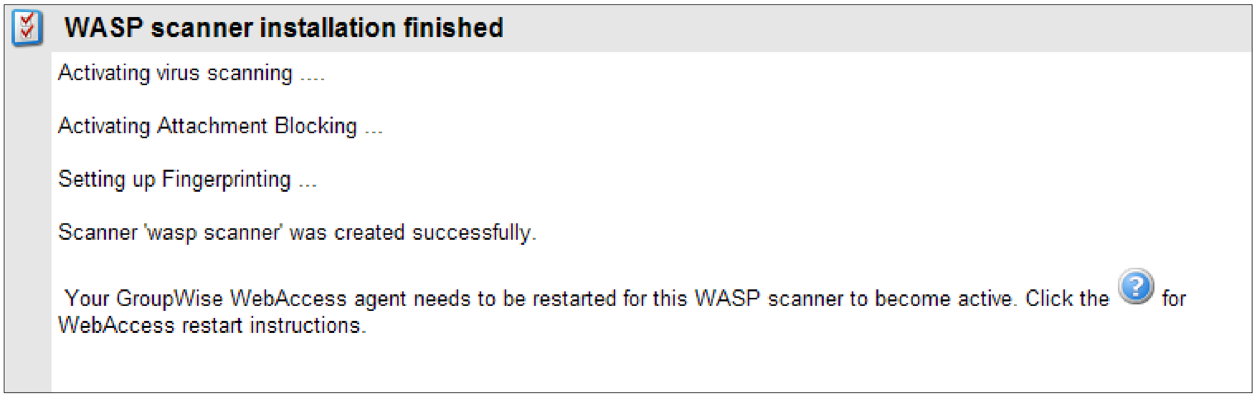


**Installing WASP scanner**

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

DO NOT change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

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



WASP scanner installation finished

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Scanner 'wasp scanner' was created successfully.

Your GroupWise WebAccess agent needs to be restarted for this WASP scanner to become active. Click the ? for WebAccess restart instructions.

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

**NOTE: Your WASP scanner 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 scanner.

WASP 2 scanners 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.

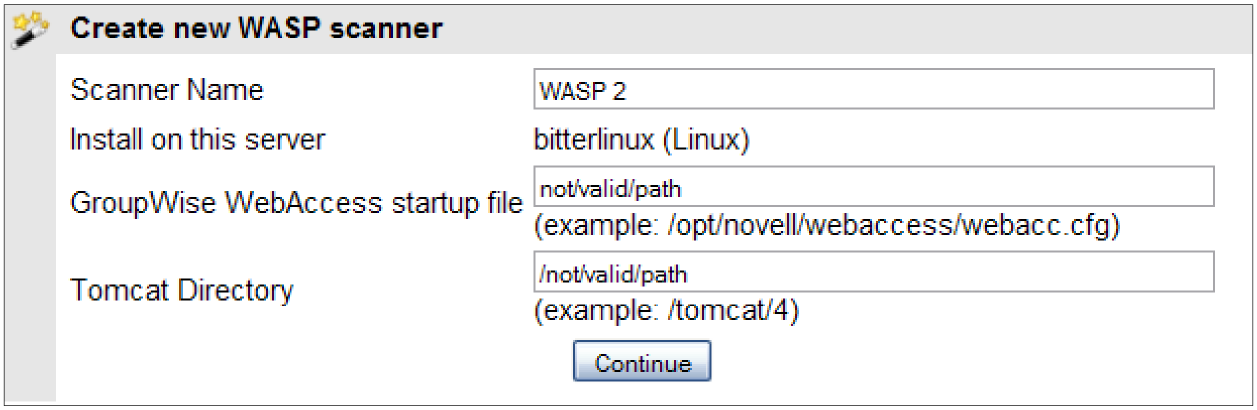
## WASP Remote Scanner

Running WASP 2 in remote mode means that WASP 2 needs to transfer the mime files via the network to GWAVA 4.5 in order to be scanned. To create a remote WASP 2 scanner, 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 scanner creation wizard as above, but when prompted for the path to the files requested, place invalid paths in the defined areas.

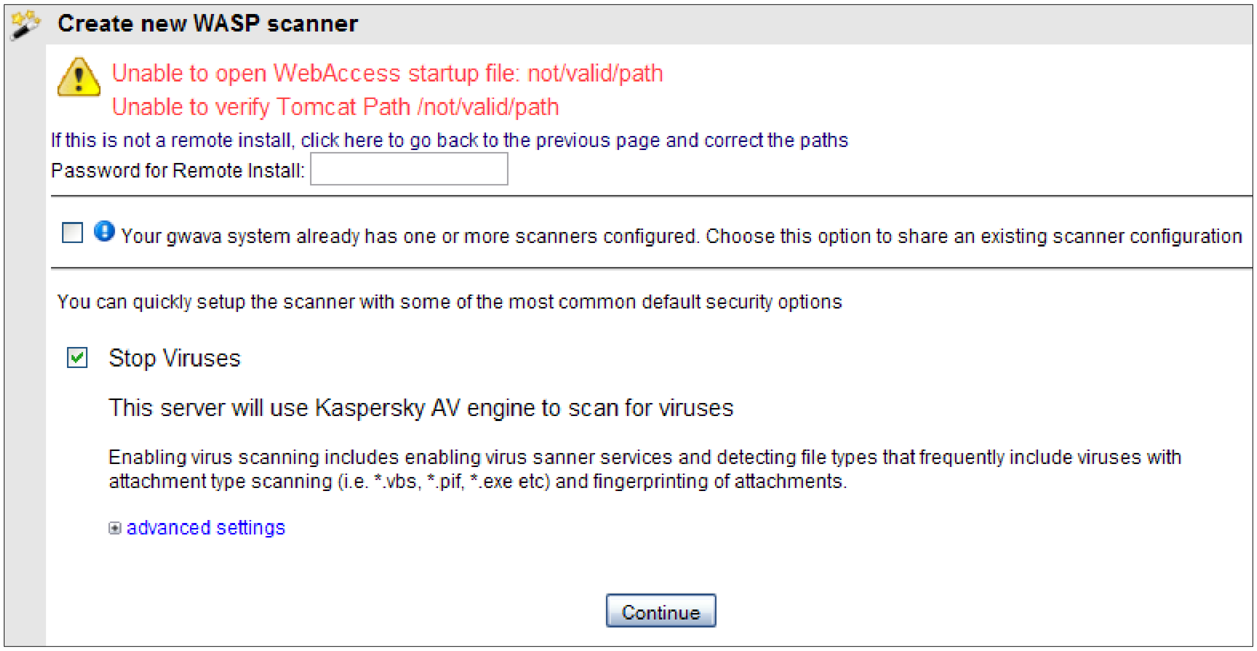


Create new WASP scanner

| | |
|---|---|
| Scanner Name | WASP 2 |
| Install on this server | bitterlinux (Linux) |
| GroupWise WebAccess startup file | not/valid/path<br>(example: /opt/novell/webaccess/webacc.cfg) |
| Tomcat Directory | /not/valid/path<br>(example: /tomcat/4) |

The installer will try to verify the path to the installation files, but will fail. This triggers the remote install mode for the scanner.

In remote mode, the installer creates a wasp user and password to connect to GWAVA 4.5. The Username is created automatically, but you must specify the password. The user and password will only be used by the wasp scanner to connect remotely to the GWAVA 4.5 server and gain access to the scanner. Any password will do. Configure as desired.



Create new WASP scanner

Unable to open WebAccess startup file: not/valid/path
Unable to verify Tomcat Path /not/valid/path

If this is not a remote install, click here to go back to the previous page and correct the paths

Password for Remote Install:

☐ Your gwava system already has one or more scanners configured. Choose this option to share an existing scanner configuration

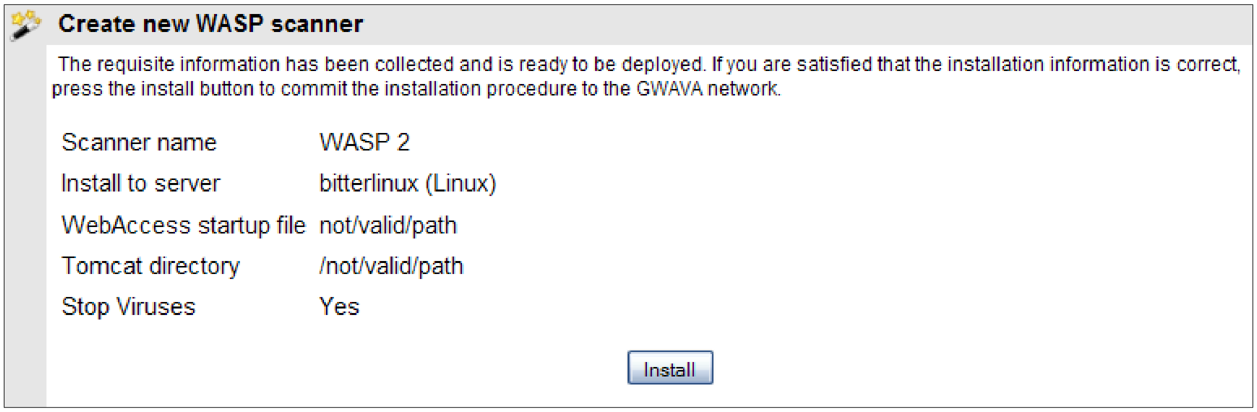
You can quickly setup the scanner with some of the most common default security options

☑ Stop Viruses

This server will use Kaspersky AV engine to scan for viruses

Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.

Verify all information, and click 'install' when the information is correct. Use the 'back' button on your browser if you need to change any of the information before you continue.

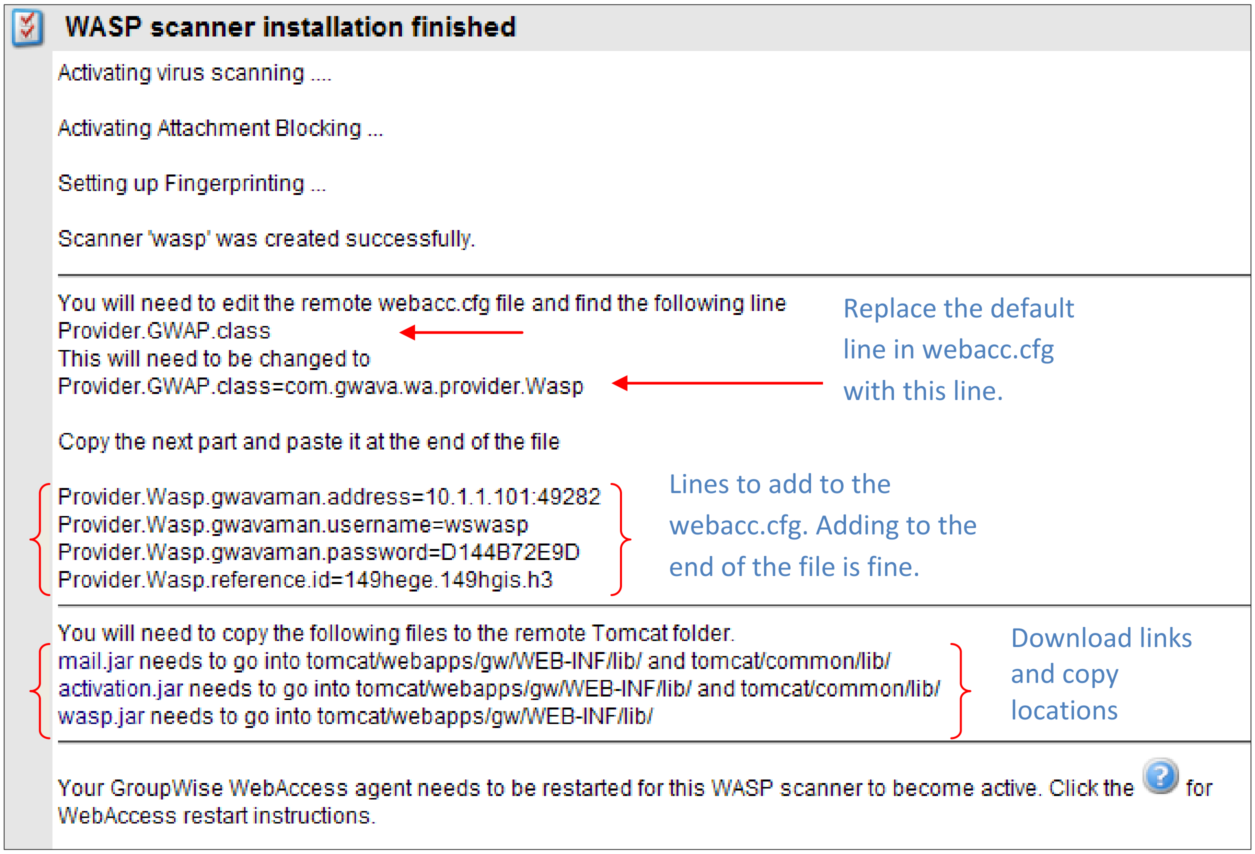


**Create new WASP scanner**

The requisite information has been collected and is ready to be deployed. If you are satisfied that the installation information is correct, press the install button to commit the installation procedure to the GWAVA network.

| | |
|---|---|
| Scanner name | WASP 2 |
| Install to server | bitterlinux (Linux) |
| WebAccess startup file | not/valid/path |
| Tomcat directory | /not/valid/path |
| Stop Viruses | Yes |

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 4.5 server and perform scans. **Make sure you copy the supplied lines before browsing away from this page.**



**WASP scanner installation finished**

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Scanner 'wasp' was created successfully.

You will need to edit the remote webacc.cfg file and find the following line
Provider.GWAP.class
This will need to be changed to
Provider.GWAP.class=com.gwava.wa.provider.Wasp

Replace the default line in webacc.cfg with this line.

Copy the next part and paste it at the end of the file

```
Provider.Wasp.gwavaman.address=10.1.1.101:49282
Provider.Wasp.gwavaman.username=wswasp
Provider.Wasp.gwavaman.password=D144B72E9D
Provider.Wasp.reference.id=149hege.149hgis.h3
```

Lines to add to the webacc.cfg. Adding to the end of the file is fine.

You will need to copy the following files to the remote Tomcat folder.
mail.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/ and tomcat/common/lib/
activation.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/ and tomcat/common/lib/
wasp.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/

Download links and copy locations

Your GroupWise WebAccess agent needs to be restarted for this WASP scanner to become active. Click the ? for WebAccess restart instructions.

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 scanner will become active.

## Recommended Scanner configuration

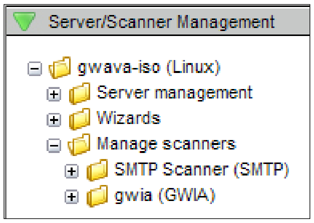
Every scanner configuration will be different depending on the different situations existing in the email world. ***However, the recommended settings are set as default, and no changes are needed to implement the best settings for a general system.***

The default settings for all scanners are as follows:

- Signature spam engine enabled
- RBL and SURBL block enabled
- Conversation Tracking enabled

The SMTP scanner also has IP Reputation enabled by default. The Signature spam engine ONLY works on Linux. Linux is the recommended platform for GWAVA.

For every situation it may become necessary to create exceptions to the scanning rules as well as adjustments to the different scanners and text filters to catch unwanted mail. Create these new rules and exceptions as required. The rules and settings for individual scanners are found under **Server/Scanner Management |<Server-name> | Manage Scanners | <Scanner name>**. See the respective sections for information on how to use each section.



## 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 scanners: scanner 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 Management home page. This page displays the system status along with News and Updates for your GWAVA 4.5 system. If there is an update available, you will be notified in the News/Updates section.

The System Status window will show your evaluation deadline, if you have not licensed your GWAVA 4.5 system, as well as the blocking statistics for your server. 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.

## Webinars

The Recorded Webinars is a link to a web page containing instructional web videos for all GWAVA products. To view the videos, simply select the desired product video name. The GWAVA 4.5 video is lower on the page, and walks through the beginning installation and setup of the GWAVA 4.5 system.

## Computer based training

Links to a recorded web training session is available through this link.

## 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 the 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 a scanner, such as scanner statistics or exceptions.

## System management

Under the System management link, default settings for the system are listed. The settings here are the base used when creating scanners. Each scanner's settings may be modified individually after scanner creation, but by changing the default settings here each scanner 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 item, while the Advanced section contains tools which should be generally left alone unless specified by support.

### System Management

### Admin accounts

Admin accounts allow you to add and remove administrator accounts from the GWAVA 4.5 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 4.5

are listed here, along with their latest report-in date, time, and location.  This page provides basic information on the system at a glance.

## 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 scanners read from. It is vitally important that the information supplied for this page is correct for the mail system.

The default internet domain as well as any additional domains determine which mail domain GWAVA 4.5 will allow through. If the domain listed is not part of your mail domain, or your mail domain is not listed, email will not be processed correctly.

The Administrator email address and name supplied here will appear on all mail notifications and digests sent by the GWAVA 4.5 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 4.5 system shows on the GWAVA 4.5 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/Scanner 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 4.5 will contact the update server and begin the download and update process.

## Package manager

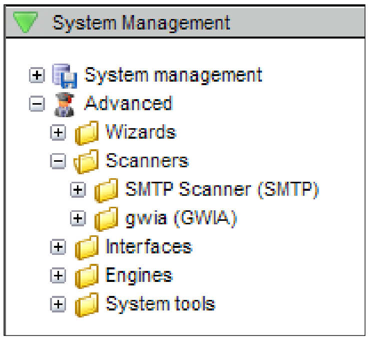
The Package manager allows the addition of third party and additional plugins to be added and installed to the GWAVA 4.5 mail system.

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 4.5 system. The uploaded package is usually zipped, and the GWAVA 4.5 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 4.5 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 nearly identical to the scanning configuration under Server/Scanner Management, but differs in that the advanced configuration items modify scanning engines, and not individual scanners, which means that if multiple scanners have been configured to share an existing scanning configuration or engine, that both scanners may be modified at the same time from this location. If the scanners in the system do not share configuration, it is recommended to use the Server/Scanner Management menu to configure them, to ensure that the correct scanner is modified. Items listed under 'Advanced' which are listed under the **Server/Scanner Management** section are explained where they reside under the **Scanner management** section. The menu items which are separate from the scanner tree found below are explained here.

## System Tools

System Tools contains powerful tools which modify the core system of a GWAVA 4.5 server. These tools are not to be used on a regular basis, and should not be used unless instructed to do so by GWAVA 4.5 support. Editing the database, removing objects and modifying Servers in the GWAVA 4.5 network may render the GWAVA 4.5 system inoperative.  Only proceed with such operations if you fully understand the process and possible repercussions and on instructions by GWAVA 4.5 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 4.5 system to other servers in a GWAVA network. This is useful to share dictionaries, settings, and statistics between multiple servers in your network. The connection between two GWAVA servers is created during server activation. Instead of setting up the GWAVA 4.5 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 4.5 configuration database. This can be used in coordination with GWAVA 4.5 support to correct some corruption and add or fix missing items in the database on occasion.

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 4.5 maintenance are listed here. Removing and renaming a GWAVA 4.5 server from the GWAVA 4.5 networks correctly severs or renames a connection between two GWAVA 4.5 servers. Removing a connected server from a network should be done prior to uninstalling the GWAVA 4.5 server in order to avoid connection issues with the remaining GWAVA 4.5 server(s).

Due to updates and changes in the GWAVA 4.5 interface, it may be necessary to rebuild the system Menu's Selecting this option causes the GWAVA 4.5 system to discard the current menu tree and system in the GWAVA 4.5 interface, and recreated them from the current system files.  If a new item has been installed or downloaded to the GWAVA 4.5 system during an update and a menu rebuild is appropriate, you will be notified on the default GWAVA 4.5 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.

### *Scanner Object Map*

The scanner map menu section is simply a linear object tree showing associations of the different scanner objects.  Multiple scanners will show multiple maps in a separate row. The view can be spawned in a scrollable window via a link at the top of the page.  Also along the top of the page, are tabs which change the 'map' shown for each scanner and interface.  This page does not have any editing windows.

## Server/Scanner Management

The Server/Scanner Management is setup in a directory tree-view organized around tasks.  The Server management offers active setup information on the GWAVA 4.5 server. The Wizards menu contains all scanner creation options. The Manage scanners menu contains all currently active and created scanners and their configuration options.

### Server management

This menu contains all of the active settings in the GWAVA 4.5 system for the GWAVA 4.5 server. Editing and saving changes in this section changes the active settings in the GWAVA 4.5 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.

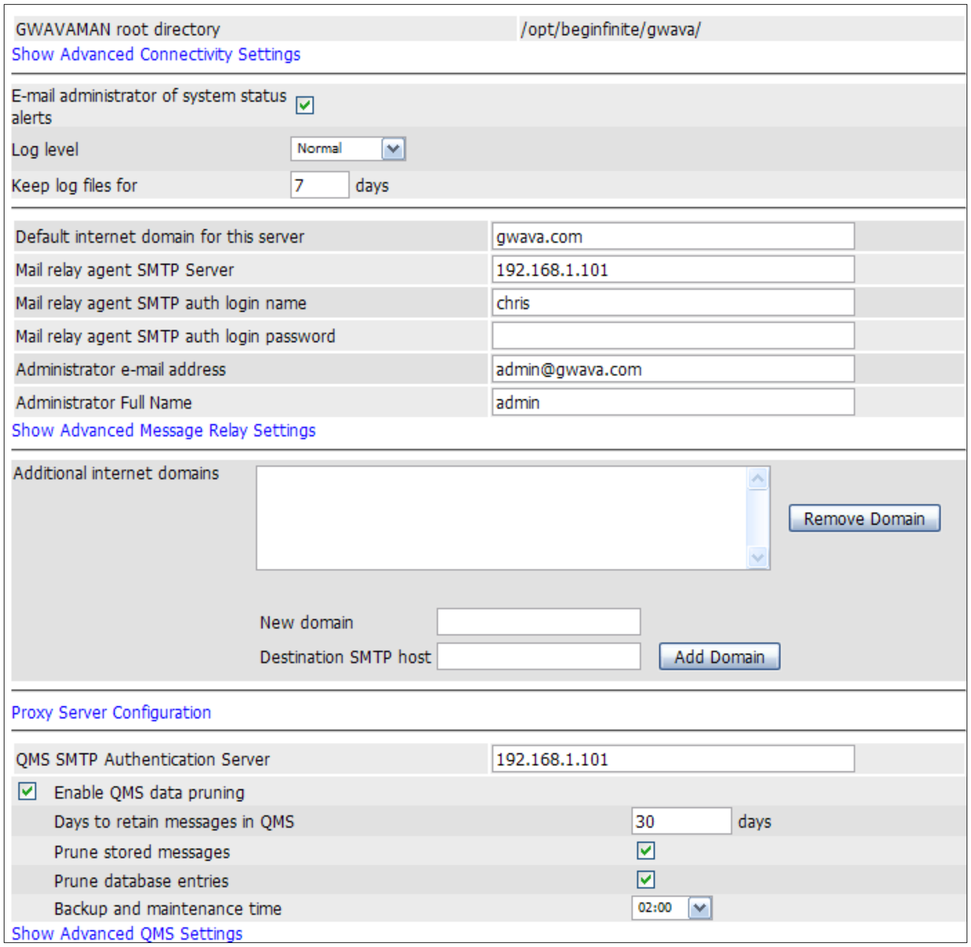
## Configure Server

In the Configure server window, the basic connection settings for the server are listed. The default log level, internet domain and any additional domains you wish GWAVA to accept mail for, the SMTP connection and authorization, and the administrator address and name are configured on this page.

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.

All domains for which the host mail system receives 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.

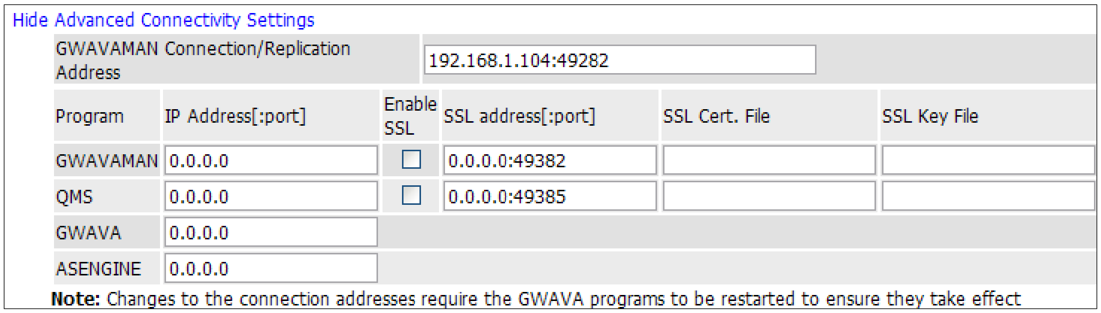
The QMS authentication server should be the connection to the GWIA for GroupWise systems, in order to allow user-level access to the quarantine manager for each user’s respective quarantined mail.



| | |
|---|---|
| GWAVAMAN root directory | /opt/beginfinite/gwava/ |
| E-mail administrator of system status alerts | ☑ |
| Log level | Normal |
| Keep log files for | 7 days |
| Default internet domain for this server | gwava.com |
| Mail relay agent SMTP Server | 192.168.1.101 |
| Mail relay agent SMTP auth login name | chris |
| Mail relay agent SMTP auth login password | |
| Administrator e-mail address | admin@gwava.com |
| Administrator Full Name | admin |
| Additional internet domains | |
| New domain | |
| Destination SMTP host | |
| QMS SMTP Authentication Server | 192.168.1.101 |
| ☑ Enable QMS data pruning | |
| Days to retain messages in QMS | 30 days |
| Prune stored messages | ☑ |
| Prune database entries | ☑ |
| Backup and maintenance time | 02:00 |

Show Advanced Connectivity Settings
Show Advanced Message Relay Settings
Remove Domain
Add Domain
Proxy Server Configuration
Show Advanced QMS Settings

SSL configuration is offered on the Linux OS platform, and is setup under the ‘Advanced Connectivity Settings’ link, which exposes the options on the page.



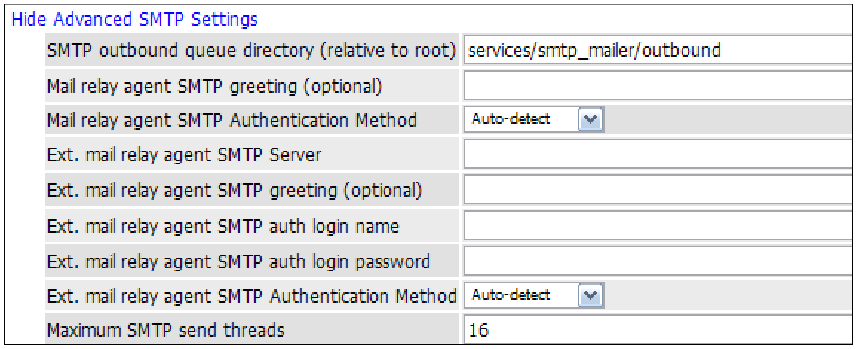
Hide Advanced Connectivity Settings

| | |
|---|---|
| GWAVAMAN Connection/Replication Address | 192.168.1.104:49282 |

| Program | IP Address[:port] | Enable SSL | SSL address[:port] | SSL Cert. File | SSL Key File |
|---|---|---|---|---|---|
| GWAVAMAN | 0.0.0.0 | □ | 0.0.0.0:49382 | | |
| QMS | 0.0.0.0 | □ | 0.0.0.0:49385 | | |
| GWAVA | 0.0.0.0 | | | | |
| ASENGINE | 0.0.0.0 | | | | |

**Note:** Changes to the connection addresses require the GWAVA programs to be restarted to ensure they take effect

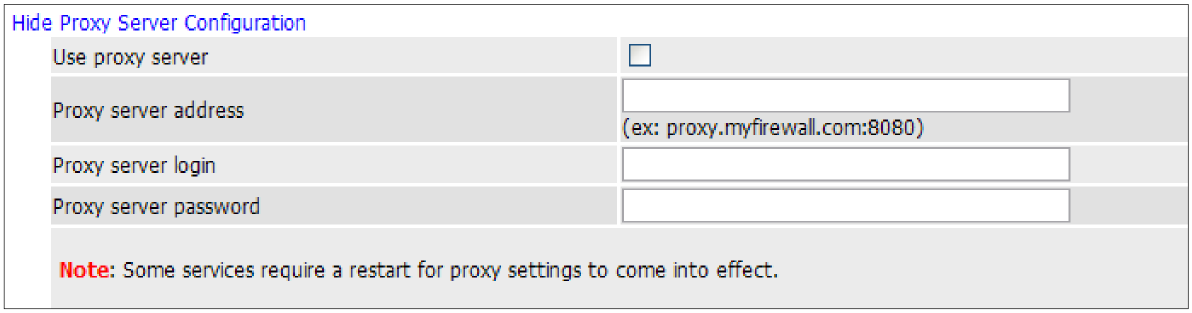
The connection addresses for the different objects in GWAVA 4.5 are listed and configured on this page. *There is no reason to configure these settings on standard GWAVA 4.5 installations*. These settings should not be changed unless instructed by GWAVA support.



Hide Advanced SMTP Settings

| | |
|---|---|
| SMTP outbound queue directory (relative to root) | services/smtp_mailer/outbound |
| Mail relay agent SMTP greeting (optional) | |
| Mail relay agent SMTP Authentication Method | Auto-detect |
| Ext. mail relay agent SMTP Server | |
| Ext. mail relay agent SMTP greeting (optional) | |
| Ext. mail relay agent SMTP auth login name | |
| Ext. mail relay agent SMTP auth login password | |
| Ext. mail relay agent SMTP Authentication Method | Auto-detect |
| Maximum SMTP send threads | 16 |

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.  Default is shown.

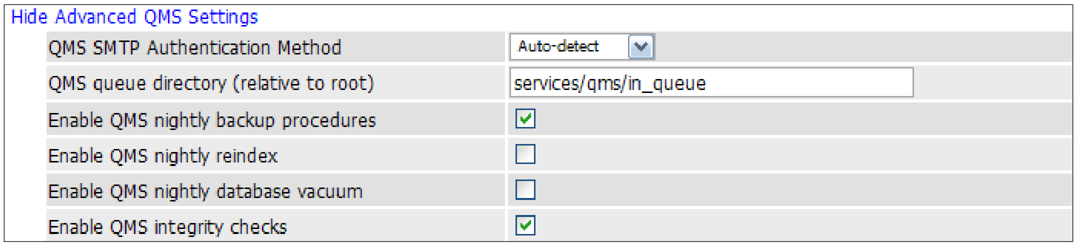


Hide Proxy Server Configuration

| | |
|---|---|
| Use proxy server | □ |
| Proxy server address | (ex: proxy.myfirewall.com:8080) |
| Proxy server login | |
| Proxy server password | |

**Note**: Some services require a restart for proxy settings to come into effect.

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


Hide Advanced QMS Settings

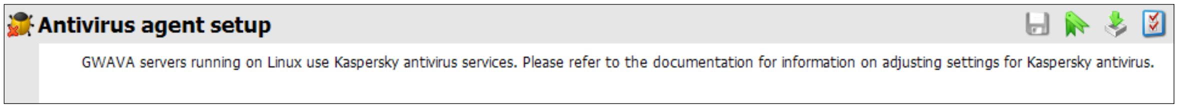
| | |
|---|---|
| QMS SMTP Authentication Method | Auto-detect |
| QMS queue directory (relative to root) | services/qms/in_queue |
| Enable QMS nightly backup procedures | ☑ |
| Enable QMS nightly reindex | □ |
| Enable QMS nightly database vacuum | □ |
| Enable QMS integrity checks | ☑ |

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 run, and should only be done so under the direction of support.

## Antivirus agent setup

### Linux

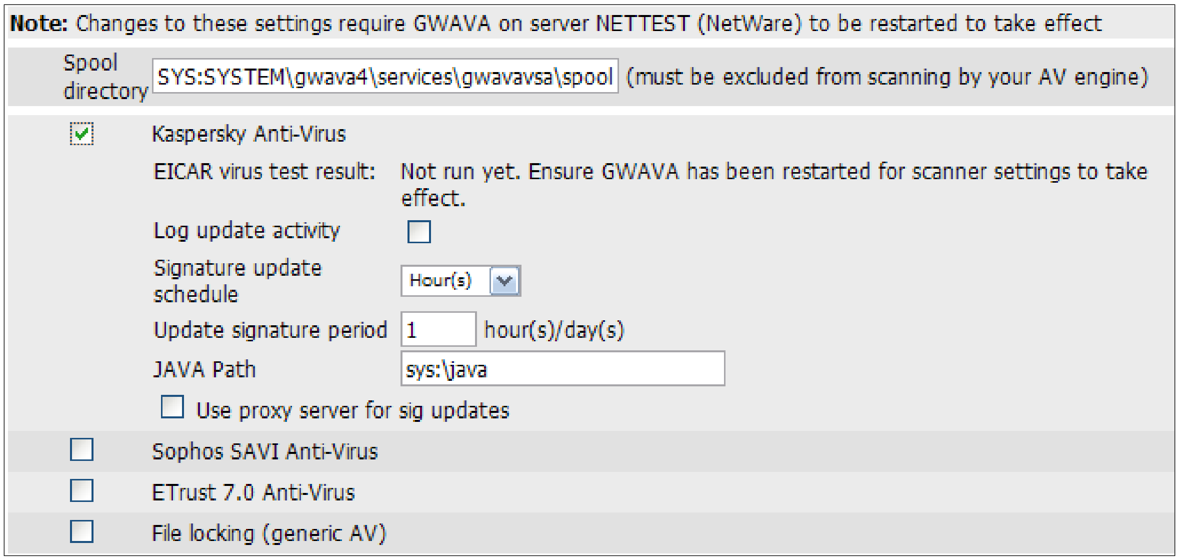
Linux systems do not need to specify or choose an antivirus engine, as the Kaspersky engine is the only one available and runs automatically. Kaspersky Antivirus will connect to the internet and download virus updates regularly, therefore the Linux antivirus only needs to be configured if the network 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/Scanner Management | <Server name> | Configure Server** page under the **Proxy Server Configuration** section.)


**Antivirus agent setup**

GWAVA servers running on Linux use Kaspersky antivirus services. Please refer to the documentation for information on adjusting settings for Kaspersky antivirus.

### NetWare

NetWare systems have several options when it comes to Antivirus software integration, though it is highly recommended to utilize the Kaspersky antivirus option as it comes integrated into the GWAVA 4.5 system and guarantees smooth function. Changes to the antivirus integration require a GWAVA 4.5 restart before any changes become active.



**Note:** Changes to these settings require GWAVA on server NETTEST (NetWare) to be restarted to take effect

Spool directory SYS:SYSTEM\gwava4\services\gwavavsa\spool (must be excluded from scanning by your AV engine)

☑ Kaspersky Anti-Virus

EICAR virus test result: Not run yet. Ensure GWAVA has been restarted for scanner settings to take effect.

Log update activity □

Signature update schedule Hour(s)

Update signature period 1 hour(s)/day(s)

JAVA Path sys:\java

□ Use proxy server for sig updates

□ Sophos SAVI Anti-Virus

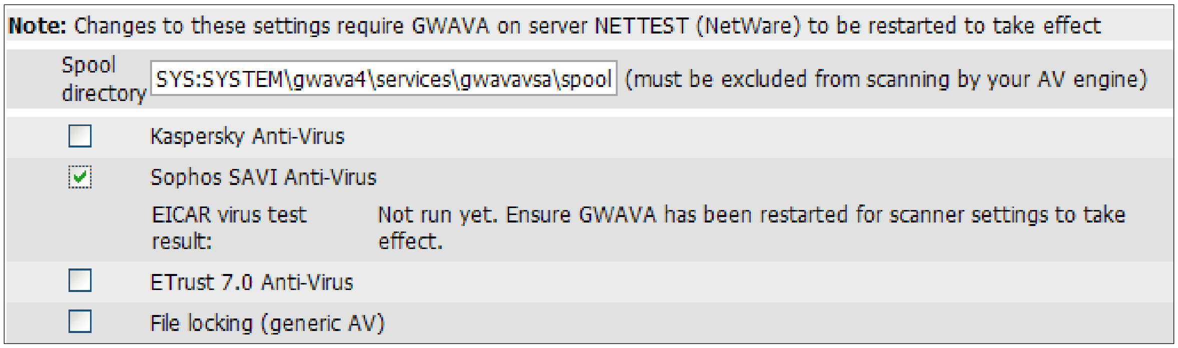
□ ETrust 7.0 Anti-Virus

□ File locking (generic AV)

The Spool directory is the location where GWAVA 4.5 receives files and places them for scanning. If the spool directory is not excluded from scanning then GWAVA 4.5 will become unreliable for antivirus statistics, scanning, and may become unstable as files currently being used or worked on by GWAVA 4.5 may be removed or locked by a resident antivirus scanner. (If there are multiple antivirus scanners on the system, the spool location MUST still be excluded from scanning.)

If the network requires a proxy server to connect to the internet, check the 'Use proxy server for sig updates' option to expand the Proxy server configuration, and enter the proxy server address, and any authentication information required. For Kaspersky, this is the only configuration required.

**For all virus integration, (other than Kaspersky), the antivirus engine should be running before GWAVA 4.5 starts, or the connection will fail.** Ensure the antivirus system is running and available before GWAVA 4.5 is started and attempts to connect to the antivirus system. Placing a delay or changing the start order in the host system autoexec.ncf file may suffice.



**Note:** Changes to these settings require GWAVA on server NETTEST (NetWare) to be restarted to take effect

Spool directory SYS:SYSTEM\gwava4\services\gwavavsa\spool (must be excluded from scanning by your AV engine)

□ Kaspersky Anti-Virus

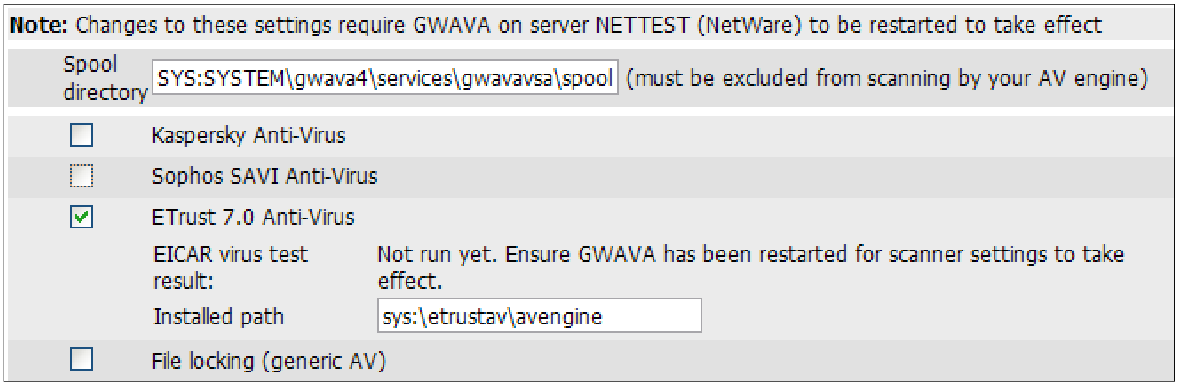
☑ Sophos SAVI Anti-Virus

EICAR virus test result: Not run yet. Ensure GWAVA has been restarted for scanner settings to take effect.

□ ETrust 7.0 Anti-Virus

□ File locking (generic AV)

If **Sophos** SAVI Anti-Virus is used, simply selecting and ensure the spool directory is excluded, then restarting GWAVA 4.5 is sufficient.



**Note:** Changes to these settings require GWAVA on server NETTEST (NetWare) to be restarted to take effect

Spool directory SYS:SYSTEM\gwava4\services\gwavavsa\spool (must be excluded from scanning by your AV engine)

□ Kaspersky Anti-Virus

□ Sophos SAVI Anti-Virus

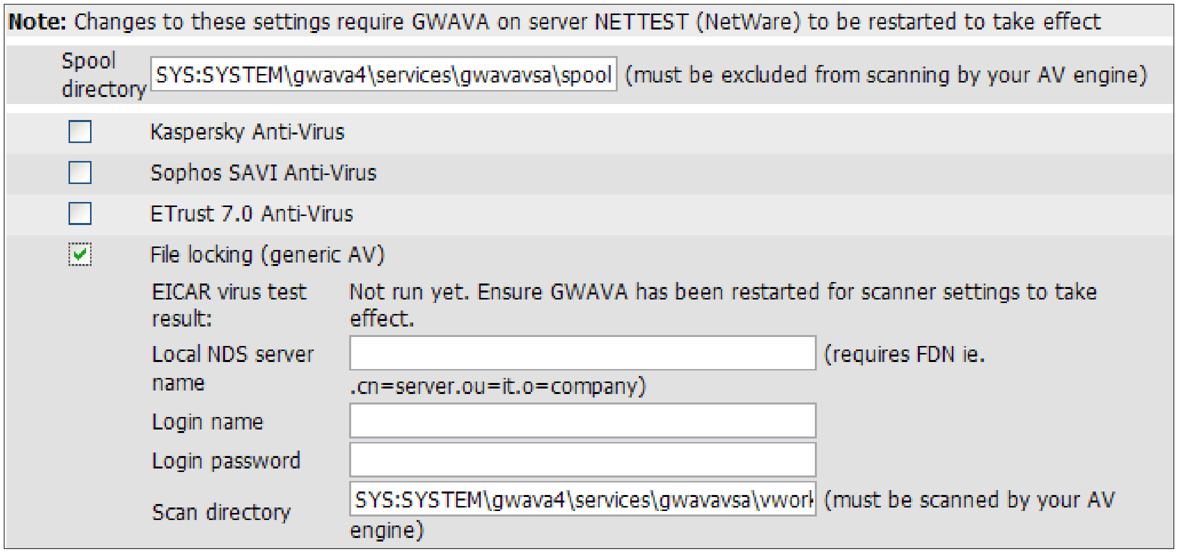
☑ ETrust 7.0 Anti-Virus

EICAR virus test result: Not run yet. Ensure GWAVA has been restarted for scanner settings to take effect.

Installed path sys:\etrustav\avengine

□ File locking (generic AV)

ETrust 7.0 Anti-Virus integration is also supported, though it requires a specified install path in order to connect to the antivirus scanner. Once again, ensure that the spool directory specified above is excluded from the antivirus scanner. A GWAVA 4.5 restart is required before changes take effect.



**Note:** Changes to these settings require GWAVA on server NETTEST (NetWare) to be restarted to take effect

Spool directory SYS:SYSTEM\gwava4\services\gwavavsa\spool (must be excluded from scanning by your AV engine)

□ Kaspersky Anti-Virus

□ Sophos SAVI Anti-Virus

□ ETrust 7.0 Anti-Virus

☑ File locking (generic AV)

EICAR virus test result: Not run yet. Ensure GWAVA has been restarted for scanner settings to take effect.

Local NDS server name (requires FDN ie. .cn=server.ou=it.o=company)

Login name

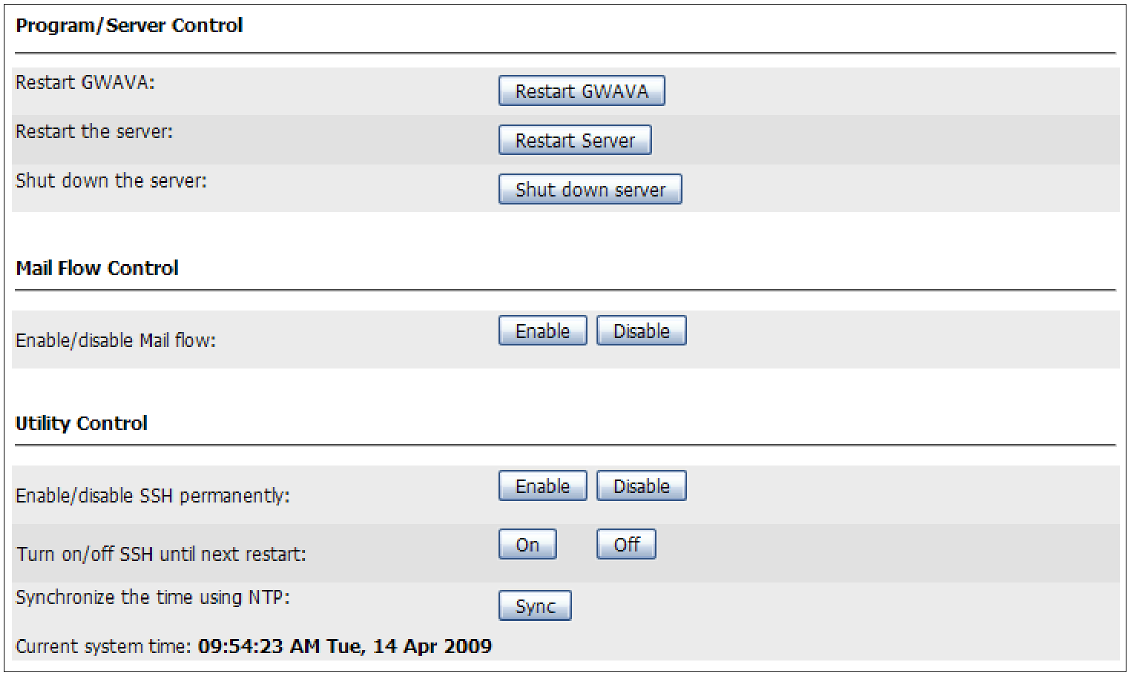
Login password

Scan directory SYS:SYSTEM\gwava4\services\gwavavsa\vwork (must be scanned by your AV engine)

If a different antivirus engine is present, the generic antivirus **File Locking** option may suffice. To enable generic file locking on NetWare, admin NDS rights are required. Specify the local NDS server, (using FDN format, as shown in the example), an administrator login name, and the correct password.

The Spool directory must still be excluded from scanning, but since the file locking is generic, the scan directory must also be specified. **The scan directory MUST be scanned by the antivirus engine**. Check and configure the antivirus engine to ensure that the spool directory is excluded, and the scan directory is included in the scanning configuration.

## Appliance control



**Program/Server Control**

| | |
|---|---|
| Restart GWAVA: | Restart GWAVA |
| Restart the server: | Restart Server |
| Shut down the server: | Shut down server |

**Mail Flow Control**

| | |
|---|---|
| Enable/disable Mail flow: | Enable Disable |

**Utility Control**

| | |
|---|---|
| Enable/disable SSH permanently: | Enable Disable |
| Turn on/off SSH until next restart: | On Off |
| Synchronize the time using NTP: | Sync |

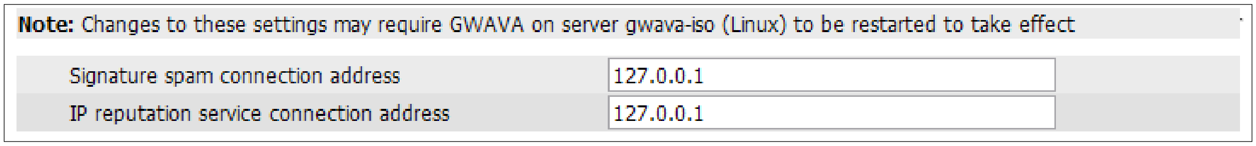
Current system time: **09:54:23 AM Tue, 14 Apr 2009**

If the GWAVA Server was installed using the GWAVA Appliance ISO, then the Appliance Control menu will be available to provide the base control of the appliance. The commands are self-explanatory; Restart GWAVA, Restart Server, Shut down server, Enable/disable Mail flow, SSH configuration, and NTP sync.

Selecting Enable/disable mail flow performs different actions depending on the type of scanner(s) connected to the system. If a SMTP scanner is connected, the receive threads will be closed, causing a the sending servers to retry sending mail later, while all other scanners will still accept mail, but queue it in a holding directory, waiting to be processed later when the mail flow is once again enabled.

Unless configured otherwise, SSH access will be opened or disabled for the default port, (22).

## SigSpam / IPRep agent setup



**Note:** Changes to these settings may require GWAVA on server gwava-iso (Linux) to be restarted to take effect

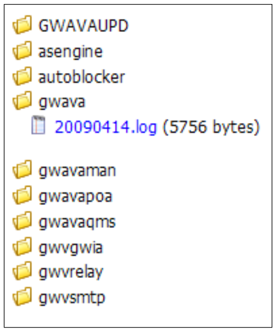
| | |
|---|---|
| Signature spam connection address | 127.0.0.1 |
| IP reputation service connection address | 127.0.0.1 |

If the GWAVA 4.5 server is installed on Netware, the signature spam engine and the ip reputation services will not be available on the local server, as they are only offered on Linux. However, a GWAVA server on Linux may provide the scanning engine for the Netware box. The connection address should be an unblocked network connection to a functioning GWAVA 4.5 server running on a Linux platform.

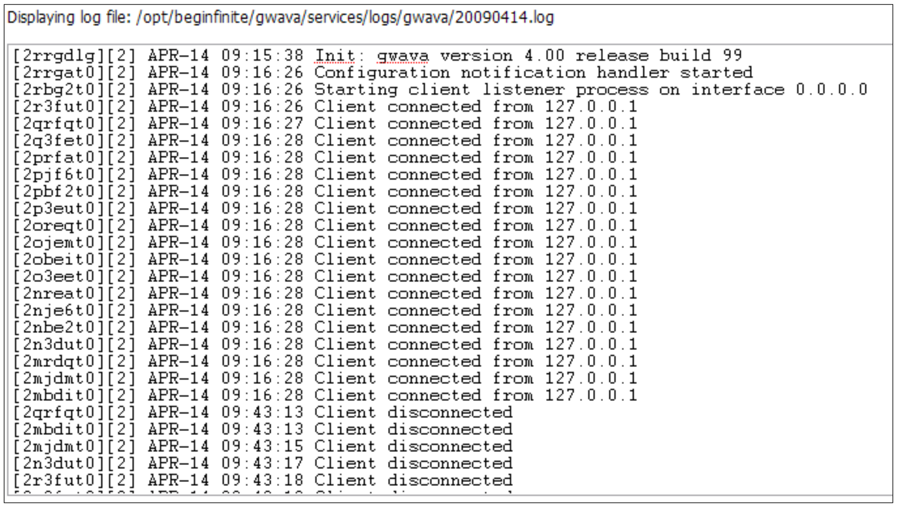
## Logs

GWAVA 4.5 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>



GWAVAUPD
asengine
autoblocker
gwava
20090414.log (5756 bytes)
gwavaman
gwavapoa
gwavaqms
gwvgwia
gwvrelay
gwvsmtp



Displaying log file: /opt/beginfinite/gwava/services/logs/gwava/20090414.log

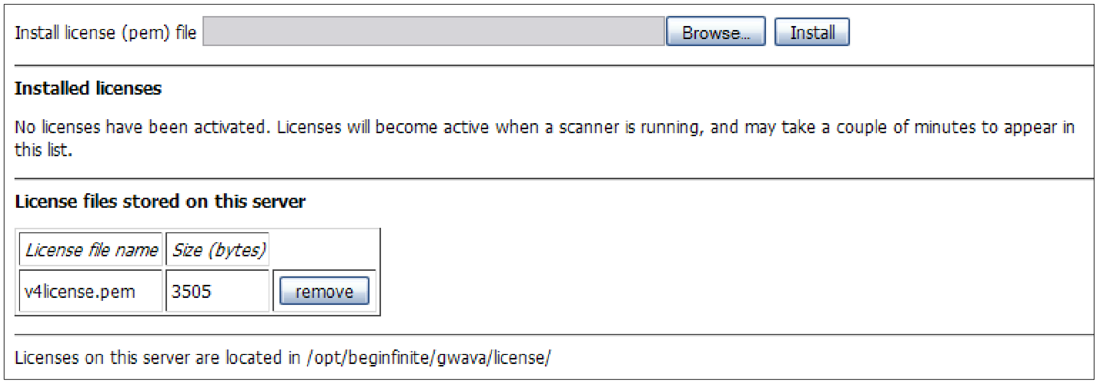
```
[2rrgdlg][2] APR-14 09:15:38 Init: gwava version 4.00 release build 99
[2rrgat0][2] APR-14 09:16:26 Configuration notification handler started
[2rbg2t0][2] APR-14 09:16:26 Starting client listener process on interface 0.0.0.0
[2r3fut0][2] APR-14 09:16:26 Client connected from 127.0.0.1
[2qrfqt0][2] APR-14 09:16:27 Client connected from 127.0.0.1
[2q3fet0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2prfat0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2pjf6t0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2pbf2t0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2p3eut0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2oreqt0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2ojemt0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2obeit0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2o3eet0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2nreat0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2nje6t0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2nbe2t0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2n3dut0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2mrdqt0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2mjdmt0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2mbdit0][2] APR-14 09:16:28 Client connected from 127.0.0.1
[2qrfqt0][2] APR-14 09:43:13 Client disconnected
[2mbdit0][2] APR-14 09:43:13 Client disconnected
[2mjdmt0][2] APR-14 09:43:15 Client disconnected
[2n3dut0][2] APR-14 09:43:17 Client disconnected
[2r3fut0][2] APR-14 09:43:18 Client disconnected
```

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

gwava – the main scanner
gwavapoa – post office scanner
gwavaman – management
gwavaqms – quarantine manager

## Licensing

GWAVA 4.5 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.



**Installed licenses**

No licenses have been activated. Licenses will become active when a scanner is running, and may take a couple of minutes to appear in this list.

**License files stored on this server**

| *License file name* | *Size (bytes)* | |
|---|---|---|
| v4license.pem | 3505 | remove |

Licenses on this server are located in /opt/beginfinite/gwava/license/

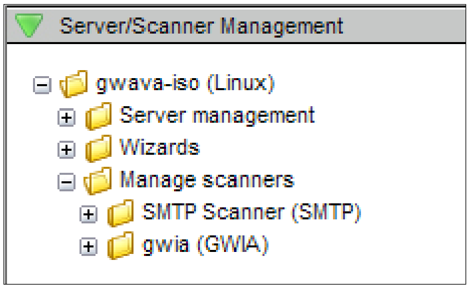
If no licenses are present, the window will state that no licenses have been found. To install a license, select the 'Browse' button and locate the unzipped license file (.pem). After the license file has been located and selected, click the 'Install' button and the license file will be uploaded to the GWAVA 4.5 server. GWAVA 4.5 will look for, and recognize the license file in a few minutes. If impatient, restarting GWAVA 4.5 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 4.5 server is listed at the bottom of the screen.

## Wizards

This feature is covered under the scanner creation section.

## Manage scanners

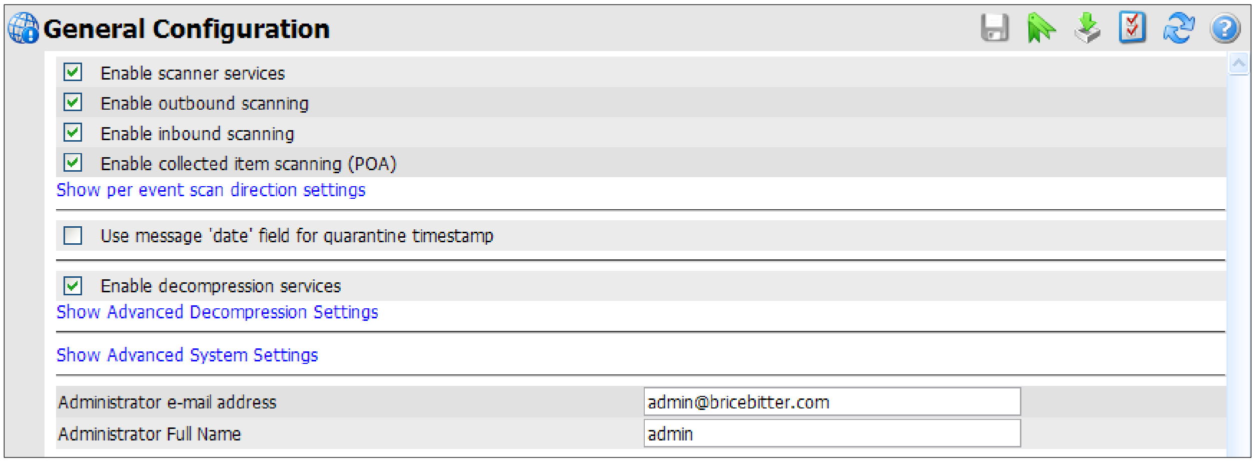
The Manage Scanners menu option contains the settings for each scanner, organized under each scanner's name. To bulk modify scanners, the scanners must share a scanner engine. See the 'Advanced' section for more information.



## Manage Scanners

The General settings of each scanner configuration contains the basic settings for the system configuration and the notification settings.

### General Configuration


General Configuration

☑ Enable scanner services
☑ Enable outbound scanning
☑ Enable inbound scanning
☑ Enable collected item scanning (POA)
Show per event scan direction settings

☐ Use message 'date' field for quarantine timestamp

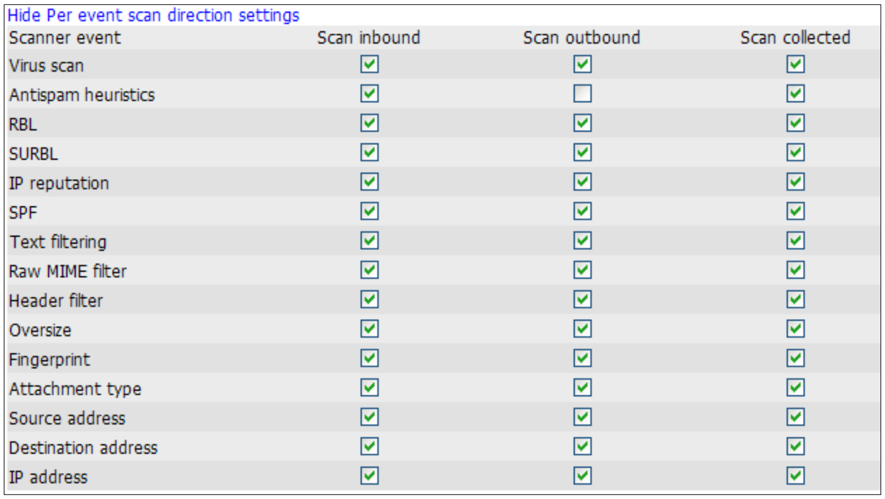
☑ Enable decompression services
Show Advanced Decompression Settings

Show Advanced System Settings

| | |
|---|---|
| Administrator e-mail address | admin@bricebitter.com |
| Administrator Full Name | admin |

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

The defaults for the above settings are shown, (all enabled).

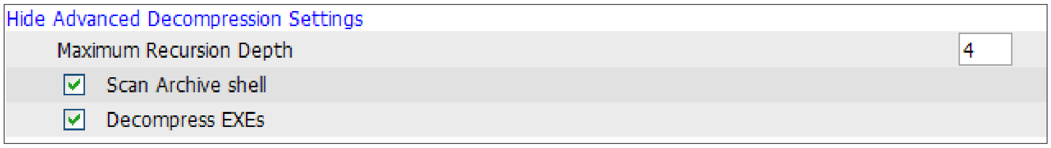


Hide Per event scan direction settings

| Scanner event | Scan inbound | Scan outbound | Scan collected |
|---|---|---|---|
| Virus scan | ☑ | ☑ | ☑ |
| Antispam heuristics | ☑ | □ | ☑ |
| RBL | ☑ | ☑ | ☑ |
| SURBL | ☑ | ☑ | ☑ |
| IP reputation | ☑ | ☑ | ☑ |
| SPF | ☑ | ☑ | ☑ |
| Text filtering | ☑ | ☑ | ☑ |
| Raw MIME filter | ☑ | ☑ | ☑ |
| Header filter | ☑ | ☑ | ☑ |
| Oversize | ☑ | ☑ | ☑ |
| Fingerprint | ☑ | ☑ | ☑ |
| Attachment type | ☑ | ☑ | ☑ |
| Source address | ☑ | ☑ | ☑ |
| Destination address | ☑ | ☑ | ☑ |
| IP address | ☑ | ☑ | ☑ |

The Per event scan direction settings perform the same as the global settings described above, except that it only applies to specific scanner events. The default is shown, with all enabled except outbound Antispam scanning. In example: if SURBL, RBL, IP reputation or SPF are enabled on the scanner, 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 scanner. The 'Scan Collected' box ONLY applies to scanning a GroupWise Post Office, and will only be useful if the scanner being modified is a POA scanner.

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



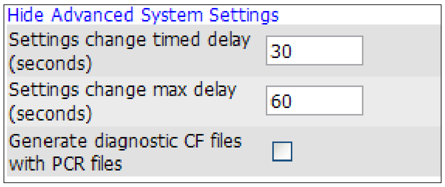
Hide Advanced Decompression Settings

Maximum Recursion Depth 4

☑ Scan Archive shell

☑ Decompress EXEs

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.

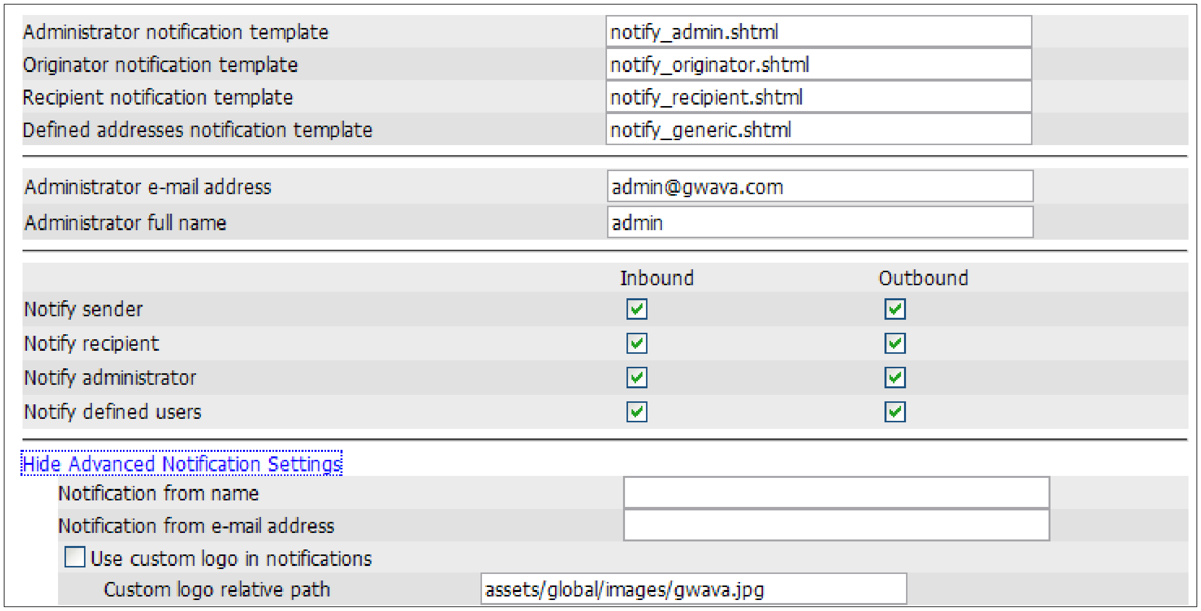


Hide Advanced System Settings

| | |
|---|---|
| Settings change timed delay (seconds) | 30 |
| Settings change max delay (seconds) | 60 |
| Generate diagnostic CF files with PCR files | □ |

By default, GWAVA 4.5 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



| | |
|---|---|
| Administrator notification template | notify_admin.shtml |
| Originator notification template | notify_originator.shtml |
| Recipient notification template | notify_recipient.shtml |
| Defined addresses notification template | notify_generic.shtml |

| | |
|---|---|
| Administrator e-mail address | admin@gwava.com |
| Administrator full name | admin |

| | Inbound | Outbound |
|---|---|---|
| Notify sender | ☑ | ☑ |
| Notify recipient | ☑ | ☑ |
| Notify administrator | ☑ | ☑ |
| Notify defined users | ☑ | ☑ |

Hide Advanced Notification Settings

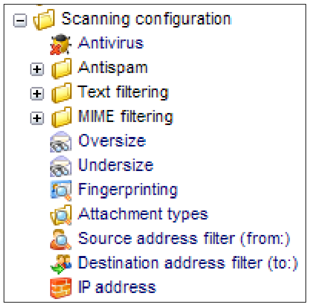
| | |
|---|---|
| Notification from name | |
| Notification from e-mail address | |
| □ Use custom logo in notifications | |
| Custom logo relative path | assets/global/images/gwava.jpg |

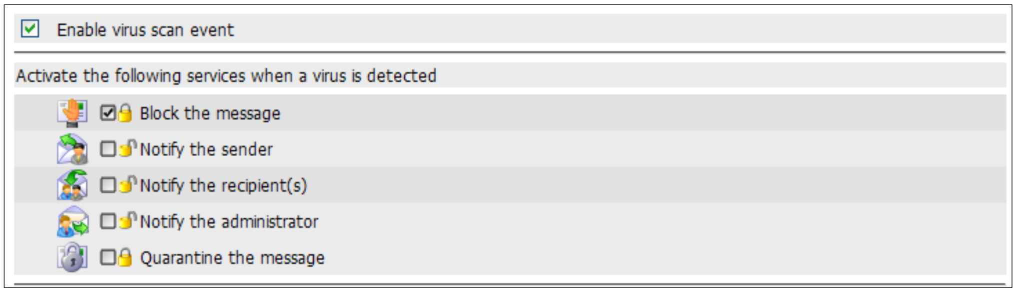
The notification options allow you to specify which templates are used to create the message, the send from address, (the admin address and name are the default used as the 'From:' address), and the events specified for notification. Events specified for notification here still depend on the notification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





☑ Enable virus scan event

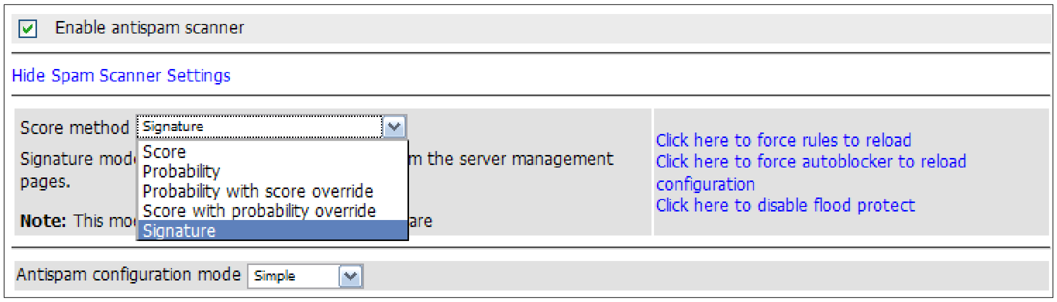
Activate the following services when a virus is detected

- ☑ Block the message
- □ Notify the sender
- □ Notify the recipient(s)
- □ Notify the administrator
- □ Quarantine the message

## Antispam | Heuristics

### *Spam Scanning Engines*

The different scanner engines may be selected for use under the **Heuristics** page, by selecting the '**show spam scanner** settings' text link, then selecting the different scanners from the '**Score method**' drop down menu.



☑ Enable antispam scanner

Hide Spam Scanner Settings

Score method Signature

Signature mod m the server management pages.

**Note:** This mo are

Click here to force rules to reload
Click here to force autoblocker to reload configuration
Click here to disable flood protect

Antispam configuration mode Simple

Score
Probability
Probability with score override
Score with probability override
Signature

The **Signature** engine, (only available on Linux), replaces the original anti-spam heuristic engine, and uses definitions and rules in an advanced method to block and sort spam. False positives are virtually non-existent and the signature engine requires no training whatsoever. Periodic updates to the rule set will be performed with the system update, when appropriate. **The Signature engine is highly recommended**. The Signature engine replaces the following two spam engines, and should be used in place of the following scanners.

The **Score** method is the heuristic scanning engine which uses a set collection of rules to grade and categorize spam. Every word or empty white space in a message combines to form a total score for each message, which is then compared to a 'threshold' score level. Mail that passes 'under' the threshold score level is allowed to continue into the system, while mail that does not exceeds the threshold score level is blocked and/or placed into the quarantine .

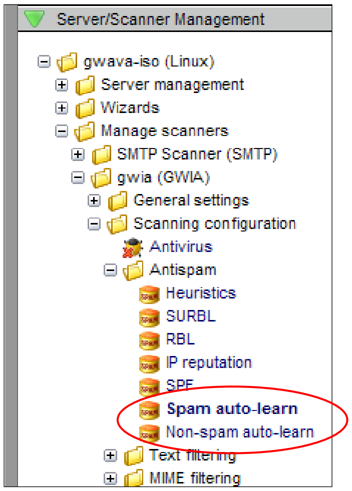
The **Probability** engine is the advanced intelligent learning engine that will actively create and change rule sets based on mail fed into the learning system. This allows the administrator to actively create custom scanner based on the mail the organization keeps and sends.   To use this engine effectively, it must be trained. Until there is a minimum of 1000 'ham' and 5000 'spam'  example messages in the learning database, the probability engine will be unreliable.

The best way to train the probability engine is through the auto-learn feeders.  The Non-span auto learn, and the Spam auto-learn services take a carbon copy of a message and place that into the advanced learning engine of GWAVA 4.5. The learning engine then consumes the message and creates a rule set based on the message, either for spam, or for non-spam, or 'ham'. None of the auto-learn training methods will disrupt the delivery of mail to users in the system. These methods are completely transparent to standard users.

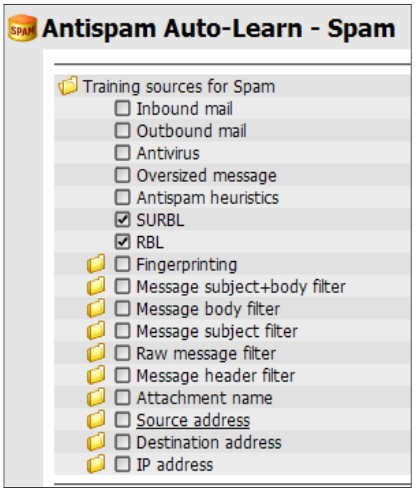
The defaults for each service and best practices are listed below.

## Spam auto-learn

The **Spam auto-learn** menu, when expanded, looks as shown with SURBL and RBL selected as training sources by default. SURBL alone is a sufficient source for training the probability engine for spam, but extending the training to RBL expands and accelerates the process. DO NOT use outbound mail or inbound mail for spam training.



The Source address option allows for the creation of a 'honey pot' account or accounts that will only receive spam, and automatically adds copies of the messages and adds them to the advanced learning engine. Source addresses, as well as any item in this list marked with a folder, may be expanded and event items individually selected or excluded. Some of the item events here must be created by the admin. To create an item event, add a new item to the filter that matches the folder item desired. For example; to create a source address to train from, enter a new address to the **Source address (from:)** filter, then return to this dialog and select the desired address as a learning source.

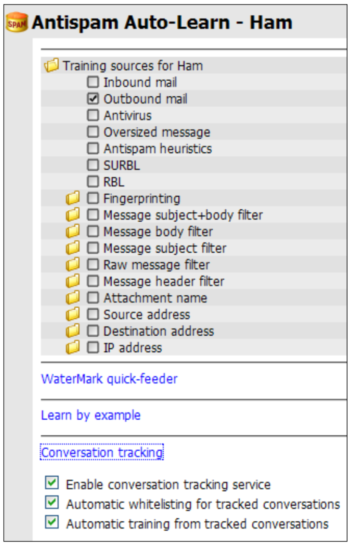


Antispam Auto-Learn - Spam

Training sources for Spam
☐ Inbound mail
☐ Outbound mail
☐ Antivirus
☐ Oversized message
☐ Antispam heuristics
☑ SURBL
☑ RBL
☐ Fingerprinting
☐ Message subject+body filter
☐ Message body filter
☐ Message subject filter
☐ Raw message filter
☐ Message header filter
☐ Attachment name
☐ Source address
☐ Destination address
☐ IP address

## Non-spam auto learn

The Non-spam, or Ham auto-learn menu options are nearly identical to the spam auto-learn. Outbound mail and Conversation tracking are enabled by default. With outbound mail, every message that passes through the GWAVA scanner to destinations outside the host domain will have an identical copy placed in the advanced learning database, as an example of good mail. Because ham requires examples of good mail, any source of mail that could include spam should NOT be used, (inbound, antivirus, oversized, Antispam, SURBL, RBL, etc…).



Antispam Auto-Learn - Ham

Training sources for Ham
☐ Inbound mail
☑ Outbound mail
☐ Antivirus
☐ Oversized message
☐ Antispam heuristics
☐ SURBL
☐ RBL
☐ Fingerprinting
☐ Message subject+body filter
☐ Message body filter
☐ Message subject filter
☐ Raw message filter
☐ Message header filter
☐ Attachment name
☐ Source address
☐ Destination address
☐ IP address

WaterMark quick-feeder

Learn by example

Conversation tracking

☑ Enable conversation tracking service
☑ Automatic whitelisting for tracked conversations
☑ Automatic training from tracked conversations

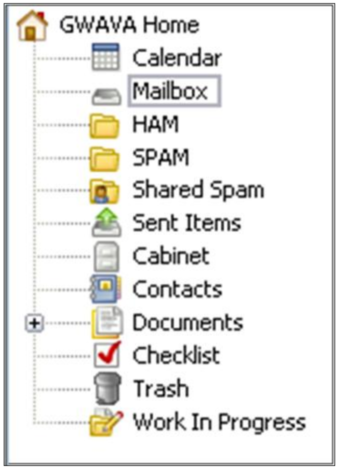
## Conversation Tracking

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.

**Ham and Spam fine tuning**

*The signature spam engine does not need fine tuning; this step only applies to the probability spam engine.* Until the probability engine is fine tuned for any specific system, there may be some false positives and negatives which make it through or are blocked by the mail system. *The Probability engine will create rules based entirely on the type of mail it is fed to create a rule set from. Feeding the system incorrect mail types will result in an faulty rule set for the filter which will produce false positives and allow spam through the system.*

To fine tune the probability engine, GWAVA 4.5 can be fed the spam that slips past the filter, as well as the ham that is caught in the quarantine, to adjust the filter rules. GWAVA 4.5 is fed this mail through 'feeder' folders created in a GroupWise account. The folders are specified in the GWAVA system, one for 'Ham' and one for 'Spam'. A module of GWAVA 4.5 connects, via IMAP, to the specified account and pulls the messages found in the 'ham' and 'spam' folders, and appropriately creates rules to the filter based on those messages.



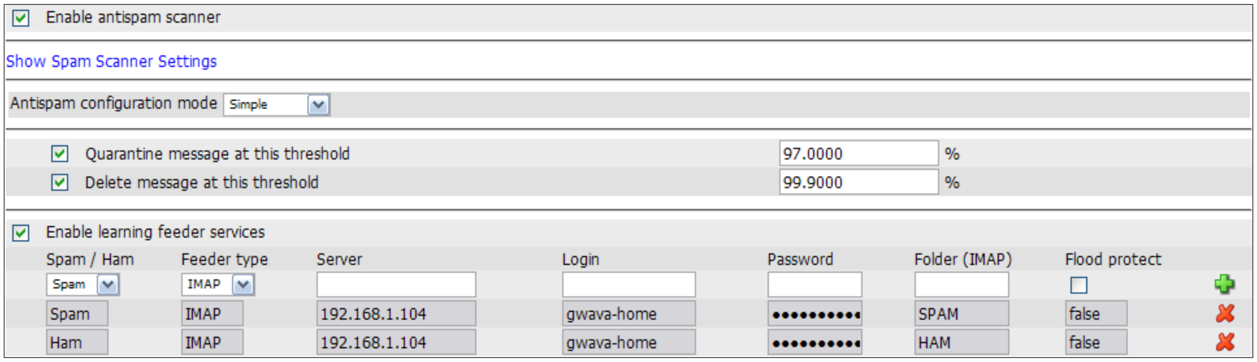
The GroupWise account does not need to be an admin account, but it is recommended that a new account be created in order for ease of management. This new account, (it can be named anything, ie. 'GWAVA Home'), should have at least three folders created at the root of the account: Shared spam, Spam, and Ham. (A shared ham folder can also be created, if desired, to increase the amount of ham collected.) The shared folders are for collecting and verifying the mail type, the spam and ham folders are the IMAP feeder folders for GWAVA.

If spam gets through the filter, the users should be instructed to move their unwanted mail into the shared spam folder, so it can be verified as spam, and placed in the spam feeder folder. *Not everything placed in the shared spam folder will be spam, depending on what users deem as 'unwanted mail'.*

False positives, ham, will be stored in the GWAVA Quarantine system. This mail will need to be released back into the system. By default, users can release messages flagged as spam and blocked from their mailbox, and can be alerted of this mail. To harvest ham for fine tuning, the Quarantine system can be set to send a blind carbon copy, (BCC), when a message is released from the quarantine. Set the BCC on release address to your feeder folder account, and each time a message is released from the Quarantine, a copy will be sent to the feeder account. *Not all messages released by users will be 'ham' or desired for a general rule set for the GWAVA filter system. Some users may release everything to their mailbox regardless of whether it is spam or not.* Fine tuning the system requires the administrator to manually sort through the released mail and only move the desired ham into the 'ham' feeder folder.

Once mail is placed in either the Ham or Spam feeder folders, GWAVA should remove them from these folders within a few minutes. These messages are consumed by GWAVA and are removed from the system. Messages that need to be available later on should not be dropped into the Ham folder, as they will be removed from the GroupWise system.

Before GWAVA can utilize the feeder folders, GWAVA must be made aware of them. The learning feeder folders option is found under **Server/Scanner Management | <server name> | Manage Scanners | <scanner name> | Scanning Configuration | Antispam | Heuristics**. To change the scanner, click 'Show Spam Scanner Settings' and select the Probability engine from the drop down menu and 'Save Changes'. When the Probability engine is selected under the **Heuristics** page, the learning feeder services option will become available.



☑ Enable antispam scanner

Show Spam Scanner Settings

Antispam configuration mode Simple

☑ Quarantine message at this threshold 97.0000 %

☑ Delete message at this threshold 99.9000 %

☑ Enable learning feeder services

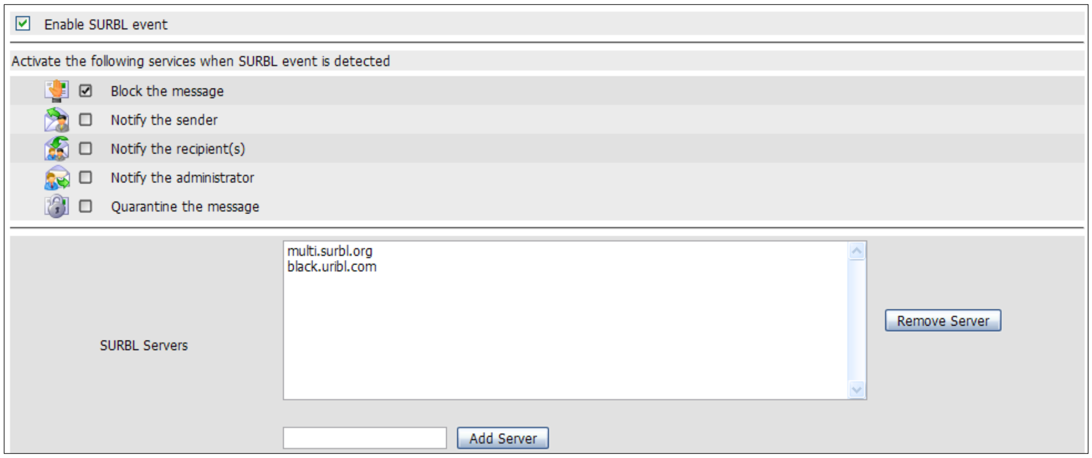
| Spam / Ham | Feeder type | Server | Login | Password | Folder (IMAP) | Flood protect | |
|---|---|---|---|---|---|---|---|
| Spam | IMAP | | | | | □ | ✚ |
| Spam | IMAP | 192.168.1.104 | gwava-home | •••••••••• | SPAM | false | ✖ |
| Ham | IMAP | 192.168.1.104 | gwava-home | •••••••••• | HAM | false | ✖ |

Enable the learning feeder services, and fill out the appropriate information. The IMAP address should match the address and port of the IMAP interface of the Post Office containing the specified user. The IP address and port are specified in the following syntax: <ip_address:port>. If no port is specified, the default port, 143, is assumed. If the Post Office IMAP is listening on a port other than 143, it must be specified. The Login name only requires the name, not the whole address. The IMAP folder must be specified and should match the Spam / Ham folder choice at the beginning. DO NOT assign your spam folder for ham feeding, or your ham folder for spam feeding as this would reverse the training and rule set. Flood protect should not be enabled unless instructed by support.

After the feeders have been setup, make sure to save the changes. Once the changes have been saved, the feeders will become active in a few minutes.

## 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.)



☑ Enable SURBL event

Activate the following services when SURBL event is detected

☑ Block the message
☐ Notify the sender
☐ Notify the recipient(s)
☐ Notify the administrator
☐ Quarantine the message

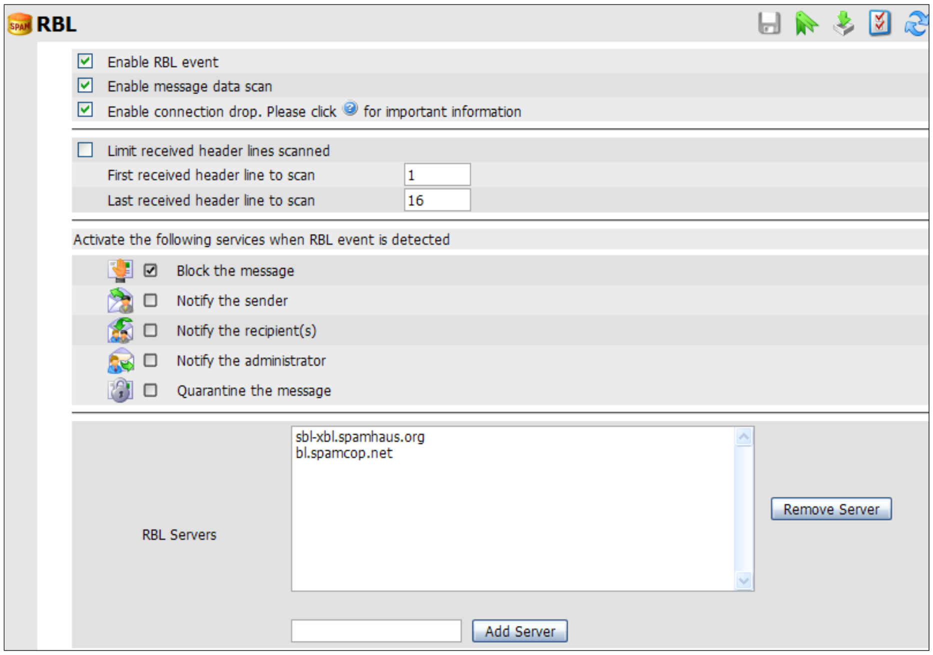
SURBL Servers

multi.surbl.org
black.uribl.com

## 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.)



☑ Enable RBL event
☑ Enable message data scan
☑ Enable connection drop. Please click for important information

☐ Limit received header lines scanned
First received header line to scan: 1
Last received header line to scan: 16

Activate the following services when RBL event is detected

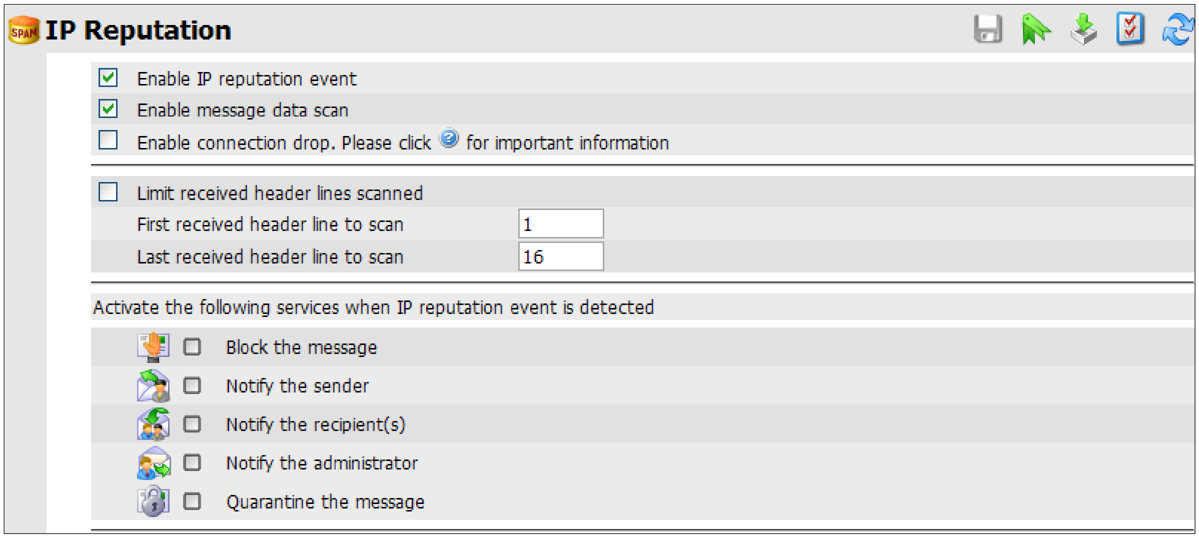
☑ Block the message
☐ Notify the sender
☐ Notify the recipient(s)
☐ Notify the administrator
☐ Quarantine the message

RBL Servers

sbl-xbl.spamhaus.org
bl.spamcop.net

## IP Reputation

IP Reputation works much like the RBL scanner does, in that it uses a black list, but also has a white list for common mail sources. But when used on a SMTP scanner 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.)



IP Reputation

☑ Enable IP reputation event

☑ Enable message data scan

☐ Enable connection drop. Please click ? for important information

☐ Limit received header lines scanned

First received header line to scan: 1

Last received header line to scan: 16

Activate the following services when IP reputation event is detected

☐ Block the message

☐ Notify the sender

☐ Notify the recipient(s)

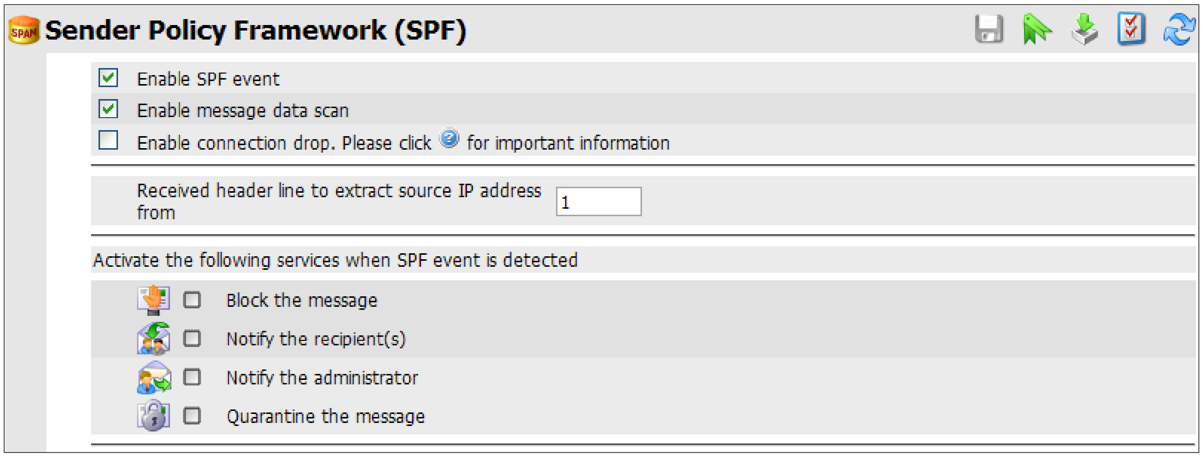
☐ Notify the administrator

☐ Quarantine the message

## SPF

Sender Policy Framework can be used with the GWIA and SMTP scanners. 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 scanner, 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.



Sender Policy Framework (SPF)

☑ Enable SPF event

☑ Enable message data scan

☐ Enable connection drop. Please click for important information

Received header line to extract source IP address from: 1

Activate the following services when SPF event is detected

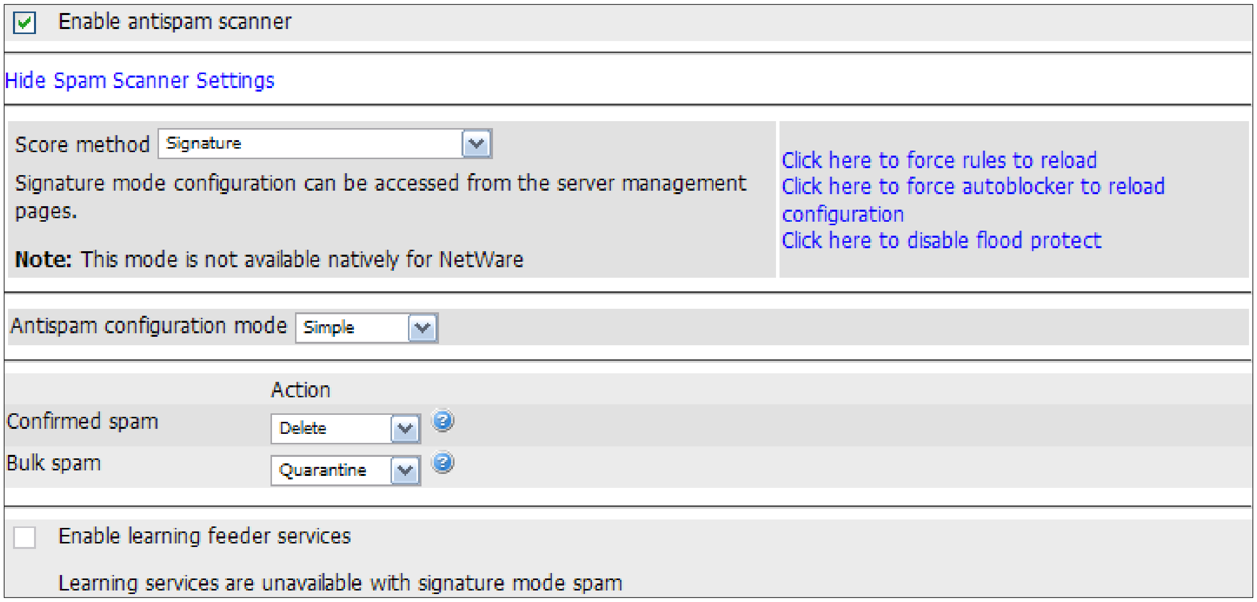
☐ Block the message

☐ Notify the recipient(s)

☐ Notify the administrator

☐ Quarantine the message

SPF can be configured to perform connection blocks in conjunction with the SMTP scanner, 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.



☑ Enable antispam scanner

Hide Spam Scanner Settings

Score method: Signature

Signature mode configuration can be accessed from the server management pages.

**Note:** This mode is not available natively for NetWare

Click here to force rules to reload
Click here to force autoblocker to reload configuration
Click here to disable flood protect

Antispam configuration mode: Simple

| | Action |
|---|---|
| Confirmed spam | Delete |
| Bulk spam | Quarantine |

☐ Enable learning feeder services

Learning services are unavailable with signature mode spam

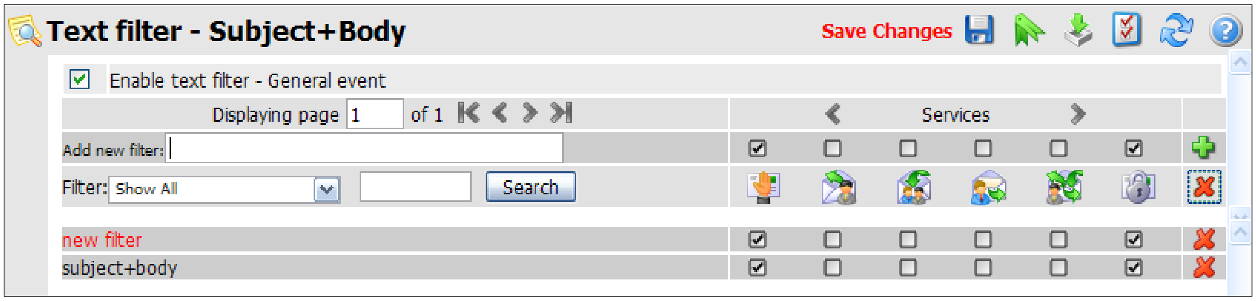
## Text filtering

### Subject + Body

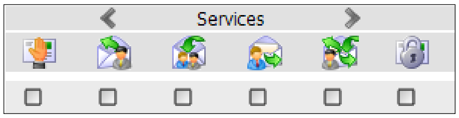
Subject + Body Text filtering searches the subject line and body of the message for a match to any filter specified. Filters must be added manually. GWAVA 4.5 recognizes all plain text filters as well as standard regular expressions, or RegEx. GWAVA does not recognize RegEx ranges, (values in between { } braces), unless the entire RegEx string is followed by  a '/q' at the end. (See the appendix for details.)

### 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.

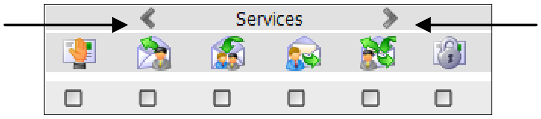


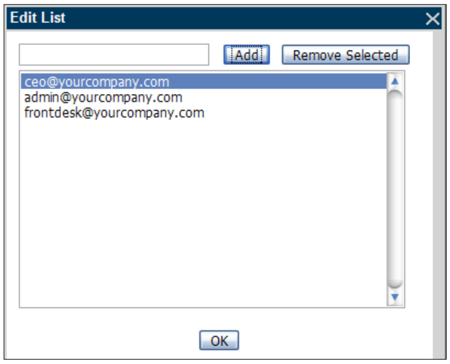
There are five, (six for some), optional actions for every scanner event or filter that fires on a message: **Block**, **Notify Sender**, **Notify Recipient(s)**, **Notify Administrator**, **Quarantine**, and, for some, **Notify Defined Addresses**.  The action icons work as a global button. Selecting the icon globally activates, or deactivates, the event for every listed option.



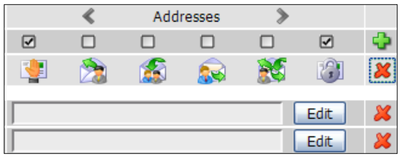
The block and the quarantine options are not the same. If you select to quarantine a message, but do not select the block action, then the message will have a copy placed in the quarantine, but still be allowed to reach the destination mailbox. Blocking a message without selecting quarantine will simply 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 under the services carousel.  To access the different options, click on either arrow to the sides of the word **Services** above the action icons until you reach 'Addresses'. Select **Edit** to open the defined address list for this action.





ceo@yourcompany.com
admin@yourcompany.com
frontdesk@yourcompany.com

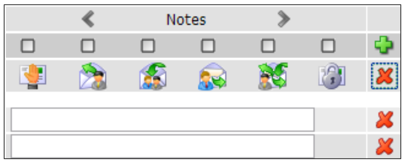


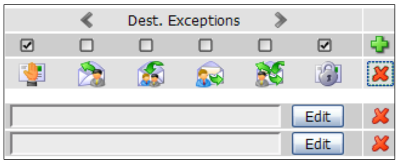
When you have defined the addresses you desire, select **OK** and enable the action.

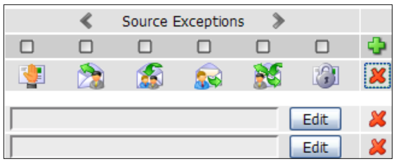
Now that addresses have been defined and the notify addresses option is active, every time this specific text filter is found in a message, the defined addresses are notified. This is only active for the text filter which the address is tied to.

In addition to the ‘addresses’ option, there are three other options available to modify and customize your text filter. The different options are self-explanatory and only apply to the text filter they are defined under. 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.

The exceptions options, both destination and source, will only apply to the filter where they are defined. Source addresses allows incoming mail to be exempted from the filter based on the source address of that mail, while the destination  exceptions allows any defined address to be exempted from the filter for all incoming mail.  These exceptions only apply to the filter which they are connected to.







The different exceptions are modified in the same manner as the ‘addresses’ field. Select the ‘edit’ button and add or remove the desired addresses.  Select ‘ok’ and make sure to save the changes before browsing away from the page to commit them to the system.

## MIME filtering

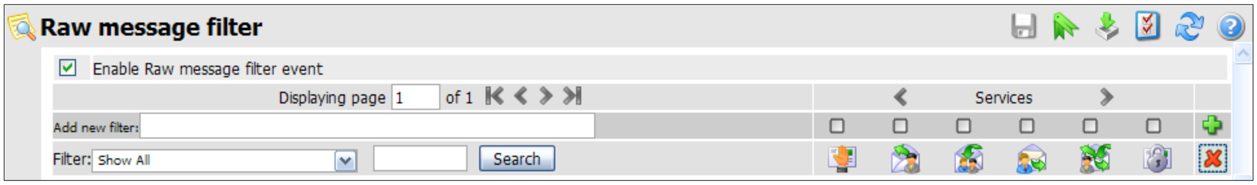
Every message passing through the mail system comes through as a MIME file. MIME filtering scans the message in its basic raw form, the MIME file, for patterns matching any filter specified by the Administrator. GWAVA 4.5 does not come with any raw message filters pre-configured. The MIME filters work 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>'.

I.e.

'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.

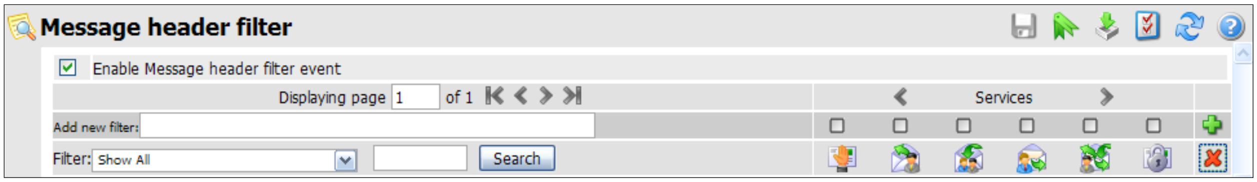


**Raw message filter**

☑ Enable Raw message filter event

### 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.

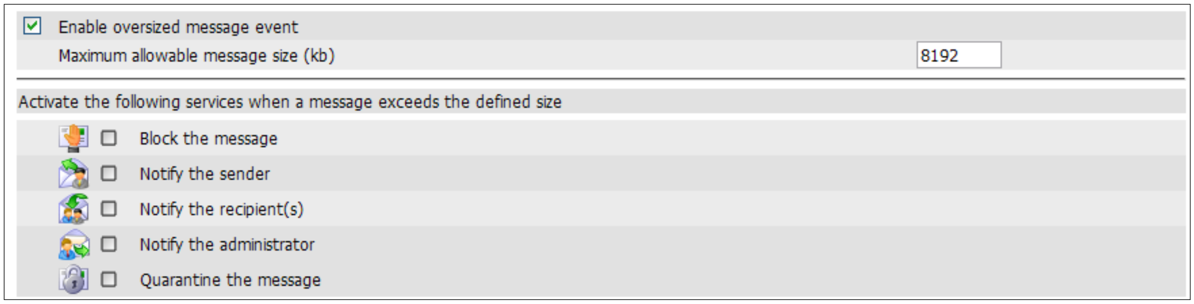


**Message header filter**

☑ Enable Message header filter event

### Oversize

The Oversize message event scanner 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.



☑ Enable oversized message event

Maximum allowable message size (kb) 8192

Activate the following services when a message exceeds the defined size

□ Block the message

□ Notify the sender

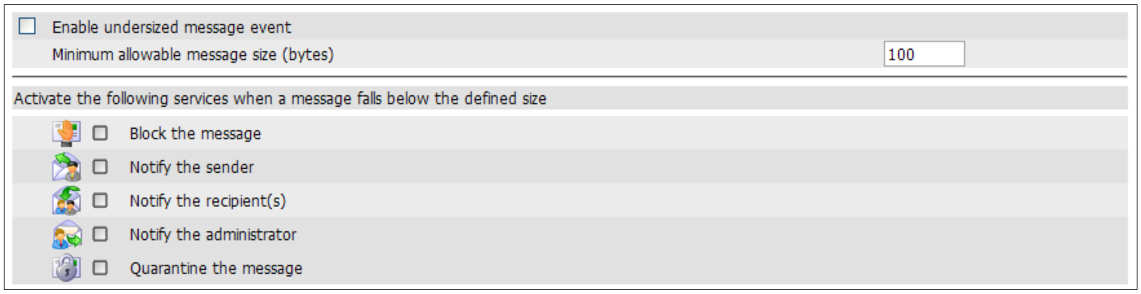
□ Notify the recipient(s)

□ Notify the administrator

□ Quarantine the message

## 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 scanner is not enabled by default, and must be enabled before it becomes active.



☐ Enable undersized message event

Minimum allowable message size (bytes) 100

Activate the following services when a message falls below the defined size

☐ Block the message

☐ Notify the sender

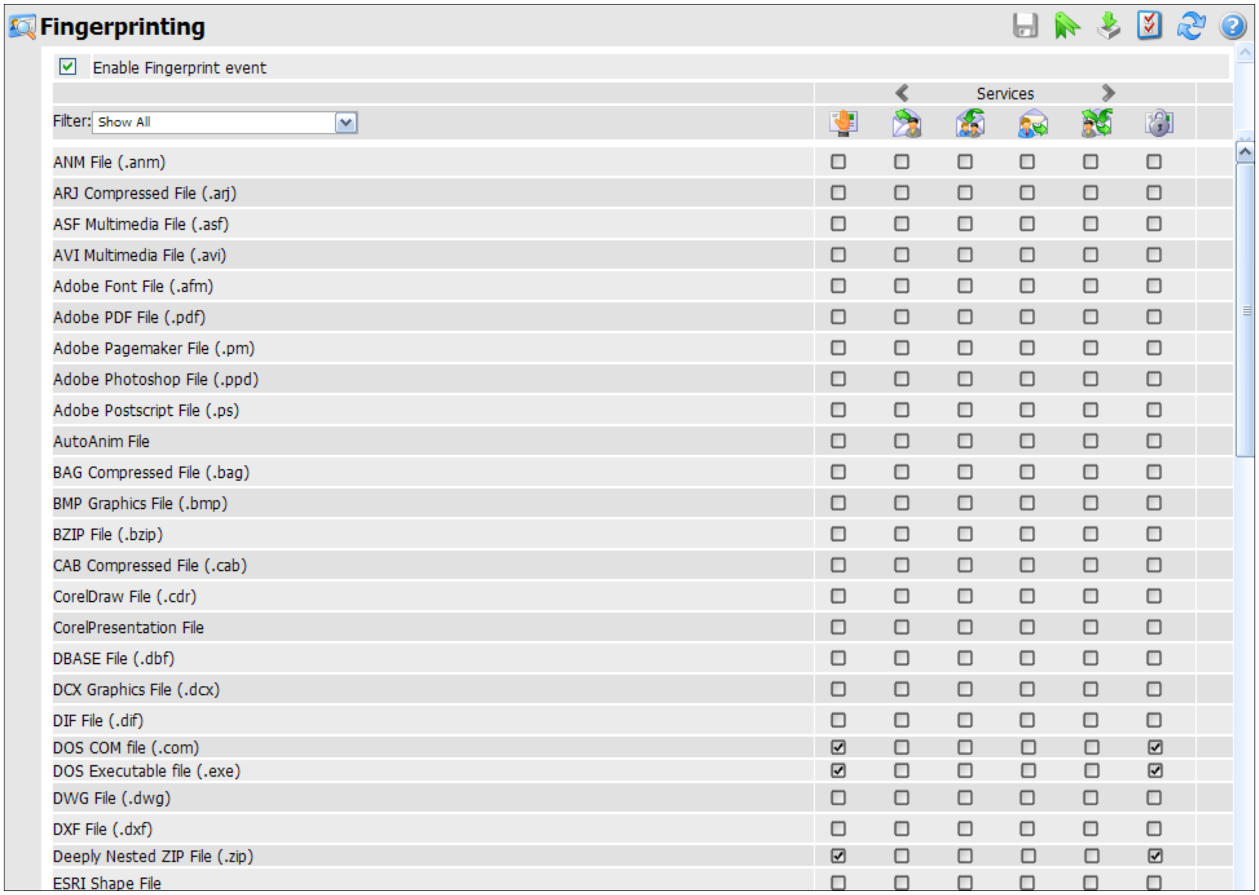
☐ Notify the recipient(s)

☐ Notify the administrator

☐ Quarantine the message

## Fingerprinting

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



**Fingerprinting**

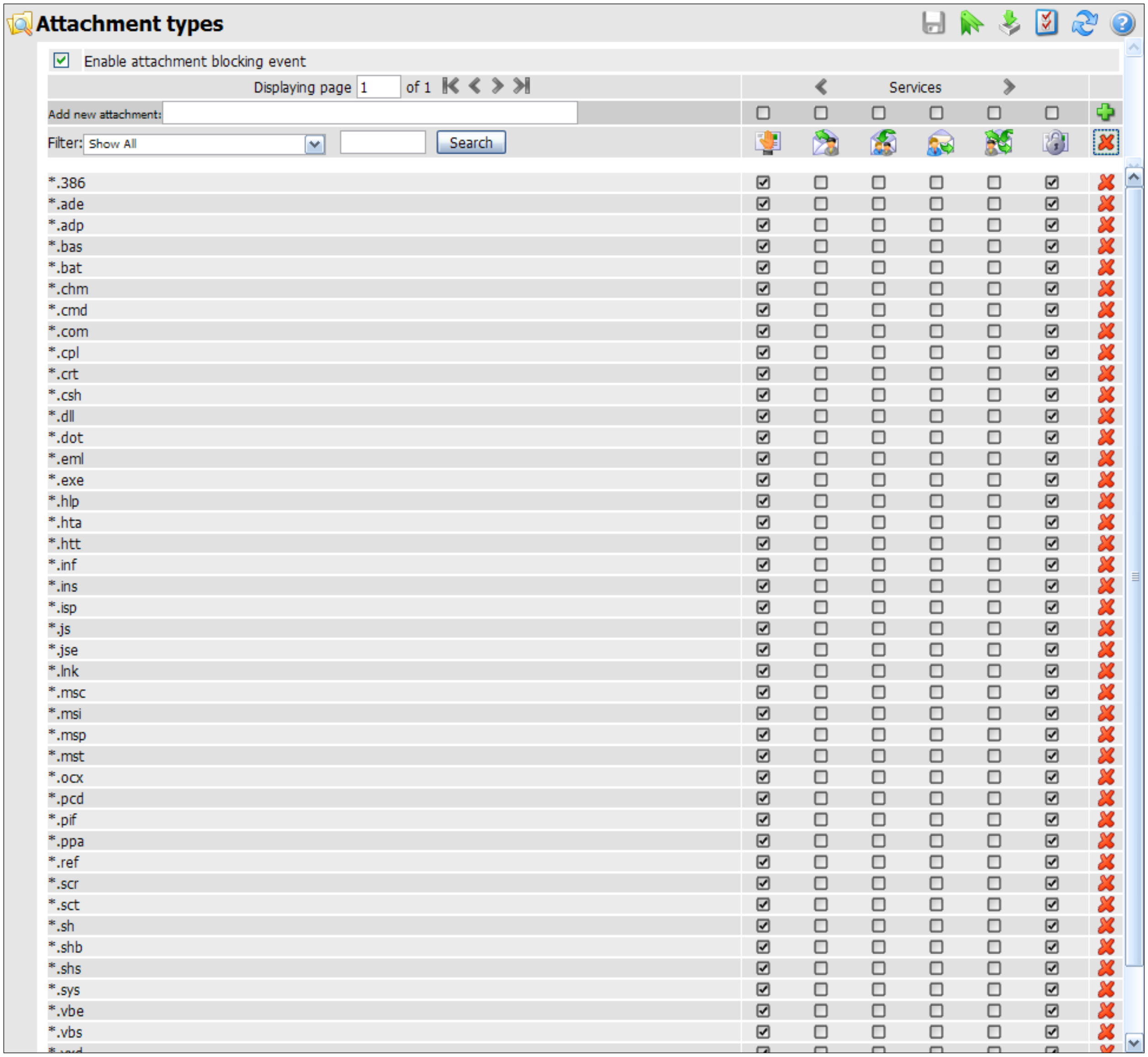
☑ Enable Fingerprint event

Filter: Show All

| | Services | | | | | |
|---|---|---|---|---|---|---|
| ANM File (.anm) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ARJ Compressed File (.arj) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| ASF Multimedia File (.asf) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| AVI Multimedia File (.avi) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adobe Font File (.afm) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adobe PDF File (.pdf) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adobe Pagemaker File (.pm) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adobe Photoshop File (.ppd) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Adobe Postscript File (.ps) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| AutoAnim File | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| BAG Compressed File (.bag) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| BMP Graphics File (.bmp) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| BZIP File (.bzip) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| CAB Compressed File (.cab) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| CorelDraw File (.cdr) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| CorelPresentation File | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DBASE File (.dbf) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DCX Graphics File (.dcx) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DIF File (.dif) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DOS COM file (.com) | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ |
| DOS Executable file (.exe) | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ |
| DWG File (.dwg) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| DXF File (.dxf) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Deeply Nested ZIP File (.zip) | ☑ | ☐ | ☐ | ☐ | ☐ | ☑ |
| ESRI Shape File | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

## Attachment types

The Attachment types event scanner 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 scanner 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.



### Attachment types

☑ Enable attachment blocking event

Displaying page 1 of 1

Add new attachment:

Filter: Show All

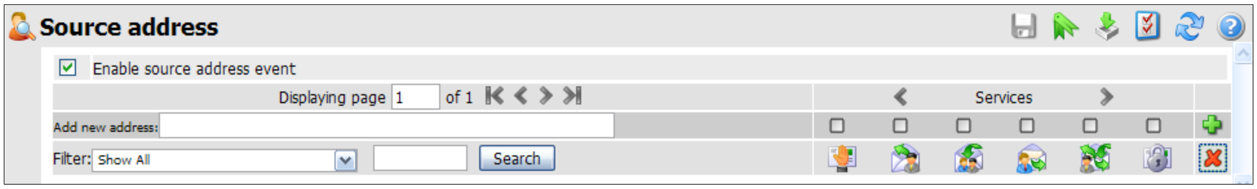
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Add new attachment: | □ | □ | □ | □ | □ | □ | ✚ |
| *.386 | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.ade | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.adp | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.bas | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.bat | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.chm | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.cmd | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.com | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.cpl | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.crt | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.csh | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.dll | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.dot | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.eml | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.exe | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.hlp | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.hta | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.htt | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.inf | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.ins | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.isp | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.js | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.jse | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.lnk | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.msc | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.msi | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.msp | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.mst | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.ocx | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.pcd | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.pif | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.ppa | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.ref | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.scr | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.sct | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.sh | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.shb | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.shs | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.sys | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.vbe | ☑ | □ | □ | □ | □ | ☑ | ✗ |
| *.vbs | ☑ | □ | □ | □ | □ | ☑ | ✗ |

## 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.

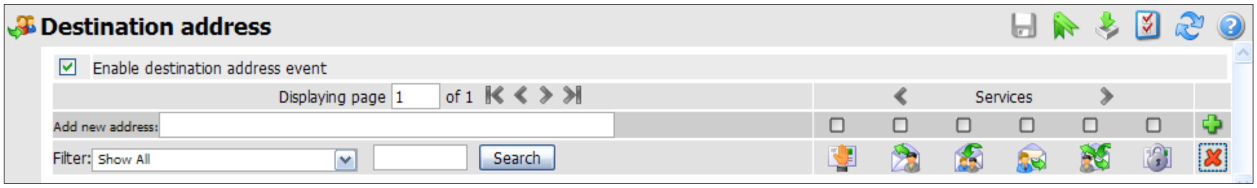


☑ Enable source address event

## 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 scanner, (except for the SPF and IP reputation scans if they are configured for connection drop).

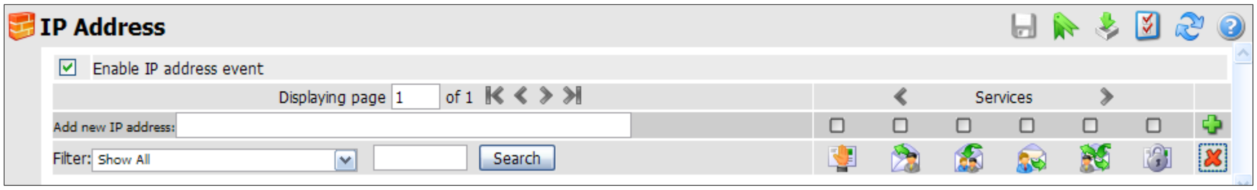


☑ Enable destination address event

## IP Address

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 addressed desired.

I.e.   192.168.56.21



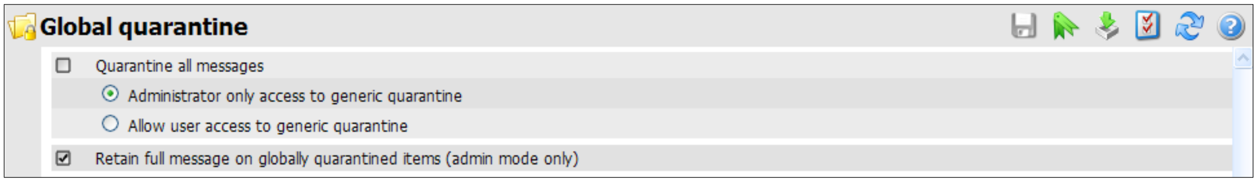
☑ Enable IP address event

## Message services

GWAVA 4.5 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.



Global quarantine

□ Quarantine all messages

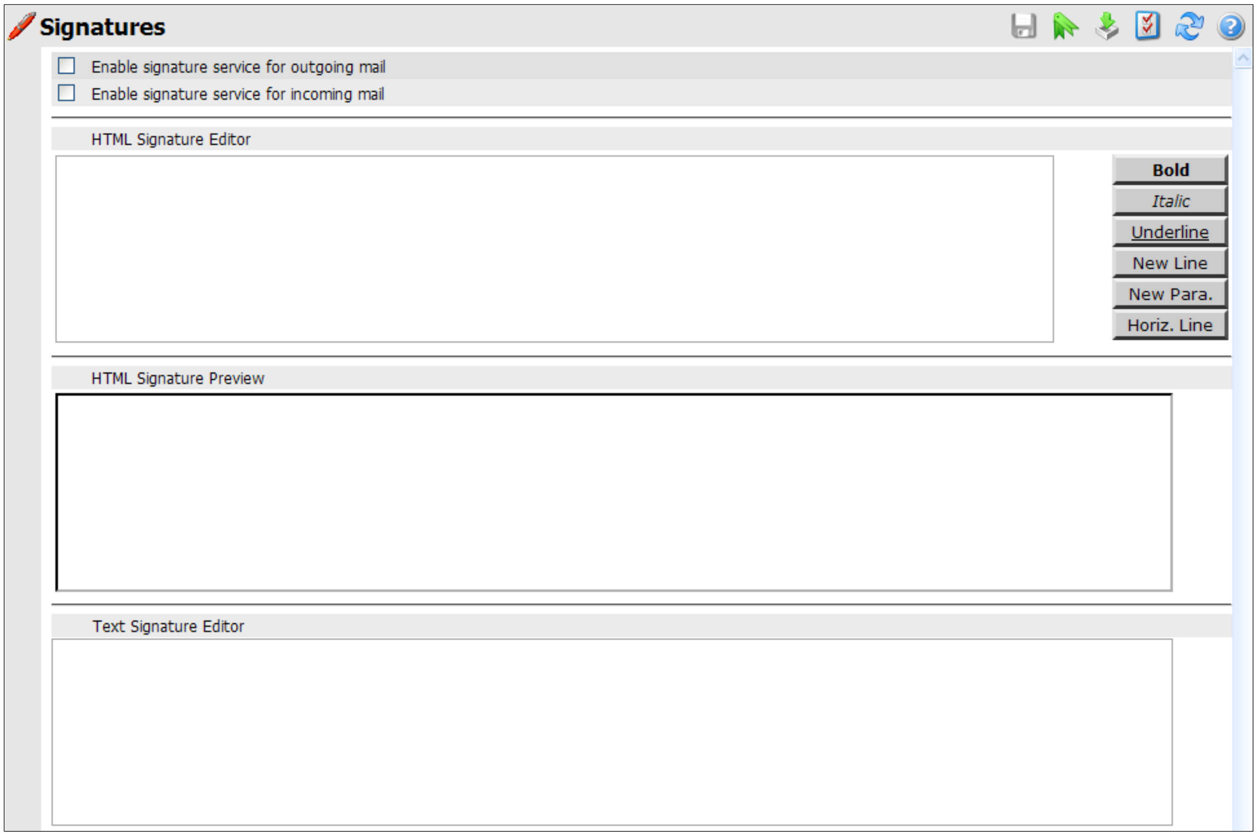
● Administrator only access to generic quarantine

○ Allow user access to generic quarantine

☑ Retain full message on globally quarantined items (admin mode only)

### Signatures

The Signatures service instructs GWAVA to add any specified signature to the selected directional mail. Signatures WILL NOT WORK with POA scanners. 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.



Signatures

□ Enable signature service for outgoing mail

□ Enable signature service for incoming mail

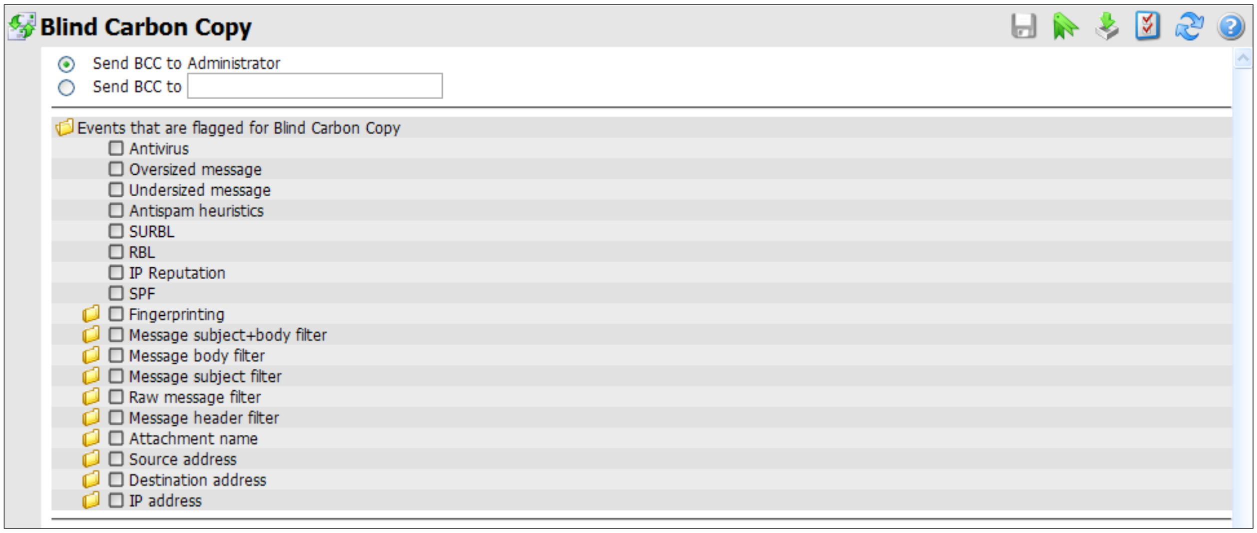
HTML Signature Editor

HTML Signature Preview

Text Signature Editor

### *Blind Carbon Copy*

The Blind Carbon Copy event instructs GWAVA 4.5 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 scanner | address under this list and specify the BCC address. After saving changes, the BCC will become active in a few moments.



Blind Carbon Copy

● Send BCC to Administrator
○ Send BCC to

Events that are flagged for Blind Carbon Copy
- □ Antivirus
- □ Oversized message
- □ Undersized message
- □ Antispam heuristics
- □ SURBL
- □ RBL
- □ IP Reputation
- □ SPF
- □ Fingerprinting
- □ Message subject+body filter
- □ Message body filter
- □ Message subject filter
- □ Raw message filter
- □ Message header filter
- □ Attachment name
- □ Source address
- □ Destination address
- □ IP address

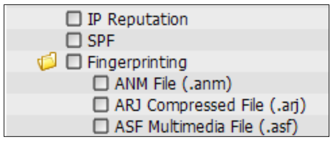
## Exceptions

GWAVA 4.5 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, etc… the offending engine should be adjusted. Adjust the scanner settings if exceptions are created regularly; the exception list should be used sparingly, when no other option applies.

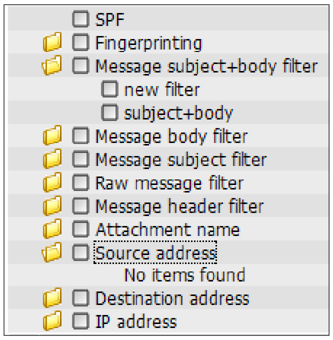
GWAVA 4.5 provides the option to create exceptions to the event scanners, to allow specific messages or addresses to pass filters that would otherwise have blocked them. An exception in GWAVA 4.5 consists of two main parts: the identifying item and the event scanner(s) it is exempted from. Until you 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 scanner. For example,



- □ IP Reputation
- □ SPF
- □ Fingerprinting
  - □ ANM File (.anm)
  - □ ARJ Compressed File (.arj)
  - □ ASF Multimedia File (.asf)



- □ SPF
- □ Fingerprinting
- □ Message subject+body filter
  - □ new filter
  - □ subject+body
- □ Message body filter
- □ Message subject filter
- □ Raw message filter
- □ Message header filter
- □ Attachment name
- □ Source address
  - No items found
- □ Destination address
- □ IP address

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 scanner 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.

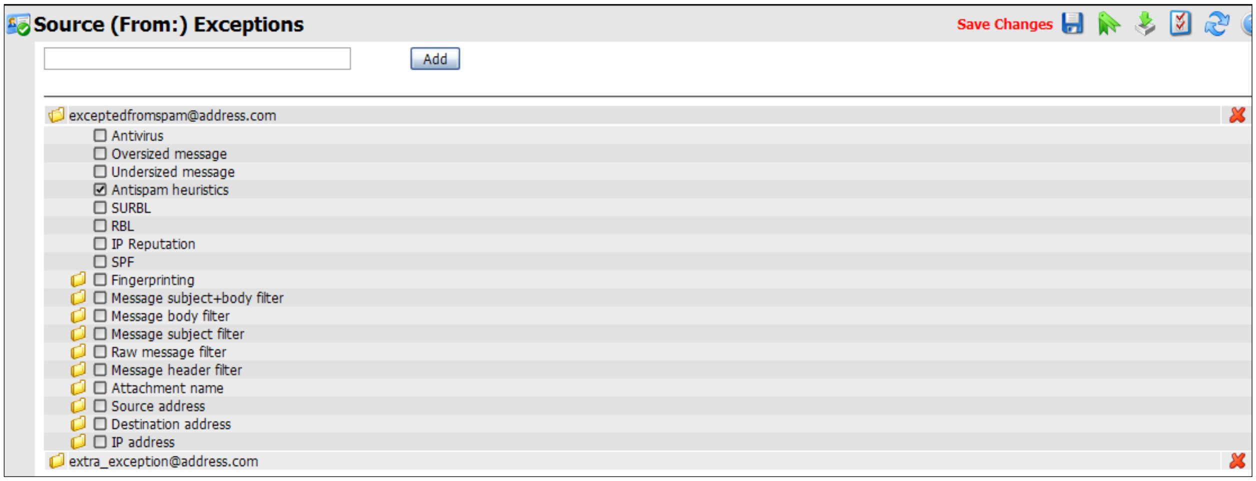
## Source address (From:)

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.  (i.e.  *@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 scanners.

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



Source (From:) Exceptions

exceptedfromspam@address.com
- □ Antivirus
- □ Oversized message
- □ Undersized message
- ☑ Antispam heuristics
- □ SURBL
- □ RBL
- □ IP Reputation
- □ SPF
- □ Fingerprinting
- □ Message subject+body filter
- □ Message body filter
- □ Message subject filter
- □ Raw message filter
- □ Message header filter
- □ Attachment name
- □ Source address
- □ Destination address
- □ IP address

extra_exception@address.com

## 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 GWAVA4.5.  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.  (i.e.  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

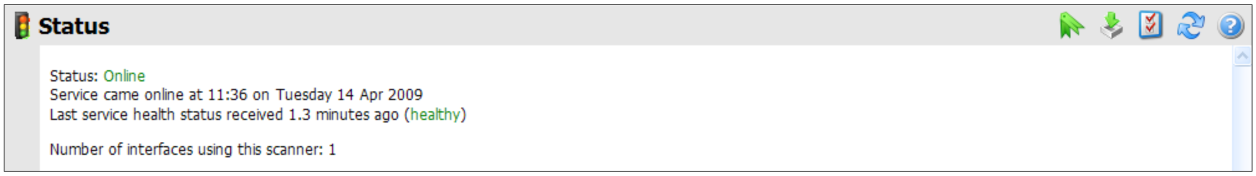
The IP Address exception searches for a specified IP address anywhere in the message header. IP addresses specified in this exception list are considered 'trusted', and no messages from these IP addresses will be blocked.

## Scanner information

The general status and statistics of any specific scanner is listed here.

### Status

The status page shows the health of the scanner, when it came online, and the last time it gave a health status. If the "(healthy)" does not appear within the first few minutes of scanner operation, or is not present later when checked, then the scanner may not be working correctly, and the logs should be checked.



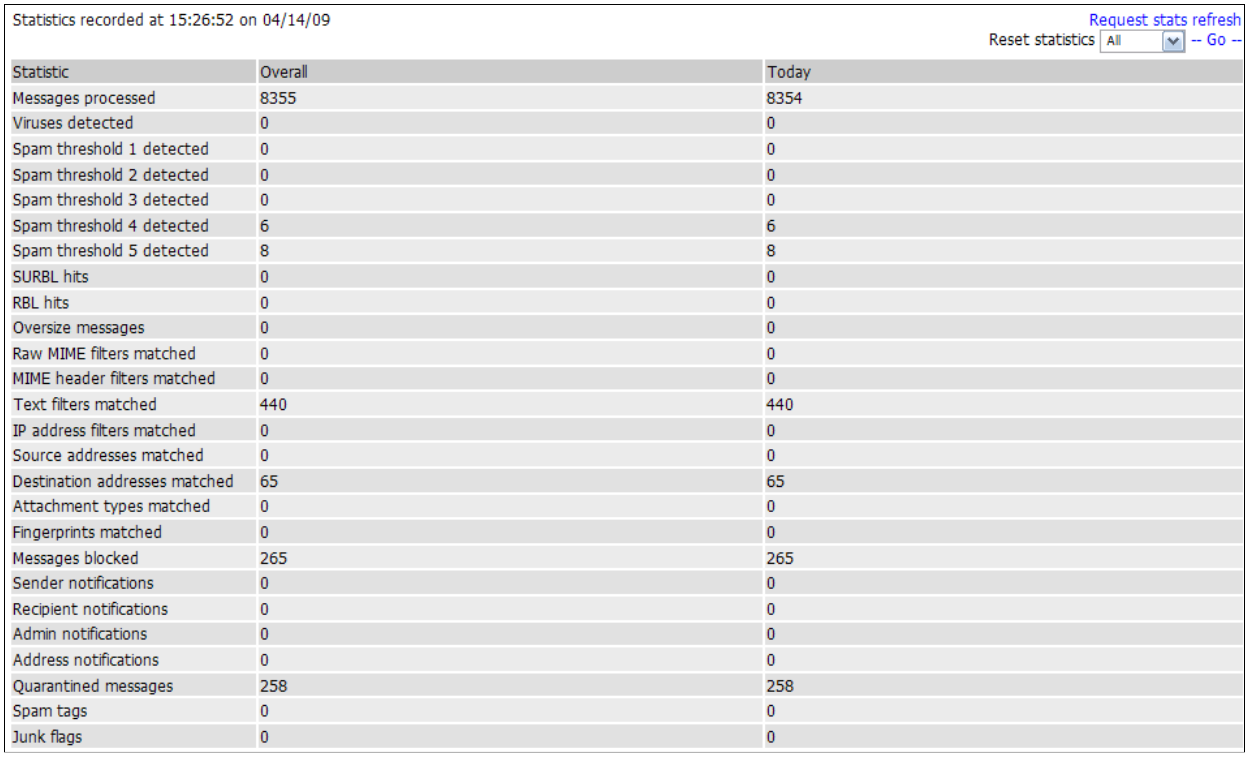
Status: Online
Service came online at 11:36 on Tuesday 14 Apr 2009
Last service health status received 1.3 minutes ago (healthy)

Number of interfaces using this scanner: 1

## Statistics

The statistics page shows each hit on every event in the scanner, by category. There are totals for each category and complete, for the current day, as well as the life of the scanner. The statistics are refreshed regularly and the refresh date is marked at the top left of the page. To request an immediate refresh, select the “Request stats refresh” hypertext at the top right of the page. Resetting the statistics, individually or all together, wipes the statistics back to zero and restarts the count.

If the virus statistics are not accurate and a third-party virus integration other than Kaspersky is being used, the spool directory may not be excluded from scanning, or the GWAVA 4.5 directory tree may be subject to scans incorrectly, double check your settings and restart GWAVA 4.5 to attempt to resolve the problem. The statistics require messages to be managed in the correct area if they are to be counted accurately. See the antivirus agent section, (pg. 33), for details.



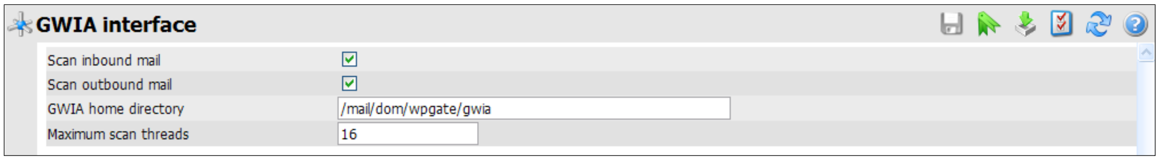
Statistics recorded at 15:26:52 on 04/14/09

| Statistic | Overall | Today |
|---|---|---|
| Messages processed | 8355 | 8354 |
| Viruses detected | 0 | 0 |
| Spam threshold 1 detected | 0 | 0 |
| Spam threshold 2 detected | 0 | 0 |
| Spam threshold 3 detected | 0 | 0 |
| Spam threshold 4 detected | 6 | 6 |
| Spam threshold 5 detected | 8 | 8 |
| SURBL hits | 0 | 0 |
| RBL hits | 0 | 0 |
| Oversize messages | 0 | 0 |
| Raw MIME filters matched | 0 | 0 |
| MIME header filters matched | 0 | 0 |
| Text filters matched | 440 | 440 |
| IP address filters matched | 0 | 0 |
| Source addresses matched | 0 | 0 |
| Destination addresses matched | 65 | 65 |
| Attachment types matched | 0 | 0 |
| Fingerprints matched | 0 | 0 |
| Messages blocked | 265 | 265 |
| Sender notifications | 0 | 0 |
| Recipient notifications | 0 | 0 |
| Admin notifications | 0 | 0 |
| Address notifications | 0 | 0 |
| Quarantined messages | 258 | 258 |
| Spam tags | 0 | 0 |
| Junk flags | 0 | 0 |

# Configure (scanner interface) settings

## Mail interface settings

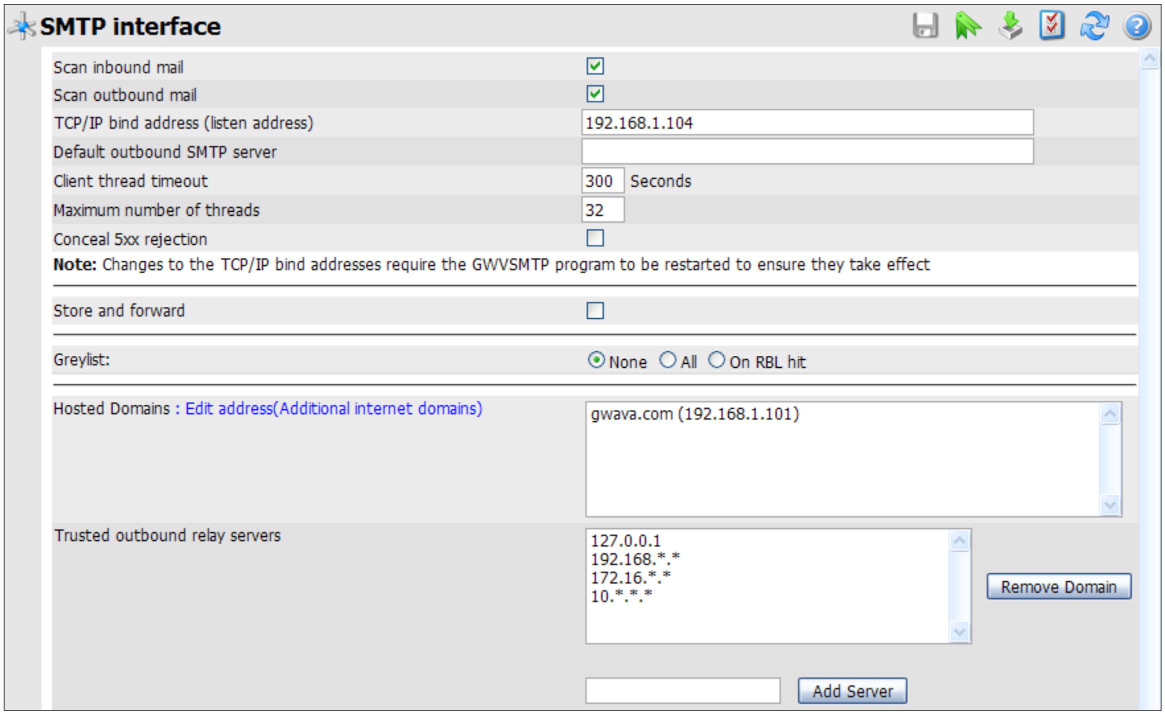
This menu item lists the basic connection and interface settings for the different scanners specified during each scanner's creation setup wizard. Each scanner type will have a different interface setting page. (See the appropriate setup wizard section for each scanner type to find information on each different scanner's settings.) A GWIA scanner'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.



GWIA interface

| | |
|---|---|
| Scan inbound mail | ☑ |
| Scan outbound mail | ☑ |
| GWIA home directory | /mail/dom/wpgate/gwia |
| Maximum scan threads | 16 |

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



SMTP interface

| | |
|---|---|
| Scan inbound mail | ☑ |
| Scan outbound mail | ☑ |
| TCP/IP bind address (listen address) | 192.168.1.104 |
| Default outbound SMTP server | |
| Client thread timeout | 300 Seconds |
| Maximum number of threads | 32 |
| Conceal 5xx rejection | □ |

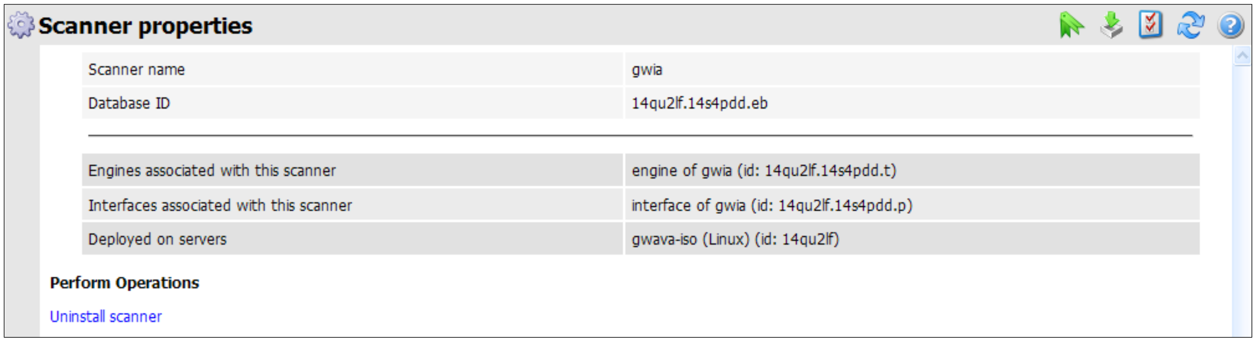
**Note:** Changes to the TCP/IP bind addresses require the GWVSMTP program to be restarted to ensure they take effect

| | |
|---|---|
| Store and forward | □ |
| Greylist: | ● None ○ All ○ On RBL hit |
| Hosted Domains : Edit address(Additional internet domains) | gwava.com (192.168.1.101) |
| Trusted outbound relay servers | 127.0.0.1<br>192.168.*.*<br>172.16.*.*<br>10.*.*.* |

# Manage Scanner object

## Scanner properties

The only option under this menu is to uninstall a specific scanner. Uninstalling a scanner presents the option to remove all scanner objects and reverse changes made in any GroupWise configuration file which GWAVA 4.5 may have altered during scanner installation.



**Scanner properties**

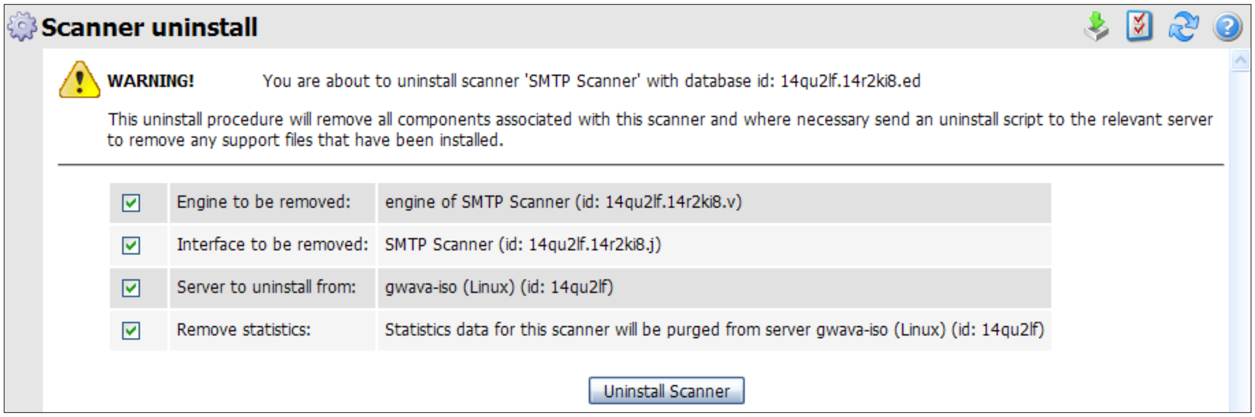
| | |
|---|---|
| Scanner name | gwia |
| Database ID | 14qu2lf.14s4pdd.eb |

| | |
|---|---|
| Engines associated with this scanner | engine of gwia (id: 14qu2lf.14s4pdd.t) |
| Interfaces associated with this scanner | interface of gwia (id: 14qu2lf.14s4pdd.p) |
| Deployed on servers | gwava-iso (Linux) (id: 14qu2lf) |

**Perform Operations**

Uninstall scanner

When you select the uninstall option you are offered appropriate options related to each scanner. They are fairly standard for all scanner types. Be aware, there is no restore option for uninstalled scanners. Once uninstalled, all selected options will be removed and no longer exist on the GWAVA 4.5 server.



**Scanner uninstall**

**WARNING!** You are about to uninstall scanner 'SMTP Scanner' with database id: 14qu2lf.14r2ki8.ed

This uninstall procedure will remove all components associated with this scanner and where necessary send an uninstall script to the relevant server to remove any support files that have been installed.

| | | |
|---|---|---|
| ☑ | Engine to be removed: | engine of SMTP Scanner (id: 14qu2lf.14r2ki8.v) |
| ☑ | Interface to be removed: | SMTP Scanner (id: 14qu2lf.14r2ki8.j) |
| ☑ | Server to uninstall from: | gwava-iso (Linux) (id: 14qu2lf) |
| ☑ | Remove statistics: | Statistics data for this scanner will be purged from server gwava-iso (Linux) (id: 14qu2lf) |

## GWAVA Quarantine system

The GWAVA 4.5 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 4.5 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 4.5 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.

i.e.
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,

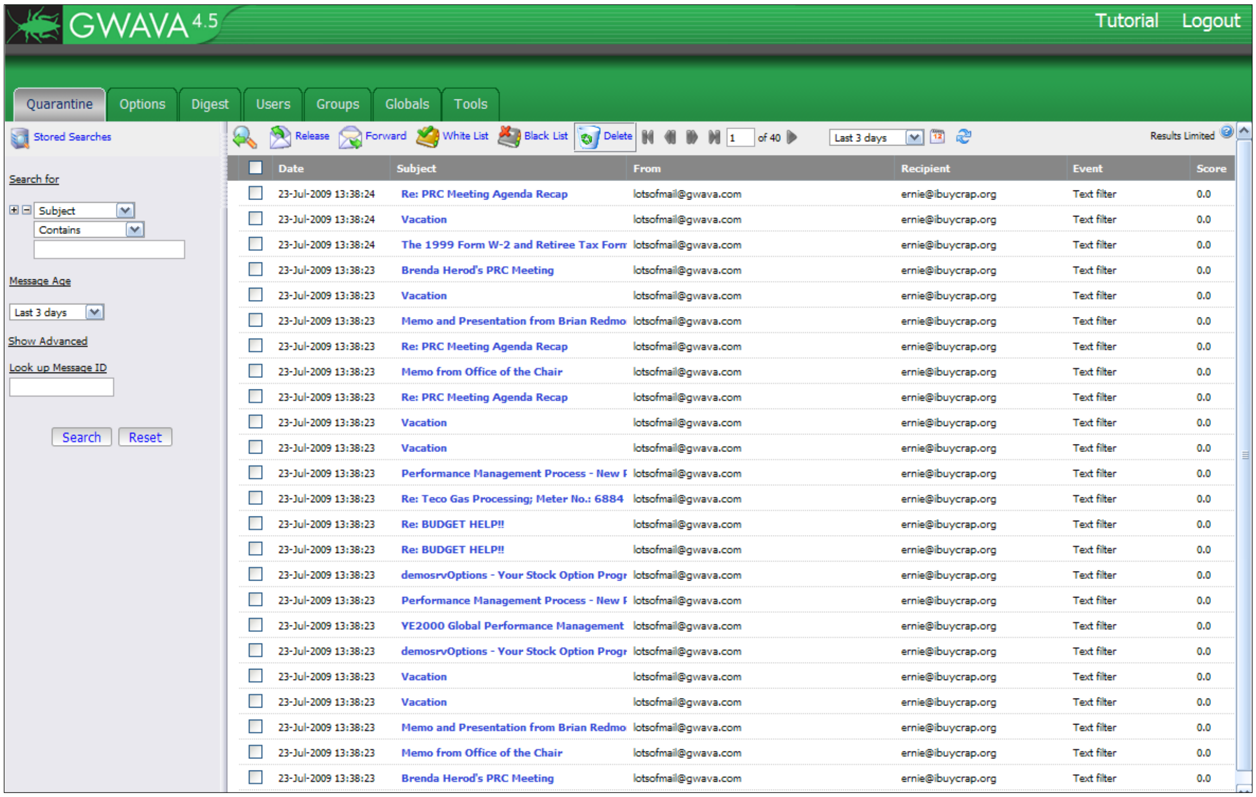
The user's options tab offers specific login, timeout, and display settings for their specific account.

## Administrator interface

The administrator user created during the initial GWAVA 4.5 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 scanner 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.



Search for: Subject, Contains

Message Age: Last 3 days

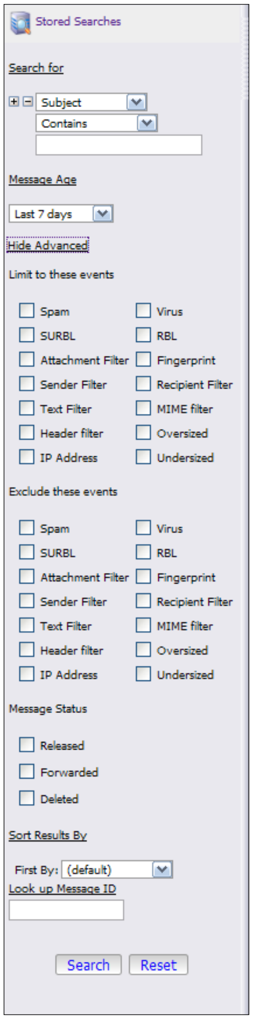
Page 1 of 40, Last 3 days

| □ | Date | Subject | From | Recipient | Event | Score |
|---|---|---|---|---|---|---|
| □ | 23-Jul-2009 13:38:24 | Re: PRC Meeting Agenda Recap | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:24 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:24 | The 1999 Form W-2 and Retiree Tax Forn | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Brenda Herod's PRC Meeting | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Memo and Presentation from Brian Redmo | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Re: PRC Meeting Agenda Recap | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Memo from Office of the Chair | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Re: PRC Meeting Agenda Recap | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Performance Management Process - New F | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Re: Teco Gas Processing; Meter No.: 6884 | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Re: BUDGET HELP!! | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Re: BUDGET HELP!! | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | demosrvOptions - Your Stock Option Progr | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Performance Management Process - New F | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | YE2000 Global Performance Management | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | demosrvOptions - Your Stock Option Progr | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Vacation | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Memo and Presentation from Brian Redmo | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Memo from Office of the Chair | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |
| □ | 23-Jul-2009 13:38:23 | Brenda Herod's PRC Meeting | lotsofmail@gwava.com | ernie@ibuycrap.org | Text filter | 0.0 |

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.

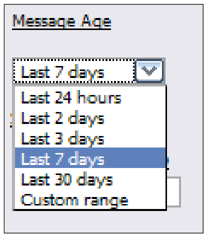

Stored Searches
Search for
⊞ ⊟ Subject
Contains
Message Age
Last 7 days
Hide Advanced
Limit to these events
□ Spam □ Virus
□ SURBL □ RBL
□ Attachment Filter □ Fingerprint
□ Sender Filter □ Recipient Filter
□ Text Filter □ MIME filter
□ Header filter □ Oversized
□ IP Address □ Undersized
Exclude these events
□ Spam □ Virus
□ SURBL □ RBL
□ Attachment Filter □ Fingerprint
□ Sender Filter □ Recipient Filter
□ Text Filter □ MIME filter
□ Header filter □ Oversized
□ IP Address □ Undersized
Message Status
□ Released
□ Forwarded
□ Deleted
Sort Results By
First By: (default)
Look up Message ID
Search
Reset

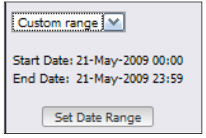
Search preferences and settings are specified on the Left side of the quarantine tab window. Expanding the **Advanced** criteria section allows the limiting to events, or exclude events from the search results. For instance, most messages in the quarantine will be caught by multiple event scanners, which 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.

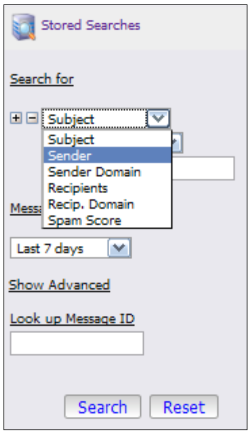


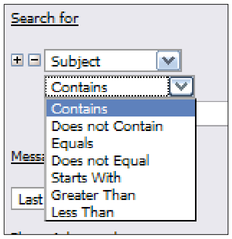


If the **Message ID** is known, (i.e. from the message digest), the message ID may be used to immediately call up the desired message.

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.

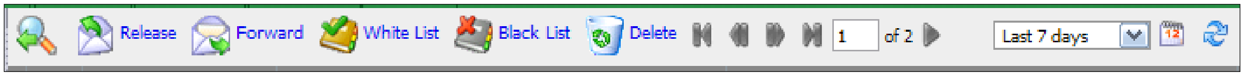
Using the **+** and **–** buttons, multiple search terms may be specified or removed from the active search.



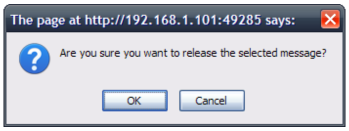


Any search may be saved by selecting the “Stored Searches” icon at the top of the search pane. The **Stored Searches** function spawns a save or load window which prompts the user to either save, delete, or load any previously saved search sessions.

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.

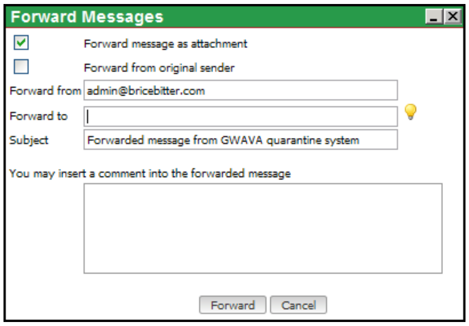


**Release –** Releasing a message from the quarantine tells GWAVA 4.5 to return that message back to the mail stream, where it will be delivered to the original recipient, unchanged.  Select a desired message(s) by placing a check in the associated checkbox, and then select the release button from the toolbar. Verify that you wish to release the message.



The page at http://192.168.1.101:49285 says:

Are you sure you want to release the selected message?



Forward Messages

☑ Forward message as attachment

☐ Forward from original sender

Forward from: admin@bricebitter.com

Forward to:

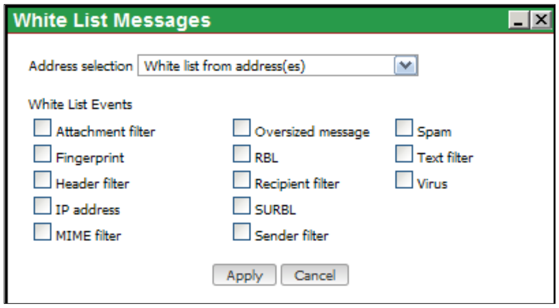
Subject: Forwarded message from GWAVA quarantine system

You may insert a comment into the forwarded 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.

**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.

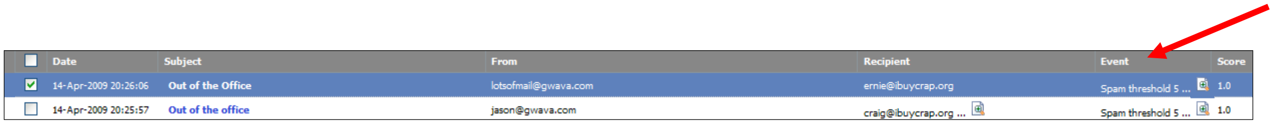


White List Messages

Address selection: White list from address(es)

White List Events

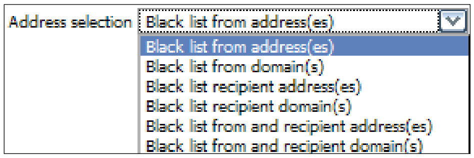
☐ Attachment filter
☐ Fingerprint
☐ Header filter
☐ IP address
☐ MIME filter
☐ Oversized message
☐ RBL
☐ Recipient filter
☐ SURBL
☐ Sender filter
☐ Spam
☐ Text filter
☐ Virus



| ☐ | Date | Subject | From | Recipient | Event | Score |
|---|---|---|---|---|---|---|
| ☑ | 14-Apr-2009 20:26:06 | Out of the Office | lotsofmail@gwava.com | ernie@ibuycrap.org | Spam threshold 5 ... | 1.0 |
| ☐ | 14-Apr-2009 20:25:57 | Out of the office | jason@gwava.com | craig@ibuycrap.org ... | Spam threshold 5 ... | 1.0 |

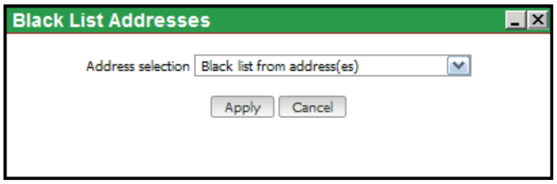
The quarantining event for each message is listed on the message row under the quarantine tab. The event column may hold more than one event per message, if there is more than one event listed, a drop-down menu will be available to display the different events for each message.

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.


Address selection: Black list from address(es)
Black list from address(es)
Black list from domain(s)
Black list recipient address(es)
Black list recipient domain(s)
Black list from and recipient address(es)
Black list from and recipient domain(s)

**Black List**

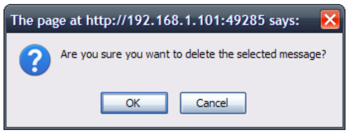
Black listing a message instructs the GWAVA 4.5 system to always block messages from the Address selection (Source address, source domain, recipient address, recipient domain, or a combination of both the source and the recipient address or domain.) Blacklisted addresses' or domains' messages are added to the quarantine.


Black List Addresses

Address selection: Black list from address(es)

**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.


The page at http://192.168.1.101:49285 says:

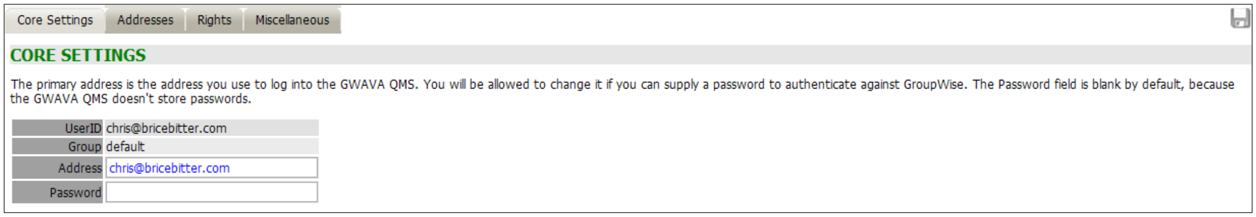
Are you sure you want to delete the selected message?

## *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 tab in this menu which is useful for Administrators is the **Miscellaneous** tab, which holds account preferences.

### Core settings

The Core settings tab under Options, displays the basic information which categorizes 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.)

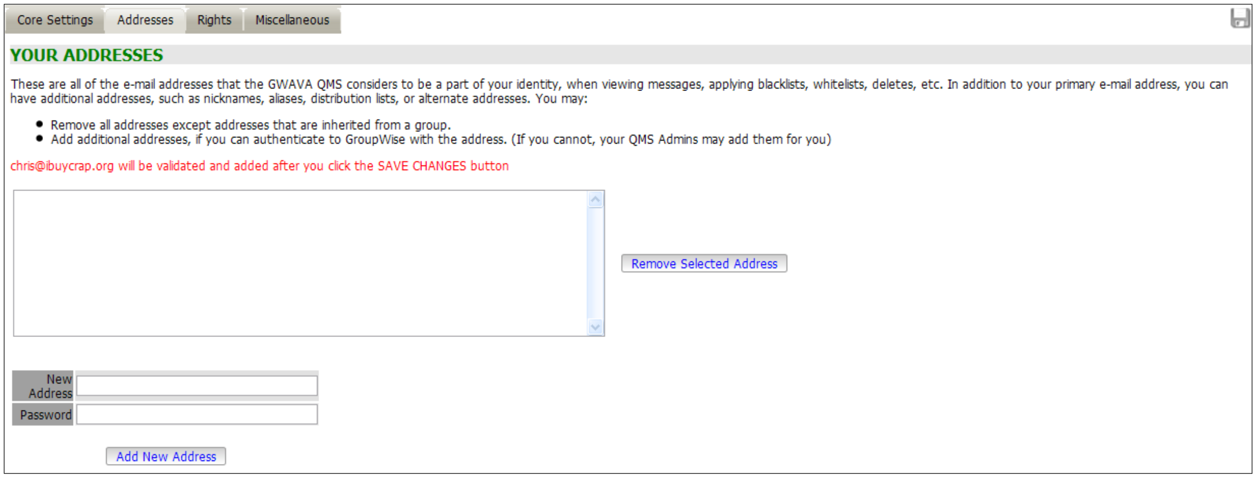


CORE SETTINGS

The primary address is the address you use to log into the GWAVA QMS. You will be allowed to change it if you can supply a password to authenticate against GroupWise. The Password field is blank by default, because the GWAVA QMS doesn't store passwords.

| | |
|---|---|
| UserID | chris@bricebitter.com |
| Group | default |
| Address | chris@bricebitter.com |
| Password | |

## Addresses



**YOUR ADDRESSES**

These are all of the e-mail addresses that the GWAVA QMS considers to be a part of your identity, when viewing messages, applying blacklists, whitelists, deletes, etc. In addition to your primary e-mail address, you can have additional addresses, such as nicknames, aliases, distribution lists, or alternate addresses. You may:

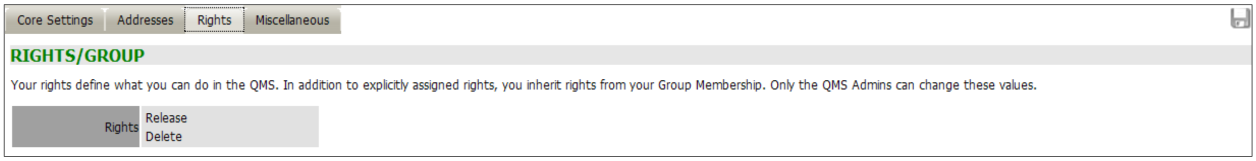
- Remove all addresses except addresses that are inherited from a group.
- Add additional addresses, if you can authenticate to GroupWise with the address. (If you cannot, your QMS Admins may add them for you)

chris@ibuycrap.org will be validated and added after you click the SAVE CHANGES button

User’s 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.



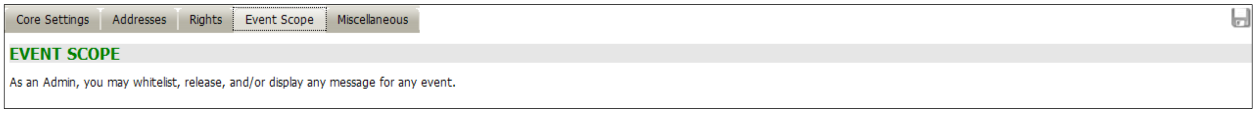
**RIGHTS/GROUP**

Your rights define what you can do in the QMS. In addition to explicitly assigned rights, you inherit rights from your Group Membership. Only the QMS Admins can change these values.

| | |
|---|---|
| Rights | Release<br>Delete |

## 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.



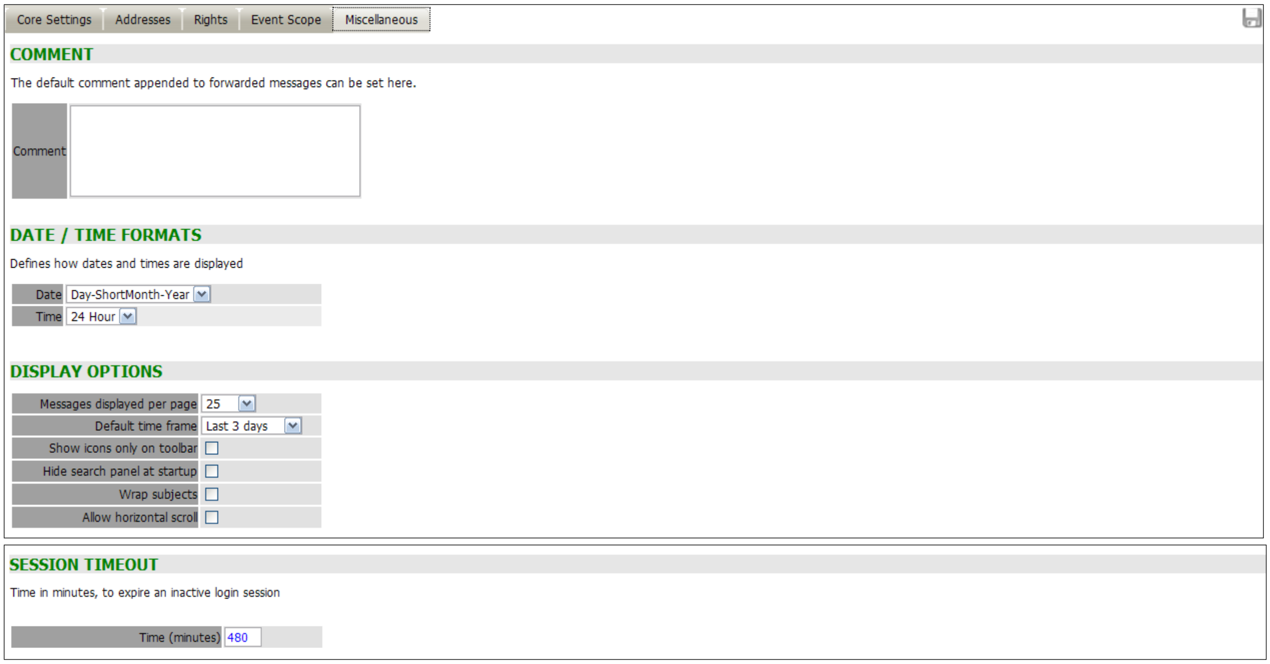
**EVENT SCOPE**

As an Admin, you may whitelist, release, and/or display any message for any event.

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.



COMMENT

The default comment appended to forwarded messages can be set here.

Comment

DATE / TIME FORMATS

Defines how dates and times are displayed

Date: Day-ShortMonth-Year
Time: 24 Hour

DISPLAY OPTIONS

Messages displayed per page: 25
Default time frame: Last 3 days
Show icons only on toolbar □
Hide search panel at startup □
Wrap subjects □
Allow horizontal scroll □

SESSION TIMEOUT

Time in minutes, to expire an inactive login session

Time (minutes): 480

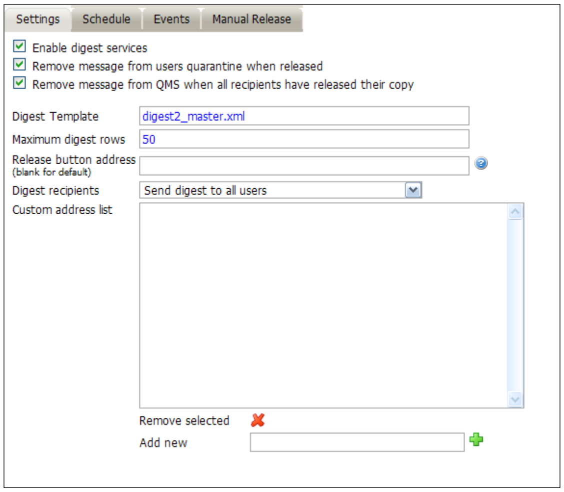
## *Digest*

GWAVA 4.5 can be setup to send regular reports to users when mail is blocked from a users address. Messages listed on the GWAVA 4.5 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.



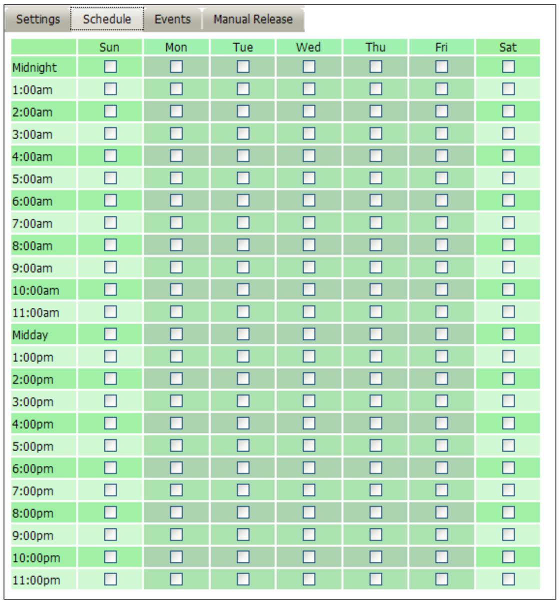
☑ Enable digest services
☑ Remove message from users quarantine when released
☑ Remove message from QMS when all recipients have released their copy

Digest Template: digest2_master.xml
Maximum digest rows: 50
Release button address (blank for default):
Digest recipients: Send digest to all users
Custom address list

Remove selected
Add new

## 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.

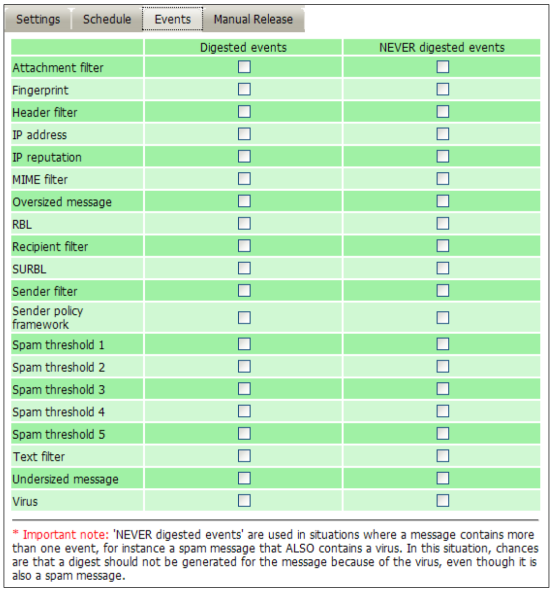


| | Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|---|---|---|---|---|---|---|---|
| Midnight | □ | □ | □ | □ | □ | □ | □ |
| 1:00am | □ | □ | □ | □ | □ | □ | □ |
| 2:00am | □ | □ | □ | □ | □ | □ | □ |
| 3:00am | □ | □ | □ | □ | □ | □ | □ |
| 4:00am | □ | □ | □ | □ | □ | □ | □ |
| 5:00am | □ | □ | □ | □ | □ | □ | □ |
| 6:00am | □ | □ | □ | □ | □ | □ | □ |
| 7:00am | □ | □ | □ | □ | □ | □ | □ |
| 8:00am | □ | □ | □ | □ | □ | □ | □ |
| 9:00am | □ | □ | □ | □ | □ | □ | □ |
| 10:00am | □ | □ | □ | □ | □ | □ | □ |
| 11:00am | □ | □ | □ | □ | □ | □ | □ |
| Midday | □ | □ | □ | □ | □ | □ | □ |
| 1:00pm | □ | □ | □ | □ | □ | □ | □ |
| 2:00pm | □ | □ | □ | □ | □ | □ | □ |
| 3:00pm | □ | □ | □ | □ | □ | □ | □ |
| 4:00pm | □ | □ | □ | □ | □ | □ | □ |
| 5:00pm | □ | □ | □ | □ | □ | □ | □ |
| 6:00pm | □ | □ | □ | □ | □ | □ | □ |
| 7:00pm | □ | □ | □ | □ | □ | □ | □ |
| 8:00pm | □ | □ | □ | □ | □ | □ | □ |
| 9:00pm | □ | □ | □ | □ | □ | □ | □ |
| 10:00pm | □ | □ | □ | □ | □ | □ | □ |
| 11:00pm | □ | □ | □ | □ | □ | □ | □ |

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.



| | Digested events | NEVER digested events |
|---|---|---|
| Attachment filter | □ | □ |
| Fingerprint | □ | □ |
| Header filter | □ | □ |
| IP address | □ | □ |
| IP reputation | □ | □ |
| MIME filter | □ | □ |
| Oversized message | □ | □ |
| RBL | □ | □ |
| Recipient filter | □ | □ |
| SURBL | □ | □ |
| Sender filter | □ | □ |
| Sender policy framework | □ | □ |
| Spam threshold 1 | □ | □ |
| Spam threshold 2 | □ | □ |
| Spam threshold 3 | □ | □ |
| Spam threshold 4 | □ | □ |
| Spam threshold 5 | □ | □ |
| Text filter | □ | □ |
| Undersized message | □ | □ |
| Virus | □ | □ |

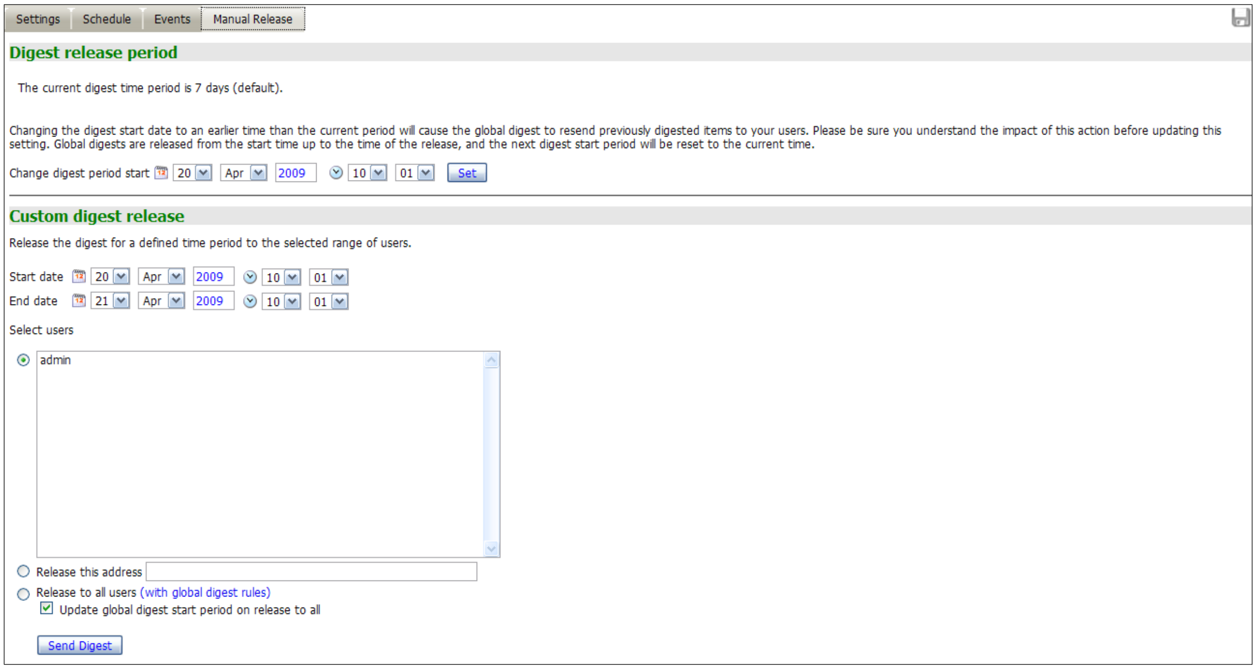
* Important note: 'NEVER digested events' are used in situations where a message contains more than one event, for instance a spam message that ALSO contains a virus. In this situation, chances are that a digest should not be generated for the message because of the virus, even though it is also a spam message.

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’.



Digest release period

The current digest time period is 7 days (default).

Changing the digest start date to an earlier time than the current period will cause the global digest to resend previously digested items to your users. Please be sure you understand the impact of this action before updating this setting. Global digests are released from the start time up to the time of the release, and the next digest start period will be reset to the current time.

Change digest period start: 20 Apr 2009 10 01 [Set]

Custom digest release

Release the digest for a defined time period to the selected range of users.

Start date: 20 Apr 2009 10 01
End date: 21 Apr 2009 10 01

Select users

● admin

○ Release this address

○ Release to all users (with global digest rules)

☑ Update global digest start period on release to all

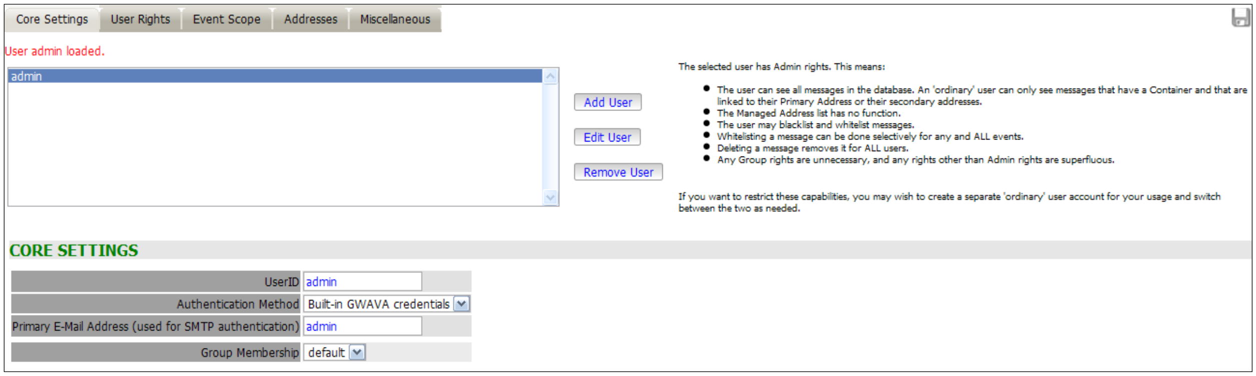
A custom digest may be sent to specific users, or all users, with a specific time frame. This bypasses the usual user list, and does not set the time stamp, unless all users are selected as the release group.

## *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 GroupWise 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 admin loaded.

The selected user has Admin rights. This means:

- The user can see all messages in the database. An 'ordinary' user can only see messages that have a Container and that are linked to their Primary Address or their secondary addresses.
- The Managed Address list has no function.
- The user may blacklist and whitelist messages.
- Whitelisting a message can be done selectively for any and ALL events.
- Deleting a message removes it for ALL users.
- Any Group rights are unnecessary, and any rights other than Admin rights are superfluous.

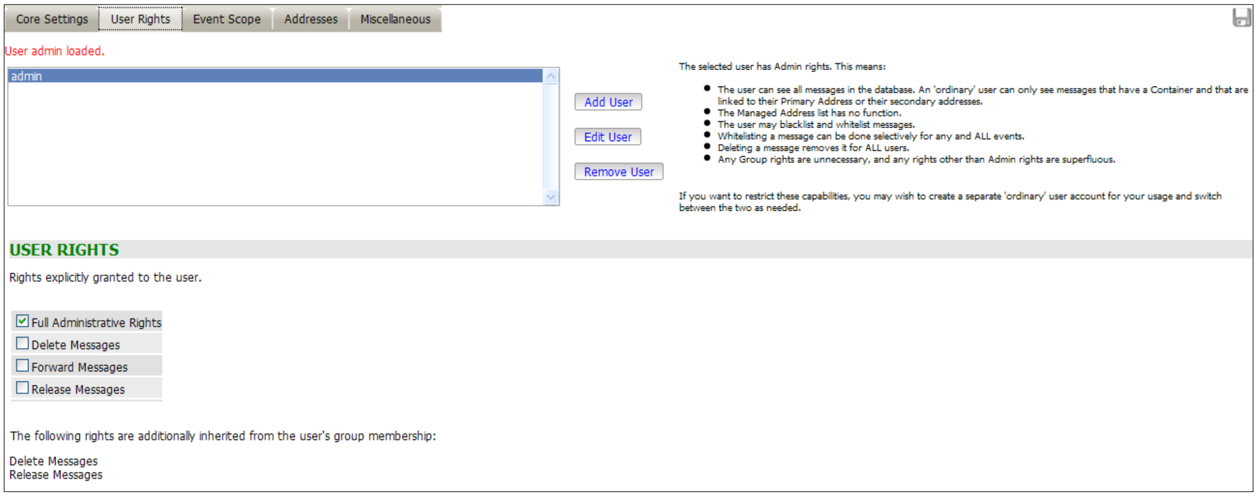
If you want to restrict these capabilities, you may wish to create a separate 'ordinary' user account for your usage and switch between the two as needed.

CORE SETTINGS

| | |
|---|---|
| UserID | admin |
| Authentication Method | Built-in GWAVA credentials |
| Primary E-Mail Address (used for SMTP authentication) | admin |
| Group Membership | default |

### 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.



User admin loaded.

The selected user has Admin rights. This means:

- The user can see all messages in the database. An 'ordinary' user can only see messages that have a Container and that are linked to their Primary Address or their secondary addresses.
- The Managed Address list has no function.
- The user may blacklist and whitelist messages.
- Whitelisting a message can be done selectively for any and ALL events.
- Deleting a message removes it for ALL users.
- Any Group rights are unnecessary, and any rights other than Admin rights are superfluous.

If you want to restrict these capabilities, you may wish to create a separate 'ordinary' user account for your usage and switch between the two as needed.

USER RIGHTS

Rights explicitly granted to the user.

☑ Full Administrative Rights
☐ Delete Messages
☐ Forward Messages
☐ Release Messages

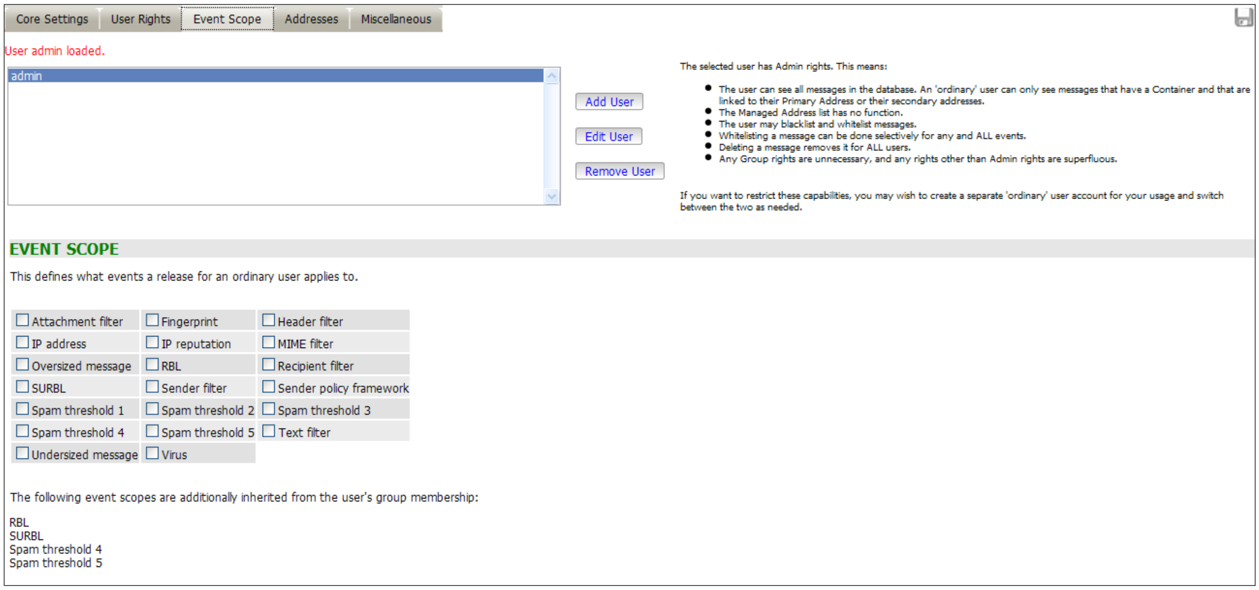
The following rights are additionally inherited from the user's group membership:

Delete Messages
Release Messages

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.



User admin loaded.

The selected user has Admin rights. This means:

- The user can see all messages in the database. An 'ordinary' user can only see messages that have a Container and that are linked to their Primary Address or their secondary addresses.
- The Managed Address list has no function.
- The user may blacklist and whitelist messages.
- Whitelisting a message can be done selectively for any and ALL events.
- Deleting a message removes it for ALL users.
- Any Group rights are unnecessary, and any rights other than Admin rights are superfluous.

If you want to restrict these capabilities, you may wish to create a separate 'ordinary' user account for your usage and switch between the two as needed.

**EVENT SCOPE**

This defines what events a release for an ordinary user applies to.

| | | |
|---|---|---|
| □ Attachment filter | □ Fingerprint | □ Header filter |
| □ IP address | □ IP reputation | □ MIME filter |
| □ Oversized message | □ RBL | □ Recipient filter |
| □ SURBL | □ Sender filter | □ Sender policy framework |
| □ Spam threshold 1 | □ Spam threshold 2 | □ Spam threshold 3 |
| □ Spam threshold 4 | □ Spam threshold 5 | □ Text filter |
| □ Undersized message | □ Virus | |

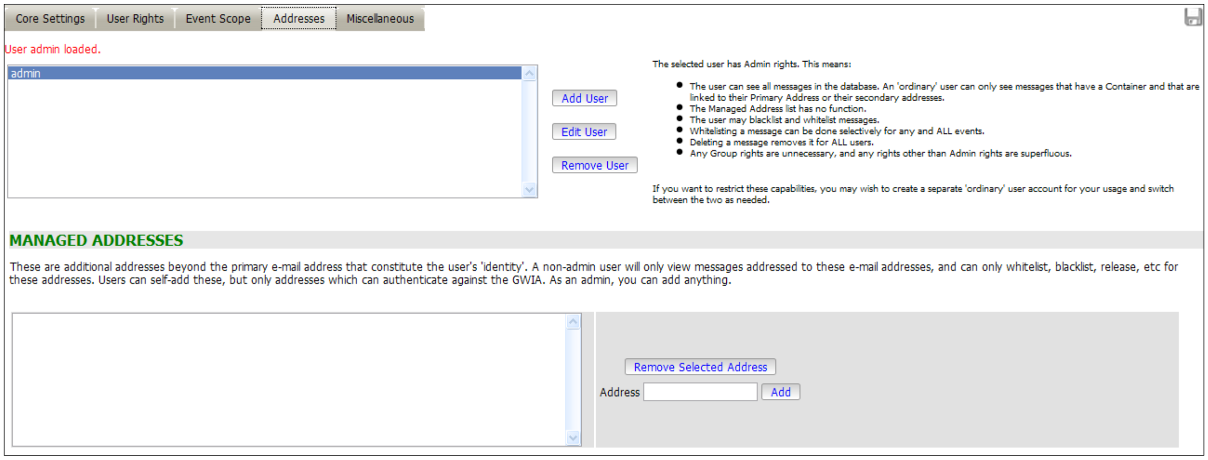
The following event scopes are additionally inherited from the user's group membership:

RBL
SURBL
Spam threshold 4
Spam threshold 5

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.



User admin loaded.

The selected user has Admin rights. This means:

- The user can see all messages in the database. An 'ordinary' user can only see messages that have a Container and that are linked to their Primary Address or their secondary addresses.
- The Managed Address list has no function.
- The user may blacklist and whitelist messages.
- Whitelisting a message can be done selectively for any and ALL events.
- Deleting a message removes it for ALL users.
- Any Group rights are unnecessary, and any rights other than Admin rights are superfluous.

If you want to restrict these capabilities, you may wish to create a separate 'ordinary' user account for your usage and switch between the two as needed.

**MANAGED ADDRESSES**

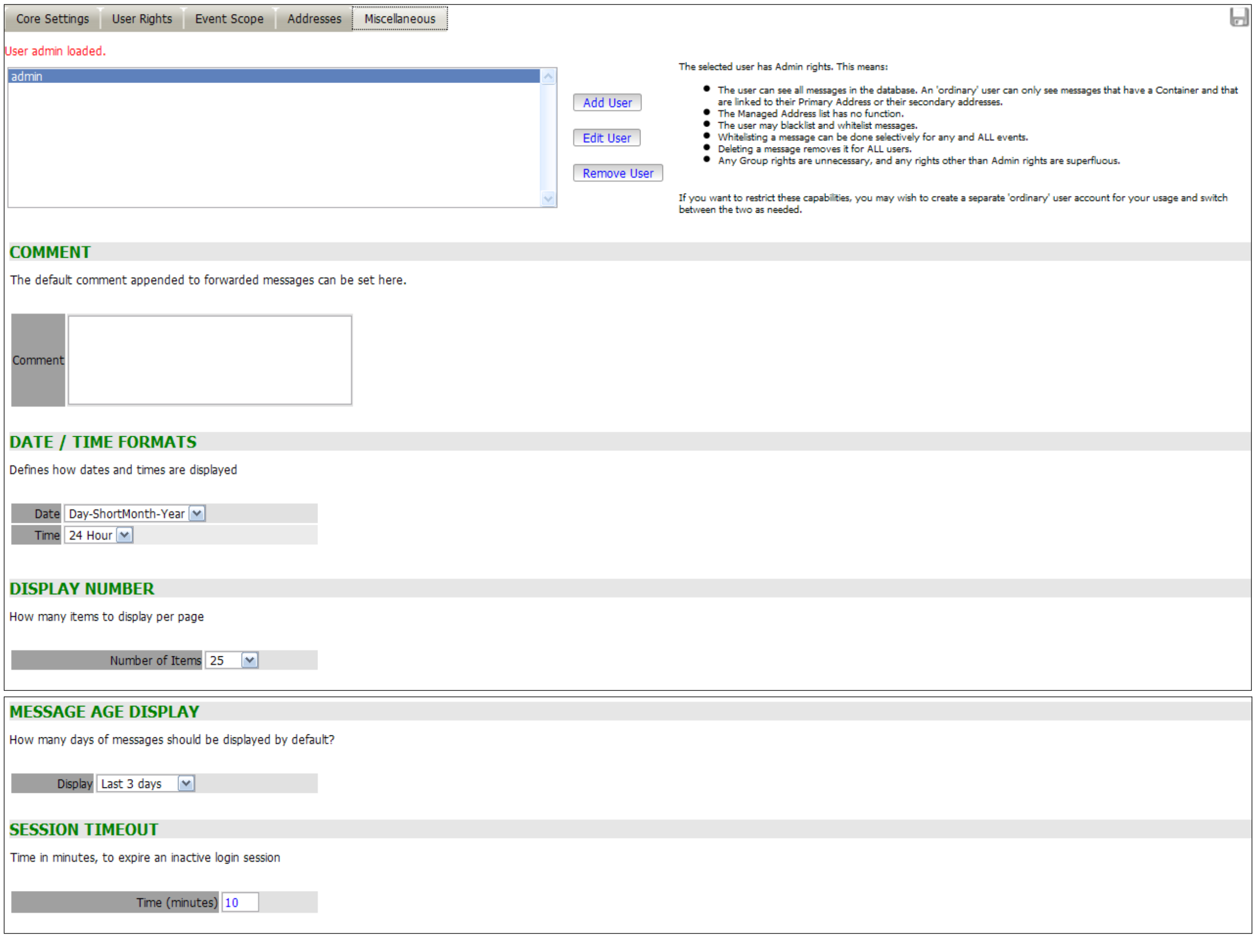
These are additional addresses beyond the primary e-mail address that constitute the user's 'identity'. A non-admin user will only view messages addressed to these e-mail addresses, and can only whitelist, blacklist, release, etc for these addresses. Users can self-add these, but only addresses which can authenticate against the GWIA. As an admin, you can add anything.

Address

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.



User admin loaded.

admin

The selected user has Admin rights. This means:

- The user can see all messages in the database. An 'ordinary' user can only see messages that have a Container and that are linked to their Primary Address or their secondary addresses.
- The Managed Address list has no function.
- The user may blacklist and whitelist messages.
- Whitelisting a message can be done selectively for any and ALL events.
- Deleting a message removes it for ALL users.
- Any Group rights are unnecessary, and any rights other than Admin rights are superfluous.

If you want to restrict these capabilities, you may wish to create a separate 'ordinary' user account for your usage and switch between the two as needed.

COMMENT

The default comment appended to forwarded messages can be set here.

Comment

DATE / TIME FORMATS

Defines how dates and times are displayed

Date: Day-ShortMonth-Year
Time: 24 Hour

DISPLAY NUMBER

How many items to display per page

Number of Items: 25

MESSAGE AGE DISPLAY

How many days of messages should be displayed by default?

Display: Last 3 days

SESSION TIMEOUT

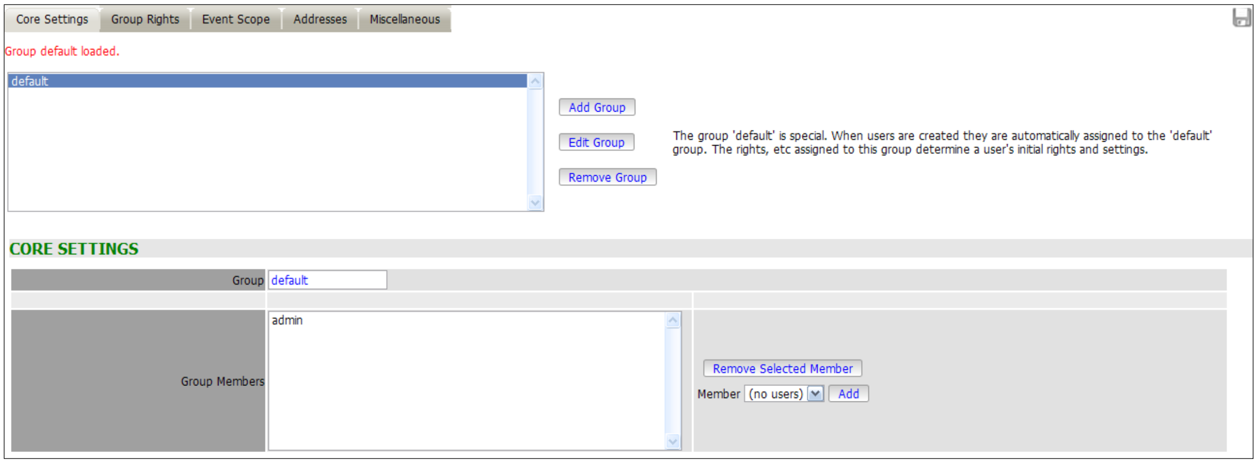
Time in minutes, to expire an inactive login session

Time (minutes): 10

### *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.



Group default loaded.

default

The group 'default' is special. When users are created they are automatically assigned to the 'default' group. The rights, etc assigned to this group determine a user's initial rights and settings.

Group: default

Group Members: admin

Member: (no users)

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.

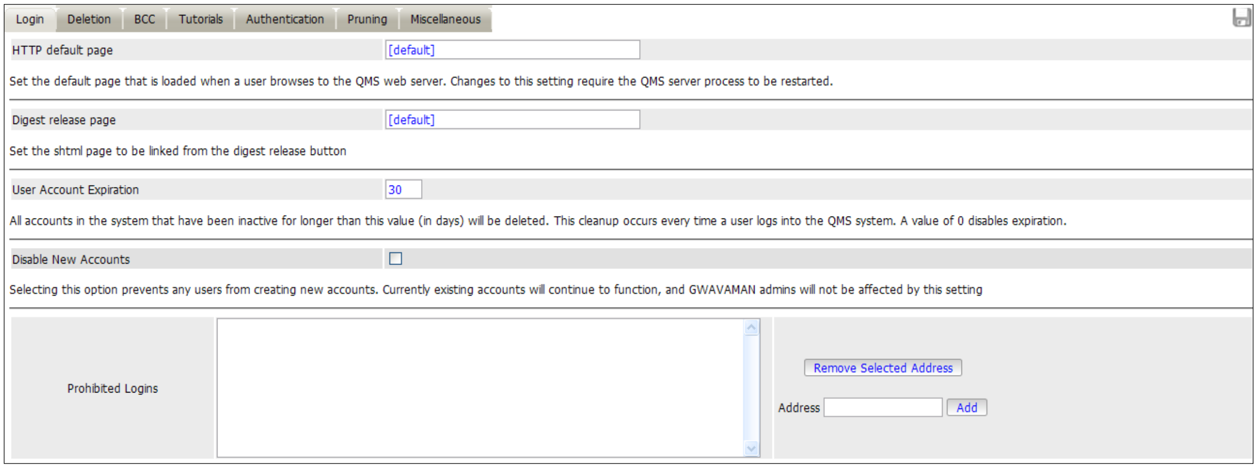
If a group address exists in the system, (i.e. sales@domain.com), the admin create a group for sales, and add the sales@domain.com address to the managed address section of the group. Having the group manage the address causes mail to that address to show up in the quarantine and digest for each user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



HTTP default page [default]

Set the default page that is loaded when a user browses to the QMS web server. Changes to this setting require the QMS server process to be restarted.

Digest release page [default]

Set the shtml page to be linked from the digest release button

User Account Expiration 30

All accounts in the system that have been inactive for longer than this value (in days) will be deleted. This cleanup occurs every time a user logs into the QMS system. A value of 0 disables expiration.

Disable New Accounts □

Selecting this option prevents any users from creating new accounts. Currently existing accounts will continue to function, and GWAVAMAN admins will not be affected by this setting

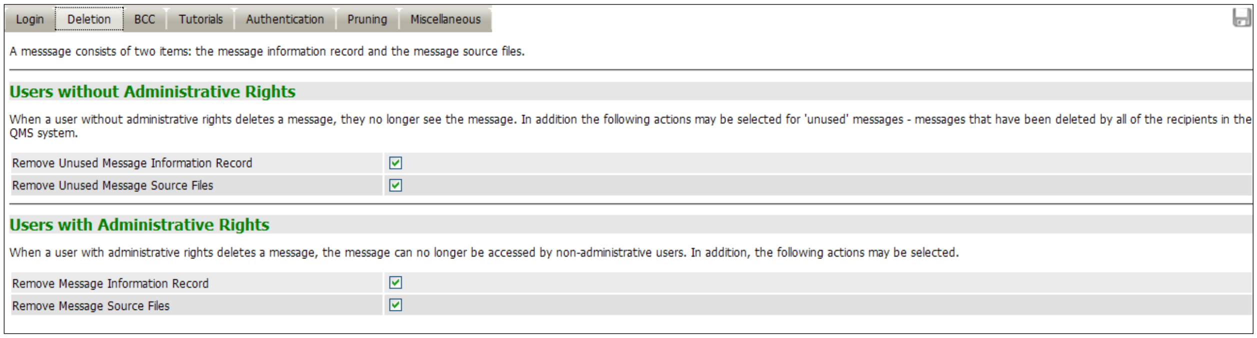
Prohibited Logins

Address

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



A messsage consists of two items: the message information record and the message source files.

**Users without Administrative Rights**

When a user without administrative rights deletes a message, they no longer see the message. In addition the following actions may be selected for 'unused' messages - messages that have been deleted by all of the recipients in the QMS system.

Remove Unused Message Information Record ☑

Remove Unused Message Source Files ☑

**Users with Administrative Rights**

When a user with administrative rights deletes a message, the message can no longer be accessed by non-administrative users. In addition, the following actions may be selected.

Remove Message Information Record ☑

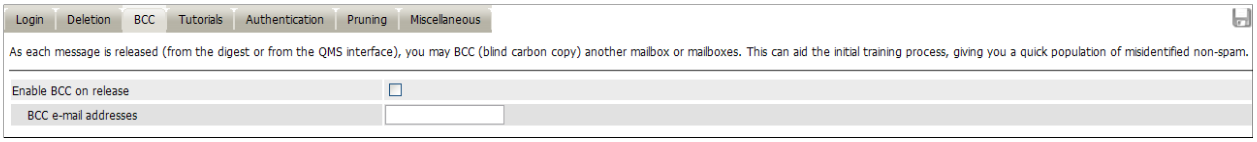
Remove Message Source Files ☑

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 is an integral part of training the probability spam engine. If the signature spam engine, recommended, is used instead of the probability engine, this option is unnecessary.  When using the probability engine, harvesting good mail and fine tuning the system to accept and allow messages that it is erroneously blocking is a challenging chore. The BCC on release option allows caught messages which are released from QMS to be blind carbon copied to a feeder address, which can then be sorted and added to the appropriate learning feeder.  **Not all messages released from QMS will be good mail.**

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



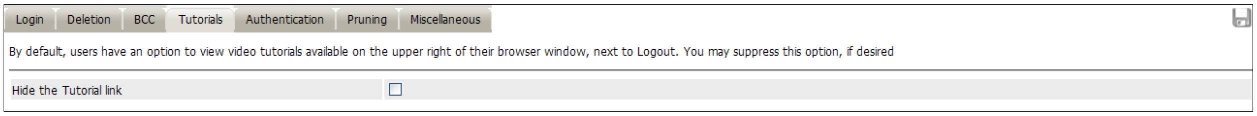
As each message is released (from the digest or from the QMS interface), you may BCC (blind carbon copy) another mailbox or mailboxes. This can aid the initial training process, giving you a quick population of misidentified non-spam.

Enable BCC on release ☐

BCC e-mail addresses

## 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.

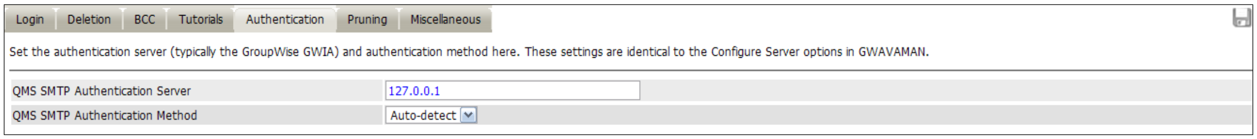


By default, users have an option to view video tutorials available on the upper right of their browser window, next to Logout. You may suppress this option, if desired

Hide the Tutorial link ☐

## 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'.



Set the authentication server (typically the GroupWise GWIA) and authentication method here. These settings are identical to the Configure Server options in GWAVAMAN.

QMS SMTP Authentication Server 127.0.0.1

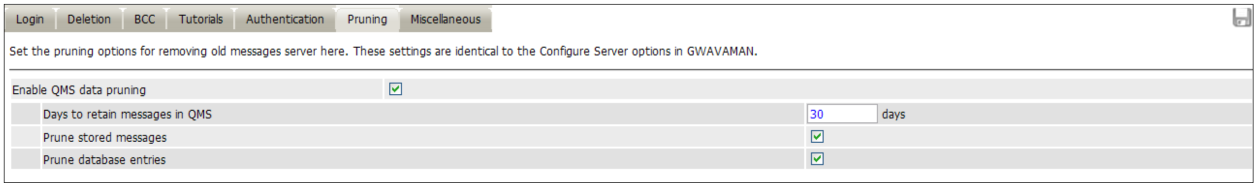
QMS SMTP Authentication Method Auto-detect

An alternate port for the SMTP may be specified, using a colon then the port number after the IP address, i.e. 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.



Set the pruning options for removing old messages server here. These settings are identical to the Configure Server options in GWAVAMAN.

Enable QMS data pruning ☑

Days to retain messages in QMS 30 days

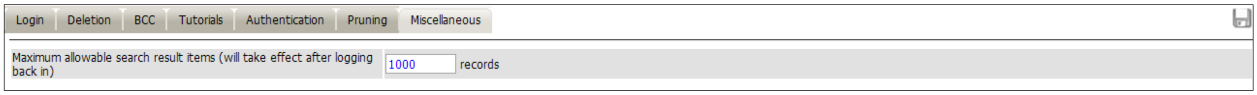
Prune stored messages ☑

Prune database entries ☑

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.

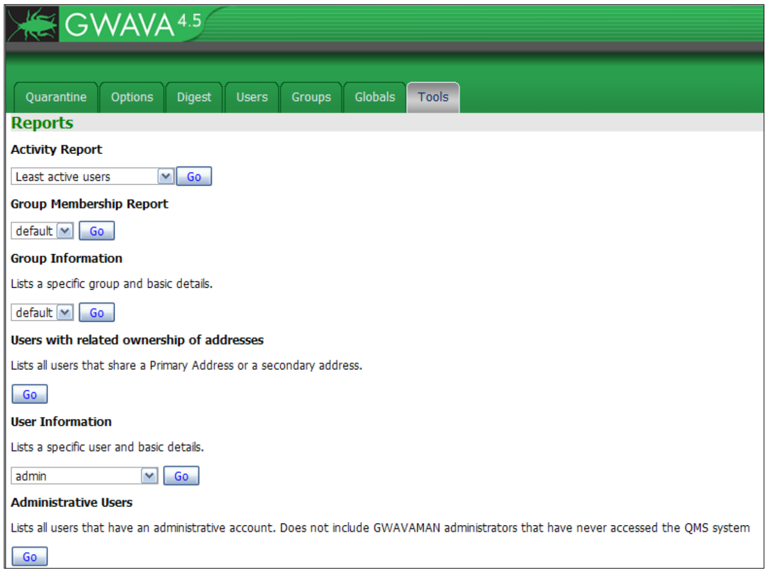


Maximum allowable search result items (will take effect after logging back in) 1000 records

## *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'.



Reports

Activity Report

Least active users

Group Membership Report

default

Group Information

Lists a specific group and basic details.

default

Users with related ownership of addresses

Lists all users that share a Primary Address or a secondary address.

User Information

Lists a specific user and basic details.

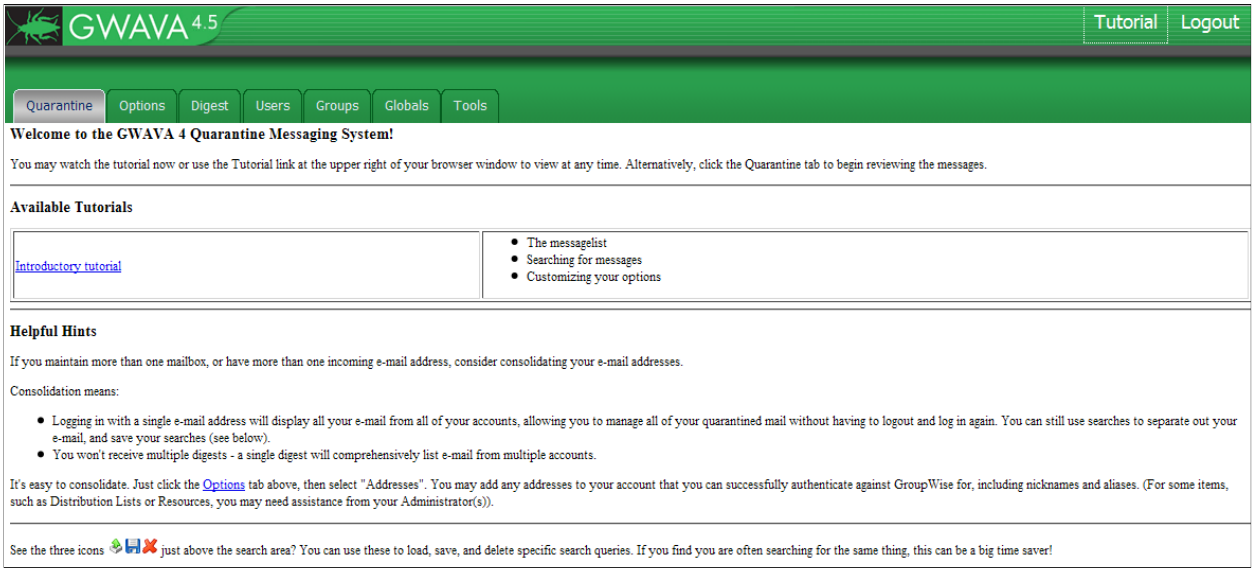
admin

Administrative Users

Lists all users that have an administrative account. Does not include GWAVAMAN administrators that have never accessed the QMS system

## Tutorials

The Quarantine tutorial link is located near the top of the page, and is customized and shown for both general users and administrators.  The tutorials, however, are not the same. General users see a tutorial tailored for default user accounts and rights, while the administrator has access to a tutorial detailing the functions of the administrator level accounts.



**Welcome to the GWAVA 4 Quarantine Messaging System!**

You may watch the tutorial now or use the Tutorial link at the upper right of your browser window to view at any time. Alternatively, click the Quarantine tab to begin reviewing the messages.

**Available Tutorials**

| | |
|---|---|
| Introductory tutorial | • The messagelist<br>• Searching for messages<br>• Customizing your options |

**Helpful Hints**

If you maintain more than one mailbox, or have more than one incoming e-mail address, consider consolidating your e-mail addresses.

Consolidation means:

- Logging in with a single e-mail address will display all your e-mail from all of your accounts, allowing you to manage all of your quarantined mail without having to logout and log in again. You can still use searches to separate out your e-mail, and save your searches (see below).
- You won't receive multiple digests - a single digest will comprehensively list e-mail from multiple accounts.

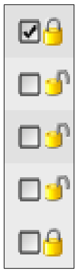
It's easy to consolidate. Just click the Options tab above, then select "Addresses". You may add any addresses to your account that you can successfully authenticate against GroupWise for, including nicknames and aliases. (For some items, such as Distribution Lists or Resources, you may need assistance from your Administrator(s)).

See the three icons ⬇💾✖ just above the search area? You can use these to load, save, and delete specific search queries. If you find you are often searching for the same thing, this can be a big time saver!

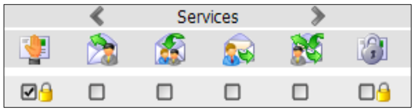
Tutorials may be accessed at any time by selecting the tutorial link at the top right of the page.

# Appendix

## Four 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 “**Enable Four State Checkboxes”.** 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. Both images show here are set to the same setting: always block, never quarantine. For the events that these settings are active for, the messages will always be blocked and never quarantined, regardless of exceptions or other actions that are active on that message.



## GWIA and SMTP scanners on the same box:

http://support2.gwava.com/kb/?View=entry&EntryID=1215

## SMTP scanner ports

If the GWAVA SMTP scanner 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

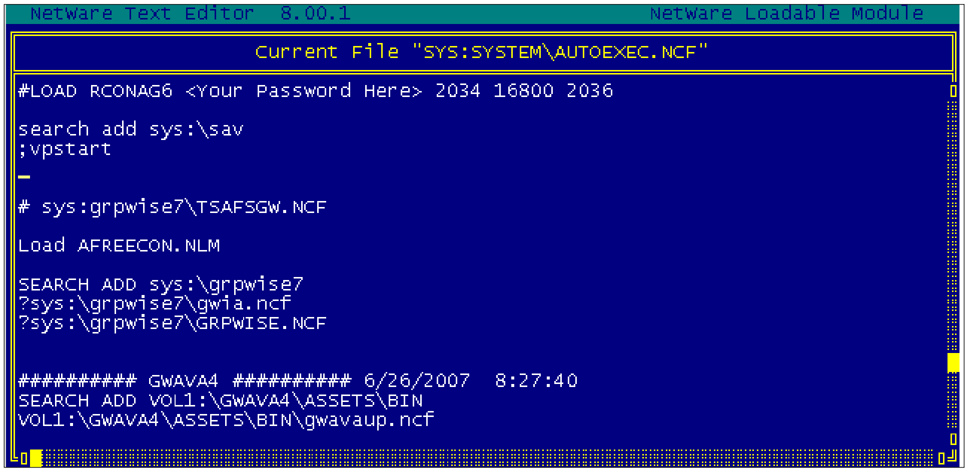
Some GWAVA scanners require the location to the active GroupWise configuration files on setup. On NetWare, the paths to these files can be found by looking through the autoexec.ncf file. Instructions, following below, describe how to use the autoexec.ncf to locate the configuration files.

### 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 scanner setup wizard.  (ie. search for 'gwia.ncf' in NetWare. For Linux, search for 'gwia.cfg'. Search in the likely GroupWise file structure to shorten the search time.)

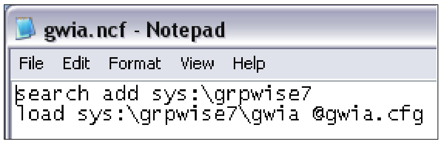
### NetWare

If the GroupWise system loads automatically during startup, load up the autoexec.ncf in an edit window by typing "edit autoexec.ncf". Scroll to the bottom of the autoexec.ncf and it should look similar to the following example.


NetWare Text Editor  8.00.1
NetWare Loadable Module
Current File "SYS:SYSTEM\AUTOEXEC.NCF"

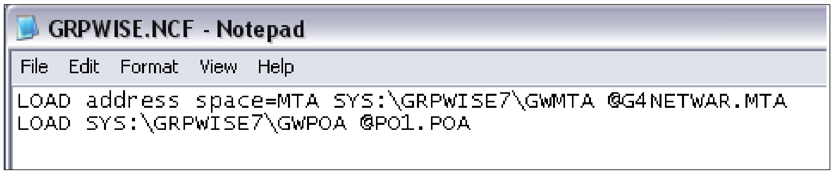
```
#LOAD RCONAG6 <Your Password Here> 2034 16800 2036

search add sys:\sav
;vpstart
_

# sys:grpwise7\TSAFSGW.NCF

Load AFREECON.NLM

SEARCH ADD sys:\grpwise7
?sys:\grpwise7\gwia.ncf
?sys:\grpwise7\GRPWISE.NCF


########## GWAVA4 ########## 6/26/2007  8:27:40
SEARCH ADD VOL1:\GWAVA4\ASSETS\BIN
VOL1:\GWAVA4\ASSETS\BIN\gwavaup.ncf
```

In the autexec.ncf, look for the gwia.ncf or the grpwise.ncf. If you found those files, look at where it is located. In this example it is located in sys:\grpwise7. Now that I know that sys:\grpwise7 has some of my data in it I can look in there for more information. From my administrative workstation I access that directory and look inside the gwia.ncf first. I now know that my gwia.cfg is located in sys:\grpwise7



```
search add sys:\grpwise7
load sys:\grpwise7\gwia @gwia.cfg
```

Now I need to find my MTA startup file so I open grpwise.ncf. After reviewing grpwise.ncf I know that my MTA startup file is named G4NETWAR.MTA and is located in sys:\grpwise7.



```
LOAD address space=MTA SYS:\GRPWISE7\GWMTA @G4NETWAR.MTA
LOAD SYS:\GRPWISE7\GWPOA @PO1.POA
```

At this point you should have enough information to complete the scanner wizard.