



Micro Focus Secure Messaging Gateway Administrator's Guide

September 2017

Legal Notices

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

Copyright © 2017 Micro Focus Software, Inc. All Rights Reserved.

Contents

Preface	5
1 Micro Focus Secure Messaging Gateway	27
Overview	27
Micro Focus GWAVA Family of Message Handling Products	27
2 Installation	29
System Requirements	29
Overview	29
System Requirements	29
Ports Used by Secure Messaging Gateway	29
OVA Installation	30
OVA Deployment	30
Secure Messaging Gateway Installation	35
ISO Installation	39
Configuration	41
Post-Install Tasks	49
On the Secure Messaging Gateway server	49
On the Email Server	52
Installing into an Existing Secure Messaging Gateway Network	53
Overview	53
Setup	53
GWAVA 6 to Secure Messaging Gateway Migration	57
Pre-migration Tasks	57
Migration	62
Setting up a Multi-Tenant System	69
3 System Administration	71
System Management	72
Manage Servers	72
Languages	75
Templates	76
User Interfaces	79
URI Association	81
Database Connections	82
File System Rights	83
Password Control	87
System Alerts	87
Scanner Diagnostic	88
Licensing	90
Online Updates	91
Module Management	92
Module Status	92
Module Management	93
Interfaces	93
Scan Engine Manager	98
Mail Relay Module Manager	99
QMS Module Manager	101

Stats Module Manager	103
Message Tracker Module Manager	103
Organization / Policy Management Overview	104
Settings	106
Manage Users	107
Manage System roles	109
Manage Custom Roles	115
Manage Organizations	118
Domain Management	122
Policy Management	125
Policy Scan Configuration	129
Exceptions	143
New Policy Wizard	145
Creating a Statistics and Tracking Policy	149
Creating a Block and Quarantine with Exceptions Policy	153
Creating an Anti-Virus Policy	159
Enabling Black List and White List	162
Setting up DKIM Verification	165
4 Quarantine System	167
Quarantine	167
Options	170
Core Settings	170
White List	171
Rights	171
Owned Addresses	171
Delegated Access	172
Digest	173
Settings Tab	174
Schedule Tab	175
Manual Release Tab	176
Users	178
User Rights	178
User Options	179
Group Membership	179
Groups	180
Settings	180
Default User	181
Message Retention	182
Forward from Quarantine	182
5 Message Tracker	183
Message Tracker interface	183
Search	184
Date Range	184
Message Details	185
6 User Guide	187
Quarantine Management System	187
Quarantine Email	187
Quarantine Management System	187

Preface

About This Guide

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

Audience

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

Technical Support

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

Sales

Micro Focus contact information and office locations: www.microfocus.com (<http://www.microfocus.com>)

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

Copyright Notice

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

© 2017 GWAVA Inc., a Micro Focus company. All rights reserved.

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

Release Notes

Revision: 307 - created 02-Oct-2017
GWAV-1976 - DKIM signing

Revision: 300 - created 28-Sep-2017
Fix some recently discovered memory leaks
GWAV-2043 Display default rights
GWAV-1757 Enhanced Message Tracking Details
Revision: 289 - created 07-Sep-2017
GWAV-2003 - Add check for loaded IA library when running scan process to prevent crash
GWAV-2024 - Fix typo
GWAV-2021 - Prevent crash when attempting to send alert and database is inaccessible
Merge GWAV-1936 - Fixes for regex filtering
GWAV-1389 - DKIM validation
GWAV-2031 - Remote connections are provided a relative path to replacement MIME messages
GWAV-1763 - Recolour digest schedule page
Revision: 280 - created 27-Jul-2017
Replaced a GWAVA reference with Secure Gateway in tracker clientsettings.php
(CheckSessionTimeout)
GWAV-1926 - Fix node settings being discarded during workbench configuration with certain combinations of nodes.
Nodes that caused this issue were filter/exception group,av,vod,quarantine,admin quarantine,block and stats
GWAV-1884 - Update instructions to be clearer on how the SMTP envelope filter works
GWAV-1879 - Restored the stopPropagation code to prevent access the search field also triggering the column sorting
GWAV-1955 - Add control of NOOP interval
GWAV-1891 - Add check for broken socket and module shutdown during NOOP command loop
GWAV-1539 - Add migration toolkit
GWAV-9171 - Fixed typo in qms.php
GWAV-1539 - Adding sqlite extension to php
Change references from GWAVA 7 to Secure Gateway
Add workaround for Chrome not allowing file upload in migration toolkit
GWAV-1982 - Add 10 minute timeout to migration script files
Merge GWAV-1585 and GWAV-1727 - New workbench navigation system
GWAV-1985 - Fix crash when TLS fail occurs
Fix issue with TLS auto mode not falling back to non-TLS connection on outbound mail
GWAV-1985 - Fix regression caught by test harness
Fix excessive memory consumption by spf tld lists
Add trusted source switch to scan diagnostics to allow triggering of outbound policies
GWAV-1984 - Fix global quarantine service always being added to migrated policy
Removed an unnecessary query for the message tracker login
GWAV-1996 - Unable to go through setup wizard for G6 Migration
GWAV-1999 - Online update requires command line input
Revision: 245 - created 29-Jun-2017
GWAV-1881 - Changed the query to determine server to use for the Message Tracker UI.
GWAV-1883 - Added code to prevent messages with "special characters" from causing the insert into message tracker to fail.
GWAV-1883 - Removed the subordinate (search tables) from message tracker.
GWAV-1900 - Unzip/Zip installed by default
GWAV-1889 - Add security option and line length limit for outbound SMTP connections
Fix outbound relay targets not using defined line limit

GWAV-1892 - Modify CTAV timestamp update query to use compact version
GWAV-1862 - Fix spelling mistake
GWAV-1857 - Sort QMS groups
Add option to SMTP interface diagnostics screen to retain received message data
GWAV-1781 - Fix spelling mistakes in documentation
GWAV-1814 - Owned Address / Delegated Access branch into the trunk.
(GWAV-1587, GWAV-1814)
GWAV-1917 - Initial work on performance stats.
Adds message size and scan speed stats for the scan engine.
GWAV-1917 - Add processing stats to smtp interface
GWAV-1877 - Cascade proxy errors from EHLO and MAIL commands into client RCPT responses
SMTP Discard target set to use interface external relay line limit
GWAV-1930 - Fixed wording issue in message tracker instructions
GWAV-1934 - Fixed a problem with the owned/delegated code that prevented an admin from
successfully releasing messages from the QMS UI
Add extra diagnostic logging to AS scan process
GWAV-1735 - Branding update from GWAVA to Secure Gateway
Fix merge problems from delegated address issue
GWAV-1924 - The CustomReleaseURI was not being passed for the digest processing so the custom
address couldn't be used.
GWAV-1924 - Manage my quarantine should also honor the custom release address
New favicon.ico file
Updated title image for digest
Revision: 215 - created 25-May-2017
GWAV-1848 - Fix potential QMS startup crash when queued items are waiting to be processed
GWAV-1852 - Add logging on completion of filters
GWAV-1852 - Add an extra log line to isolate performance issue
GWAV-1784 - Disable Connection Drop Services and DoS for trusted Relays
GWAV-1851 - Unable to release message from QMS with Blank Sender
GWAV-1858 - Fix whitelists not converting patterns into regular expressions
GWAV-1839 - SMTP connection limiting
GWAV-1838 - QMS Roles link
GWAV-1864 - Digests no longer sending when disabled
GWAV-1767 - Message Tracker Service help modifications
Revision: 200 - created 27-Apr-2017
Fix custom user digest setting not displaying correctly when set to EXCLUDED
Fix qms prune data/info options not displaying the correct state when items are disabled
Fix custom roles not able to be removed
Merge GWAV-1830 - Override EHLO/HELO host
Fix Message Tracker role ID causing custom role creation issue on first attempt
Add missing test harness files
Modify wording of "View HTML Messages" to "View Message HTML" in QMS rights
GWAV-1845 - Fix invalid path error in browser console when loading admin UI
GWAV-1499 - Upload large files through PHP
Revision: 189 - created 30-Mar-2017
Fix issue with HTTP upload process mapping source data type to incorrect method
Fix HTML signature populating TEXT signature in UI when reloading node
Add option to disable multi-threaded filters within an engine module

GWAV-1689 - Custom Roles

GWAV-1815 - Add move object button to domains management page

GWAV-1771 - Policies created with wizard can now be deleted/moved/cloned immediately after creation

Implement cipher list support for SMTP module SSL

GWAV-1502 - Alter user last login info for users that have no login data recorded

GWAV-1773 - Add exception handling to filter calls and fix possible usage of nullptr if MIME message cannot extract root entity during fingerprint tests

Merge GWAV-1810 - Staggered DB sequences

Add missing icon to notes box on workbench

GWAV-1482 - Fix filters not saving in Chrome

GWAV-1701 - Fix issue when parent events of events are removed, causing cascade deletes of attached events

GWAV-1770 - New policies created with the wizard are suffixed with a number if a duplicate name would occur to make it easy to distinguish

Fix log retention days not saving

Fix resetadmin startup switch to allow creation of new accounts, and to apply the selected user to the System Admin role if it's not linked to ensure a UI is available to use

Add deep exception handling of suspect fingerprint functions

Adding libarchive13/xenial-backports to default install.

GWAV-1764 Fix unformatted date in digest template.

GWAV-1835 - Modify text filter search algorithm to reduce complexity of generated regexes to prevent runaway expressions.

Added exception handling to catch and report other such instances that are not procedurally detectable.

GWAV-1764 Fix unformatted date in digest template.

GWAV-1592 Fix blank notifications

Revision: 165 - created 24-Feb-2017

GWAV-1240 - Message tag docs

GWAV-1772 - Update to Cyren AVSDK 5.4.30-r1

GWAV-1589 - QMS control service

GWAV-1779 - Update to latest ctengine version 8.01.00001

Gwav-1775 - From address in QMS is not the same as GWVSMTP

GWAV-1780 - Update to CTIPD 4.01.0000.1

GWAV-1554 - Add Message Tracker to GWAVA 7

GWAV-1793 - Add a log entry suggesting the cause of error when loading domains as being related to an invalid date being provided in the OU expiration date field

Add validation check to expiry date input field in Manage Organizations page

GWAV-1793 - Modify date to todays date when invalid

GWAV-1767 - Fixed wording for message tracker service node

The message tracker service was not correctly looking up filter information

GWAV-1398 - Rework get_message_data.php for QMS and message tracker to better handle the creation of the JSON tables.

This fixes the problem where some characters would break the JSON.

Revision: 154 - created 26-Jan-2017

Bug GWAV-1557 Establish connection to Qms Database each time a different OU is selected using the OU selector

Bug GWAV-1543 Fixed issues with Digest release in multi-OU environment.

Merge GWAV-1546, which includes:

Support for OpenOffice fingerprint
 Support for MSOfficeXML fingerprint
 Support for password protected compressed zip files
 Support for corrupt zip file detection
 Support for deep/wide compressed files
 Support for zip files that are not application files
 Fix bug in FileHandling read file into memory when number of bytes to read matches the target file size-1
 Support for libarchive13/xenial-backports
 GWAV-1544 Support for Interface control
 GWAV-1025 - Fix broken zip test not requesting file commit to disk, creating false positive
 GWAV-1733 - Fix text issue in Manage Organizations instructions
 GWAV-1736 - Update to latest ctengine version 8.00.0125.1
 GWAV-1737 - Update to latest ctupd version 4.00.0036.1
 GWAV-1559 - Fix crash when multithreaded scanning is used with filters that require disk access to extracted MIME entities
 GWAV-1478 - Fix gwvrelay crash caused by invalid memory access
 GWAV-1558 - Policy qualification to have additional conditions
 GWAV-1524 - Cloning an OU does not bring across node comments
 GWAV-1744 - Fix crash caused by multithreaded sync issue
 GWAV-1765 - Unable to clone policies fixed
 GWAV-1766 - Unable to move policies fixed
 Revision: 141 - created 13-Oct-2016
 Fix misreporting of source address exception when no exception has occurred
 Bug: GWAV-1476, Fixed content type for logo
 Fixed problem with php sessions
 Modify label for server bind address to source bind address
 Revision: 134 - created 30-Sep-2016
 Bug#GWAV-1487 - Fix crash when applying text signature
 Add server version info to titlebar for sysadmins
 Bug#GWAV-1474 - Fix error saving properties of newly created users when UI page is not refreshed
 Enable licensing code
 Beta label removed
 Online updater refreshes titlebar after completing update process
 Revision: 127 - created 28-Sep-2016
 Added default digest template and forward as attachment template to install new system script
 Bug GWAV-1476.
 Minor fixes to the digest template
 Bug GWAV-1484 Add right to allow or prevent a user from being able to view the HTML message body
 Documentation updates
 Bug gwav-1486 added code to SendNoopKeepAliveCommands function to handle an exception if it occurs in the SendNoop method
 Bug GWAV-1473 Added more support for admin statuses (users without associated email address in quarantine)
 Bug GWAV-1476 More minor changes to digest template
 Modify initial setup script to create default relay addresses on the 172 range using CIDR for full private address range coverage

Add option to OU management to restrict user account names to the domains hosted by the OU
Add option for outbound SMTP connections to use a relay host list
Bug#GWAV-1362 - Add button panel to role management page
Add refresh button to the title bar
Add automatic tip popup to system web setup
Implement interface session independence to allow qms and management interfaces to be usable simultaneously within the same browser
Add missing help image to system web setup
Alter duplicatestring function to return null on memory allocation error rather than throwing an exception
Add const correctness to base 64 decode function
Roll back changes to concurrent login system which has issues running on php7
Update online updater to correctly decode XML content for scripts
Add PHP CURL support to appliance
Revision: 118 - created 15-Sep-2016
Change status AttachmentAccessed to Viewed Message
Fixes to status column to allow for not clearing the checkboxes
Fixed view message status settings
Fixed accessed attachment user status setting
Bug#GWAV-1451 - Fix errors in setup script caused by IE page caching
Bug#GWAV-1454 - Fix setup script not completing caused by IE page caching
Bug#GWAV-1455 - Fix text containment during setup process in IE
Bug#GWAV-1447 - Add setting for defining smtp response when gwava scan engines are unresponsive.
Defaults to 4xx response
Fix gwvrelay issue stalling when mail from is empty and no original SMTP protocol line was available
Add system alerts
Add system notifications
Add licensing management code
Add helper function to get notification default template id and language
Fix alert system reporting wrong module id
Add collapsing sections to system alert page
Add alert system test
Documentation additions
Add custom ssl session capability to network socket class
Fix IP address filters not saving properly
Bug#GWAV-1459 - Add CDIR notation support for IP address filter, IP exceptions, SMTP interface IP rejection and relay sources
Bug#GWAV-1463 - QMS remote upload detects SSL requirement and switches accordingly
Fixed GWAV-1402 Message sender was not being used as sender for release instead it was QMS module contact email address.
(Fixed query in ReleaseProcessor.cpp)
Fixed problem with global digest
Change purge to perform purges in batches if there is a backlog of purge records
Fixed crash in purge processing where StorageDirectory had not be set but was being used
Fixed release so it only sends to current owners.
GWAVA 7 start script
Fixed a problem with reading and processing Ou properties when a user logged in.

Bug#GWAV-1466 - Fix clone/move operations not working on newly saved objects
Bug#GWAV-1337 - Updated admin landing page to reference www.gwava.com for help
Bug#GWAV-1469 - Fix bug introduced causing double 5xx smtp errors when message is blocked
Add license installation and management page
Fix for custom digests in multiple OU environments
Updated datatables.min.css to utilize the sort arrow icons in the images subfolder
Fixed problem when there were no messages to display in the datatable
Digest will report all quarantined items
Updated database schema to support license system
Revision: 107 - created 30-Aug-2016
Bug#GWAV-1400 - Fix UI sourced data encryption not functioning correctly
Bug#GWAV-1404 Add rolling log retention time
Changes to Forward code.
(Change isn't complete until additional change to QMS module is completed)
User list was using the admin's organizational unit select
White and Black list were not displaying properly for a non-admin user
Bug#GWAV-1415 - Set IP reputation host to default value in UI if it has not been configured
Bug#GWAV-1413 - QMS white list link created during policy creation wizard
Bug#GWAV-1405 - Default RBL servers added to new RBL nodes when edited
Bug#GWAV-1406 - Altered RBL instructions
Add demo license key system
Gwava 7 look update to release from digest email page
Gwava 7 look update
Bug GWAV-1416 fix
Problem when single user was selected for digest release
Fixed exception due to logging
Fixes to qms forward message processor
Minor fix to digest template
fix to close the forward message dialog
Fixes to the message forward process
Add attachment number column to message properties
Added forward as attachment (from quarantine) template and language support
Fixes to the forward from quarantine process
The php template for the forward as attachment from quarantine process
Refresh of digest template
Add logging of client connection trust status to SMTP client connections
Remove unused 3rd party web components
Add section checkbox toggles for OU lists
Add functionality to rolling log to set expiration time
Fix startup crash caused by new logging code
Bug#GWAV-1425 - Correct case of 'QMS Module Manager' menu item
Bug#GWAV-1426 - Fix policy wizard erroring when policies already exist
Bug#GWAV-1388 - Add diagnostics section to SMTP interface settings and add option to force the peer IP address to a defined value
Changes to digest template selector and preferred digest language selector
Changes to forward as attachment template selector and preferred forward as attachment language selector
Added more detailed logging to Purge and Release processes

Bug#GWAV-1217 - Fix missing help button on attachment name node
Added code to refresh/reload the user settings in the session after configuration changes have been saved
Modified the message list to limit the toggle check box to only the current page.
Add contact email property to user accounts for notification purposes
Bug#GWAV-1438 - Fix default action of IP reputation connection drop not matching UI
Bug#GWAV-1438 - Add additional logging to IP reputation service in SMTP interface
Add new right to allow/disallow the ability to view or download attachments
Set the default value in the interface to false for the the Access attachments right.
Bug#GWAV-1432 - Add additional logging to LDAP sessions.
Alter response to 4xx fault when LDAP can't validate recipient address
Bug#GWAV-1230 - Add missing SPF node editor files
Bug#GWAV-1430 - Fix php error when user logs in over non-ssl link
CTIPD update to v4.00.0035.5
Spam Engine update to 8.00.0122
AV Engine Update to 5.4.25-r1
Clear the selection status message on delete
Added select all entries on page and selection status to while list and black list tables
Bug#GWAV-1390 - Warning icons are removed from menu when page is selected
Bug#GWAV-1429 - Add separate bind address option for scan engines
Fix login page border inconsistency in IE
License system back end code added
Add support for stl strings to XML parse helper functions
Set default bind address to IP servers to 0.0.0.0
Bug#GWAV-1419 - OU clone updated to create links between interfaces and roles
Fixed minor logging problem in RBL scan
Bug#GWAV-1419 - Prevent self provision with email address when domain is already provisioned
Add skinned pages for self provisioning services
Bug#GWAV-1412 - Redirect to QMS on local server now maintains original host
Removed unlink right checkbox
Fixed delete as user to just mean remove ownership
Added message status column to main QMS browse/search table
Modified data loading queries to get QMS message status information for display
Modified schema to add message status columns to message_core table
Added trigger functions to update message_core status information
Added deletion constraint to message_status table
Added unique constraint to messages status table
Added owner count information for message status to QMS insert query
Change Release processing.
Release only sends the message to the message recipients it does not remove message from quarantine
Added error code and default user name to login when the client timeout has occurred
Added status updated when attachment is accessed
Forced data reload after whitelist,blacklist,forward,release,delete,unlink operations so that status column shows updated status
Switched to color status icons
Added "My User Interface Section" to options page
Revision: 86 - created 04-Aug-2016

GWAVA 7 Install script update
Added Write permission to the slave_in_queue and slave_out_queue
Added additional logging to the QMS remote upload process.
Added more configuration options to the digest page
Added code to get new settings from the digest administration page
Implement new SSL management class
Add interface-engine priority influence system
Fix available user interfaces not being applied to cloned OU's
Add login auditing
Add logged in user details
Add SMTP interface IP address denial
Add SSL manager class
Removal of status of non-running programs
Bug#GWAV-1355 - Fix SMTP interface attempting to authenticate when username is empty
Add Ould to the QMS directive file
Add under construction license page
Add clone interface option to SMTP interface page
Add alert icon to QMS module page when database connections will be disconnected
Add internal direction to policy wizard when internal is selected
Add logging of path to QMS queue files
General aesthetics tidy up of gwava management UI
Add gwava logging of meta data of interest that is sent from interfaces
Added last login information for display in UI
Font family change for last login display
Added last login information
Added OU selection support for Admin user
Bug#GWAV-1358 - QMS role not assigned correct file system rights during install fixed
Bug#GWAV-1357 - Update user provisioning system to use correct smtp authentication mechanisms
Update management pages to display instruction pages as they become available
Bug#GWAV-1374 - Add online update check at login and display notification icon in title bar
Replace in-place editor used for node and accordion title editing
Remove redundant stats column
Enhanced tooltip on Postgres info icon
Added reload schedule notification and handler
Move most qms/digest properties to OU properties
Added more changes for the OU selector in the QMS UI
Update login process with wide range of error code reporting
Make user self-provisioning system aware of domain patterns
Bug# 1381 - Fix crash when TLS negotiation fails
Bug# 1356 - Fix SSL not enabled by default in gwvsmtp
Add system log download to server management page
Bug#GWAV-1277 - Tidy up manage servers XML info
Bug#GWAV-1382 - Emit email address info in address exception handler
GWAVA7 Script Updates
Reduce the default postgres connection pool count to 8 from 16
Add application names to postgres connections to allow for easy identification of gwava module connections from Postgres admin tools

Add missing update check page
Rework provisioning authentication system to honour all advertised AUTH types secure and insecure
Fix SMTP provisioning not working after previous adjustments
Bug#GWAV-1378 - Add support for SysLog logging
Bug#GWAV-1379 - Add logging to AV/Spam engine
Bug#GWAV-1380 - Add logging to RBL engine
Bug#GWAV-1374 Add missing online update report page
More granular error codes exposed during login when login fails
Add missing PHP LDAP prerequisite
Update user provisioning to support all advertised authentication options in auto mode
More changes required to support options/settings moving from QMS database to Organizational Unit properties database.
Hide Managed Addresses option
Hide Primary and Secondary Address report
Change format of custom address lists properties from comma delimited to XML
Fixed bug when list entry from custom address list was removed.
Bug#GWAV-1387 - Fix 404 error on navigation panel image request
Bug#GWAV-1386 - Remove references to old js files
Alter upsert queries to use more efficient syntax
Fix RBL logging alignment
Add user login information to admin UI
Add user account disabling to admin UI
Add admin controllable authentication method for users
Implement password expiration for provisioned users
Adjust UI pages to cope with multiple inclusions
Add forced SSL redirection option to login system
Bug#GWAV-1400 - Passwords for SSL passphrase are now encrypted
Put beta label back on title
Updated login page
Latest changes and fixes to QMS user interface
Fixed the quarantine message culling process (supports message storage distributed by organizational unit id)
Minor change, updated the gwava logo to the new gwava 7 look.
Alter DES encryption algorithm to generate matching encrypted data to the PHP mcrypt function
Revision: 49 - created 27-Jun-2016
Script to set the timezone for the server
During authenticate user we will check for a whitelist or blacklist for the user's organizational unit
Added whitelist support
Added blacklist support
GWAVA 7 script updates
Appliance Scripts
gwava7 script type for ctibd.bin
Updated spamip configuration port to 4931
Set permissions on QMS module root path
Set group and permission on storage path
Set group and permission on cache path
Added change group at startup to slave_in_queue path.
Files for previous patches

Bug#GWAV-1339 - Add pop-up text to search toggle bar in QMS
Bug#GWAV-1320 - Fix saving of carbon copy address list property
Fix name of carbon copy node help file
Add ctcpd control in OS scripts
Enable message release from the Qms UI.
Modified the release process to handle UI release from QMS
Add QmsWhiteListLink and QmsBlackListLink tables
Add NoAppLaunch recognition into module auto-restart system
Add qms link configuration to black and white list nodes
Fix OU reload not working when policies are modified
On startup the InQueueManager will write permissions (755) on the message storage directories.
We will also set these permissions on newly message created storage directories.
This is necessary so that the Qms web UI can read the mime files to display information to the user.
Added nohup to the command to start gwavaman.
Without it the gwavaman process was being killed when the script completed execution.
Added stored procedures to Add entries to the Black and White Lists.
Added the digest template
Removed the sleep at then end of the script.
trying nohup on start of gwavaman
Still trying to see any errors.
Gwavaman still doesn't seem to start properly.
More slight DEBIAN_FRONTEND change
added sudo to setting of DEBIAN_FRONTEND
Added DEBIAN_FRONTEND setting
Added sleep before trying to start gwavaman
Added header display tab for qms administrators
Policy setup wizard added
Add appliance control scripts
Add appliance install script
Add default RBL server to server install wizard
Fix duplicate RBL server config which had already been configured
Modify the default RBL list installed by the setup wizard to include sbl-xbl.spamhaus.org and
bl.spamcop.net
Add signature service
Add message body footer writer, which supports signature service
Bug#GWAV-1318 - Altered log line to distinguish it better
Remove Submit Spam and Ham Icons and Rights
Fixed where tools tab was still displayed for standard qms user
Add auto-populate user field on login page for digest directed login
Add basic OU stats
Add beta logo image
Denial of service added to SMTP interface
Add on-demand creation of stats databases
Update MIME message class for use with Signature Service
Add missing source object to linux make file
Update online update system to revert all files prior to switch to cope with file modifications
Add missing constraint to black/white list tables

Blacklist event now fully implemented
Fix module start button not working correctly
Add module auto-recovery
Enable/disable log at server level now updates active modules
Add server targeting for DB notification system
Fixed some memory leaks in BuildInsertQuery.cpp.
Digest will now be sent even if the message was not blocked.
If an item is in the Quarantine then it should be included in the digest regardless of block state.
Add a couple tables (message_cache, attachment_cache) to qms database.
Update to qms UI, add a few things to the qms management page and post install.
First docs.
GWAV-1201
Add base scripts for policy creation wizard
Update all roles to include the correct interfaces
Add missing constraint to database property table
Add optional online update stream source file
Tidy up server config page with collapsible sections
Add LDAP support
Add misconfiguration indicators to UI
Update initial install script to complete startup configuration
Add unique message process id to log
Add NOOP thread for SMTP during scan process
Add stub service for Signatures
Implement node level decompression
Add clone and move options to policy page
Modify startup code to wait for database to be ready
Add menu item for licensing page
Update role ui access for policy based roles
Fix database connection password not being saved
Fix crash caused by db opener when null data exists
QMS remote upload support added
Update qms remote upload script to return error status if rights are incorrectly defined
Add priority ordered service firing to accommodate block state being available to QMS
Fix event id being recorded from instance id causing qms to emit the wrong event
Implement blended admin and regular quarantine services
Fix gwava crash when binary is mismatched with database schema
Add exception handler during AV signature merge
Removal of QMS digest database creation script
Rename ip address UI components to match their new filter name designation
Default digest template
Add IP reputation button image
Add generic notification template
Update notification templates to extract sender domain for the message id
Admin UI fixes for node editor positioning of nodes and connector lines when workbench is scrolled
Replace forgot password with login help button in login page when self provisioning is not enabled
Icons added to properly reflect service padlock states
Add template installation system

Add text filter exceptions
Add ZM signature to EXE fingerprint
Report exception types loaded with policies
Updated DB install script
Preparatory code for domain pattern matching system
Change description of executable fingerprint to reference all file types caught
Add UI support for domain pattern matches
Add UI support for policy level decompression settings
Add admin email address field to UI for OU
Add libarchive to gwava project
Add exception while list class
Expose the system root folder to the admin UI
Add system root path to DB and add this to server management UI page
Exception loader function refactored to accommodate Whitelist loading
Domain pattern matches added
Add path defaults for gwvrelay and qms ui
Add more complex sample message to scan diagnostics
Added Image Analyzer process
Implement gwvrelay relative path setup
Add icon for smtp envelope exception
Changed QMS in_queue path to support QMS module root path instead
Add IP reputation node page to admin ui
Fixes for QMS digest and release processes
Merge domain lookup into domain pattern matches
Add LibArchive type to file container extractor
Fix libarchive locking up if given empty filename
Add regex bounding to ends optionally with ^ and \$
Revision: 21 - created 10-May-2016
Fix start and restart all module control buttons on module status control page
Update user management page with new role selection system
Add button image for admin quarantine
Replace admin UI twin list boxes with checkbox lists
Fix module status page restart button sending unloadmodule command
Fix module start button not sending correct command
Send configuration reload to gwvrelay when module settings are altered
Fix gwvrelay path case issue causing non-delivery on linux
Fix gwvrelay message test button being setup multiple times
Add header tag service
Update server install script to set default relay target setting
Add initial template management pages
Add tables to support black/white list components
Fix new templates not saving
Tag header services UI fixes
Notify service added
Locale aware template system added
Add predefined sample message to scan diagnostics page
Add image analyzer edit node

Add skeleton components for blacklist and whitelist
Add language system
Add edit box for user interface redirect button in user interface management page
Update templates page to be language aware
Fix ssl cert configuration to work without certificates
Add header line replacement functionality to MIME message class
Removed the use of SPF records, now only TXT records will be searched for SPF information (per RFC 7208)
Updated database build script
Add user and ou move functionality to UI
Add DSN template selection for smtp interface
Finished functionality in blacklist UI node
Add stub object and UI node for image analyzer
Implement container extraction in fingerprint and attachment name events
Updated DB setup script
Move message direction event into received node
Service locking implemented
Partial address blocking implemented at SMTP interface
Updated template folder structure and added readme for using custom templates
Fix for black/whitelist using incorrect objects in database
Add whitelist node editor
Fix service merge functionality which was build incorrectly
Add initial notification template sources
Add decompression to fingerprint and attachment name events
Add new container extraction system including bz2 and zip format extraction
Add logging of ip address when CTIPD connection fails
Update reference in setup script for the correct Postgres requirement
Revision: 15 - created 23-Mar-2016
Updated sources.xml
CTIPD library file
Revision: 10 - created 23-Mar-2016
Linux spam library files
CTIPD updates.
Default config file for CTIPD
RBL implemented for policy level scan
Add scan diagnostic page
Replace XML based in put fields with easy to use UI
Fix REST response putting valid recipient addresses into attributes of a single element
New selection highlighting for scanner nodes
Fix servers on module status page grouping by name instead of id
Add RBL scanning of received header IP addresses
Add RBL scanning of received header IP addresses
Add icon for SPF event
Add message test for gwvrelay
Fix roles not displaying user interfaces correctly
Add message generator option to take precreated message as a string
User auto provisioning setup added to domains page

Self provisioning through login process implemented
Fix authentication switcher showing multiple buttons
Fix new user setup not working if user 'unnamed user' exists
Fix new user passwords not working
Revision: 5 - created 16-Mar-2016
GWAVA 7 Base system files
Revision: 1 - created 15-Mar-2016
Creation of GWAVA7 update repository

1 Micro Focus Secure Messaging Gateway



Overview

Micro Focus Secure Messaging Gateway provides inbound & outbound protection for your company's enterprise network & messaging system, including antivirus, anti-spam, cybercrime protection, DDOS protection, and porn blocking with built-in image analysis!

This solution uses the latest technology to ensure that your messaging system and network are free of viruses, malware, and spam. Micro Focus Secure Messaging Gateway also monitors network traffic to prevent pornographic images, and protects against cybercrime and DoS/DDoS attacks.

Micro Focus Secure Messaging Gateway protects business networks and communication data for thousands of organizations around the world in industries including government, education, financial services, healthcare, and business.

Micro Focus Secure Messaging Gateway provides the best zero-hour antivirus protection available for both inbound and outbound traffic. Viruses are stopped before an outbreak occurs, which saves you thousands of dollars in lost time and data.

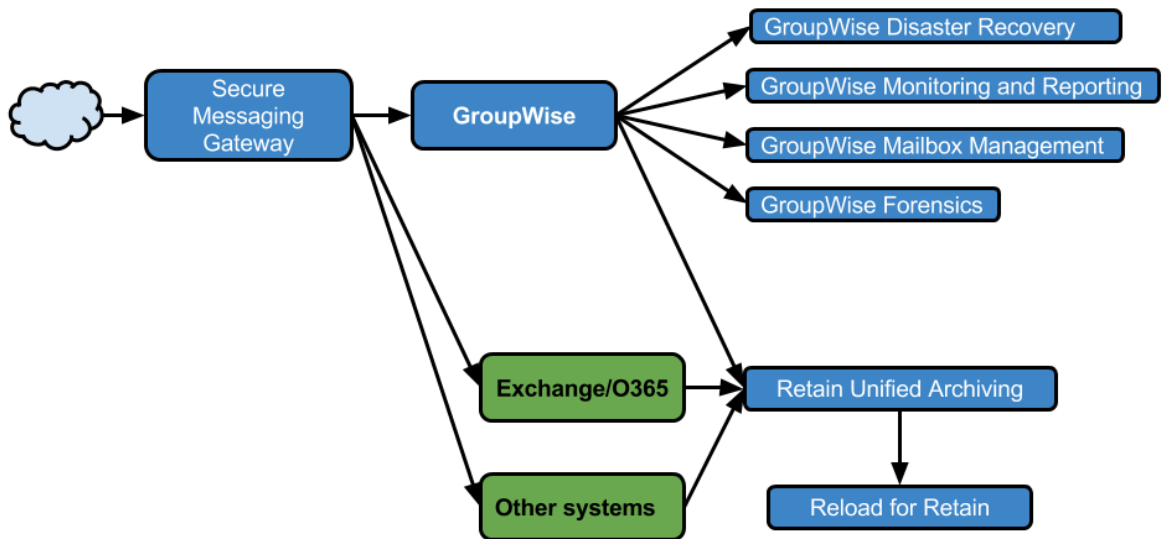
Micro Focus Secure Messaging Gateway provides multi-layer spam defense to protect email and keep unwanted traffic away from your collaboration system.

Micro Focus Secure Messaging Gateway actively monitors your network to protect it from cyber-crime, pornographic files, and DoS/DDoS attacks. Micro Focus Secure Messaging Gateway also provides internet traffic filtering and web content scanning to ensure that malicious websites and similar content cannot access your network.

Micro Focus GWAVA Family of Message Handling Products

- ♦ *Micro Focus Secure Messaging Gateway* is a message scanning product that protects your system from malware and spam.

- ♦ *Retain Unified Archiving* is an archive storage product that is designed to keep messages from GroupWise, Exchange/O365, GMail, BlackBerry, Bloomberg, Notes, mobile, social and other messaging platforms for the long term to meet data retention legal requirements and has powerful search capabilities for eDiscovery.
- ♦ *GroupWise Disaster Recovery powered by Reload for GroupWise* is a hot-backup and disaster recovery product for GroupWise. It keeps a few weeks of data and can easily restore messages, calendar items, address books, and even whole users. It can also act as a fully functional Post Office in times when the GroupWise POA is down.
- ♦ *Reload for Retain* is a backup solution for Retain. The Retain archive keeps items for the long term and often becomes the only repository of an item. Without a backup you can leave yourself open to legal liability if the items are lost before the retention period has passed. Reload for Retain provides high speed backups and can temporarily take over duties of the Retain server should an incident occur.
- ♦ *GroupWise Reporting & Monitoring powered by Redline* is a comprehensive, customizable, monitoring and reporting tool for GroupWise.
- ♦ *GroupWise Forensics powered by Reveal* provides essential auditing and oversight capabilities that legal, human resources, and auditing personnel need within GroupWise.
- ♦ *GroupWise Mailbox Management powered by Vertigo* is the Enterprise Mailbox Management tool for GroupWise.



2 Installation

System Requirements

Overview

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

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

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

System Requirements

Micro Focus Secure Messaging Gateway is supplied as an OVA template or ISO image and is supported by Hyper-V, VMare and VirtualBox. The virtual machine (VM) is pre-configured to provide the recommended settings:

1 CPU

2 GB Ram

60 GB disk space

Ports Used by Secure Messaging Gateway

During the installation process Secure Messaging Gateway downloads and installs updates to the Ubuntu operating system. Bypass any web filters and/or open the appropriate port(s) on the firewall that might prevent these downloads or the install process will fail.

The Secure Messaging Gateway is set behind a firewall the following powers should be open for mail flow and system functions or services:

Inbound and general traffic

25 – TCP Inbound (Used for Mail)

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

80 – TCP

443 – TCP

Outbound traffic

53 – UDP Outbound (DNS Lookup)

80 – TCP Outbound (Updates services for Antivirus, Signature Engine, and GWAVA system.)

123 – TCP Outbound (Network Time Protocol (NTP))

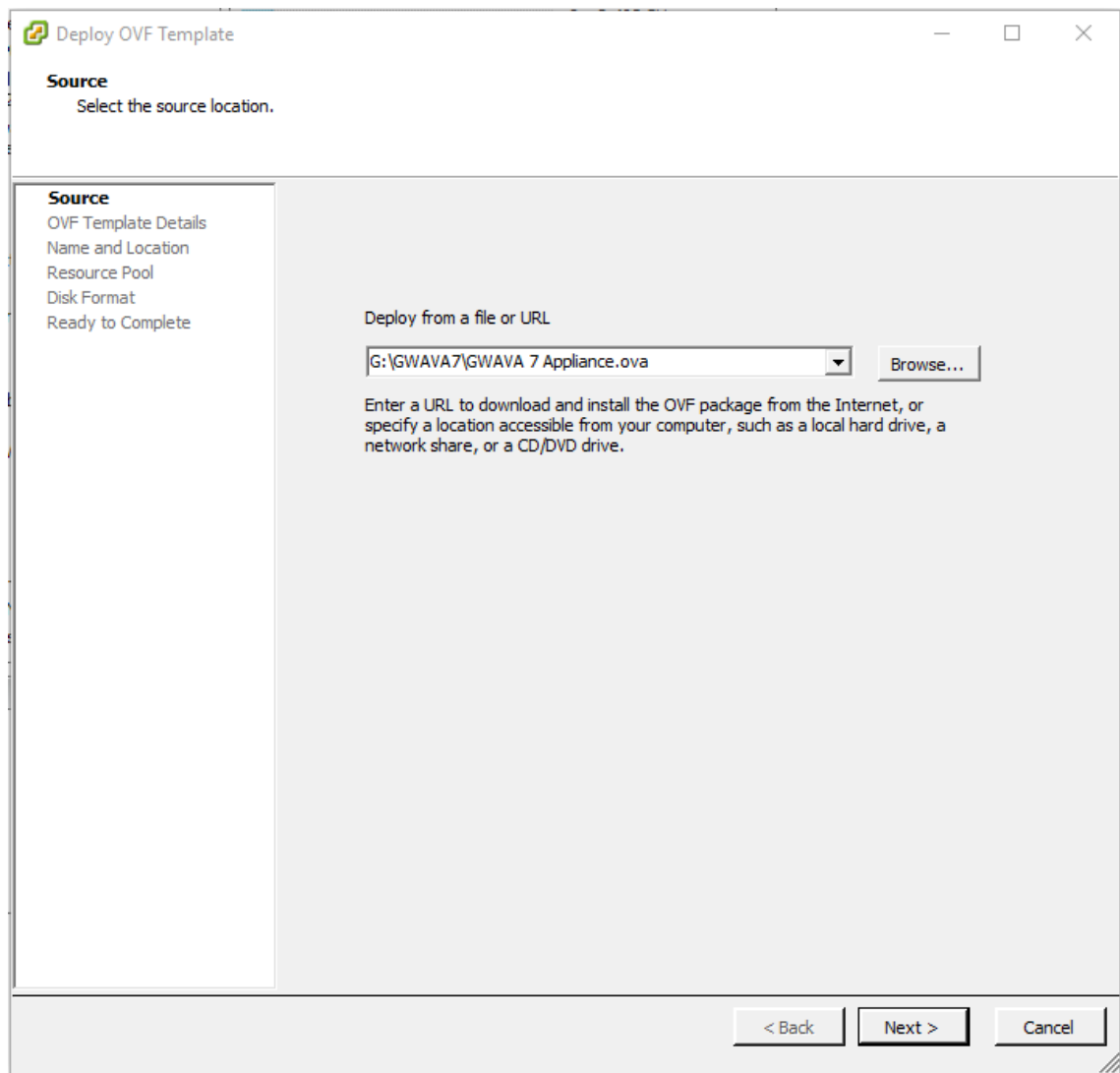
OVA Installation

Server Deployment Setup and installation settings are similar across all supported systems. Installation in VMware is shown below.

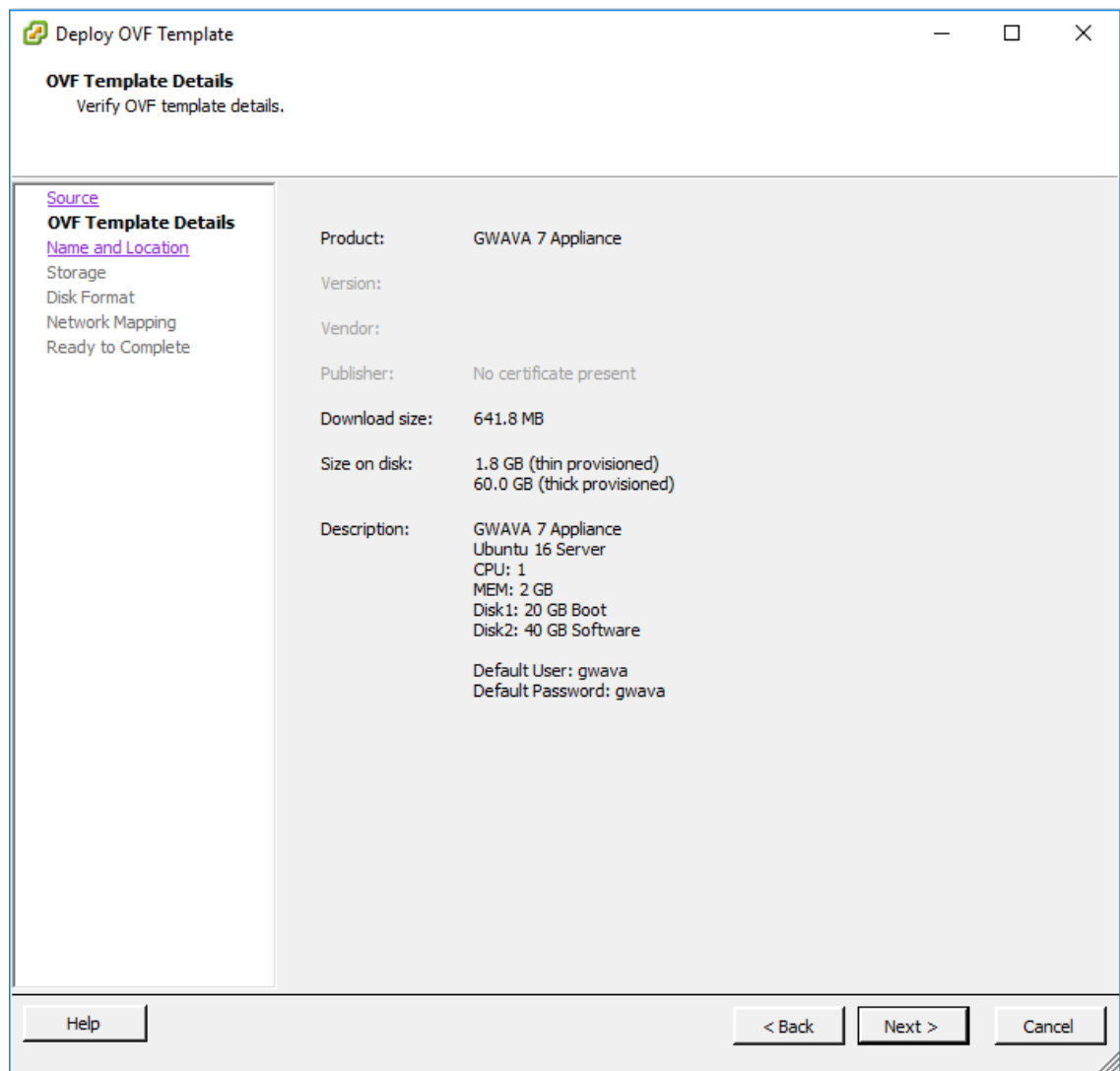
OVA Deployment

Download OVA file and deploy the OVA template in the VM system.

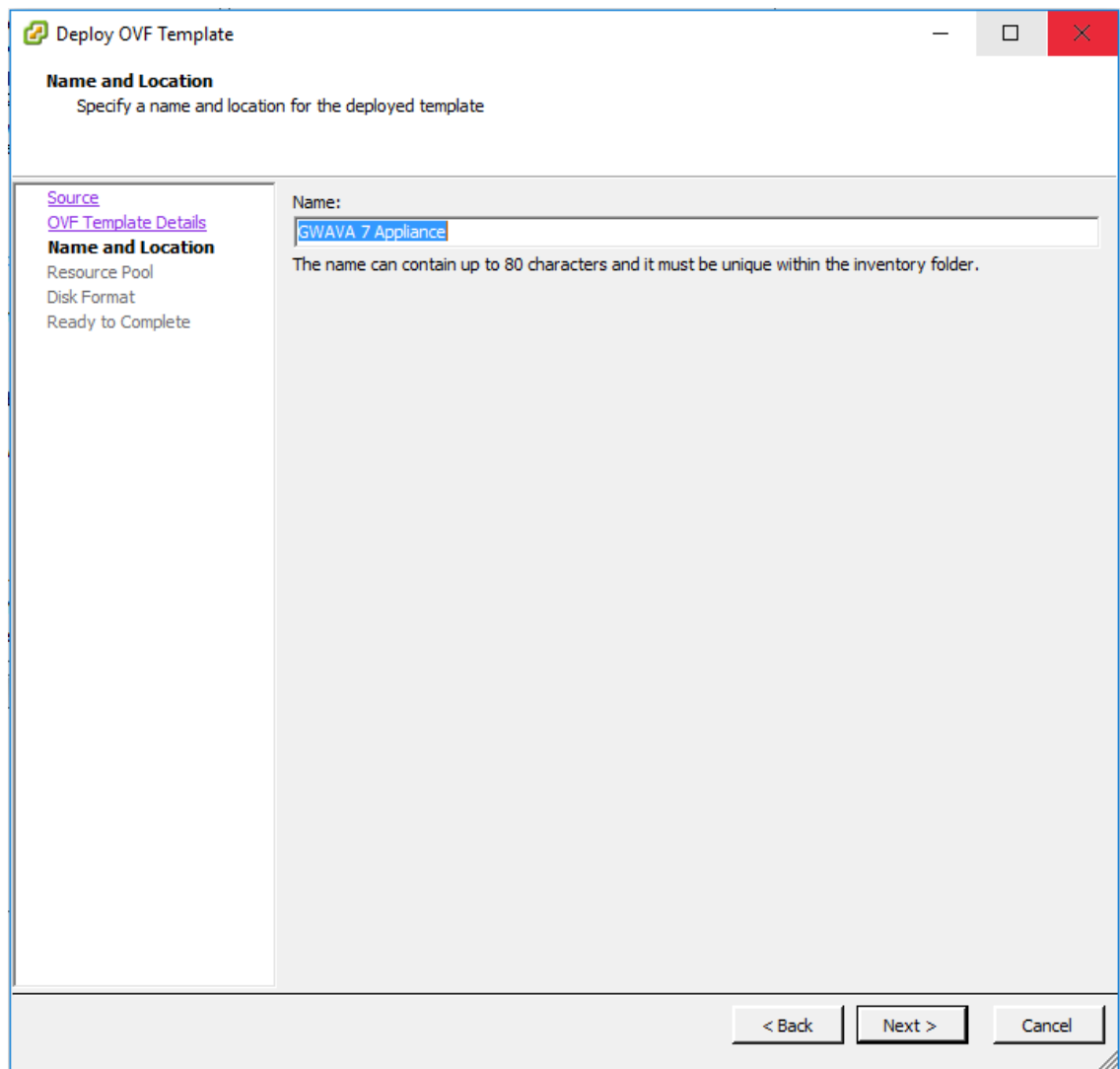
1. In the virtual server, open the virtual machine deployment wizard and browse to where the Secure Messaging Gateway .ova file has been saved to select it.



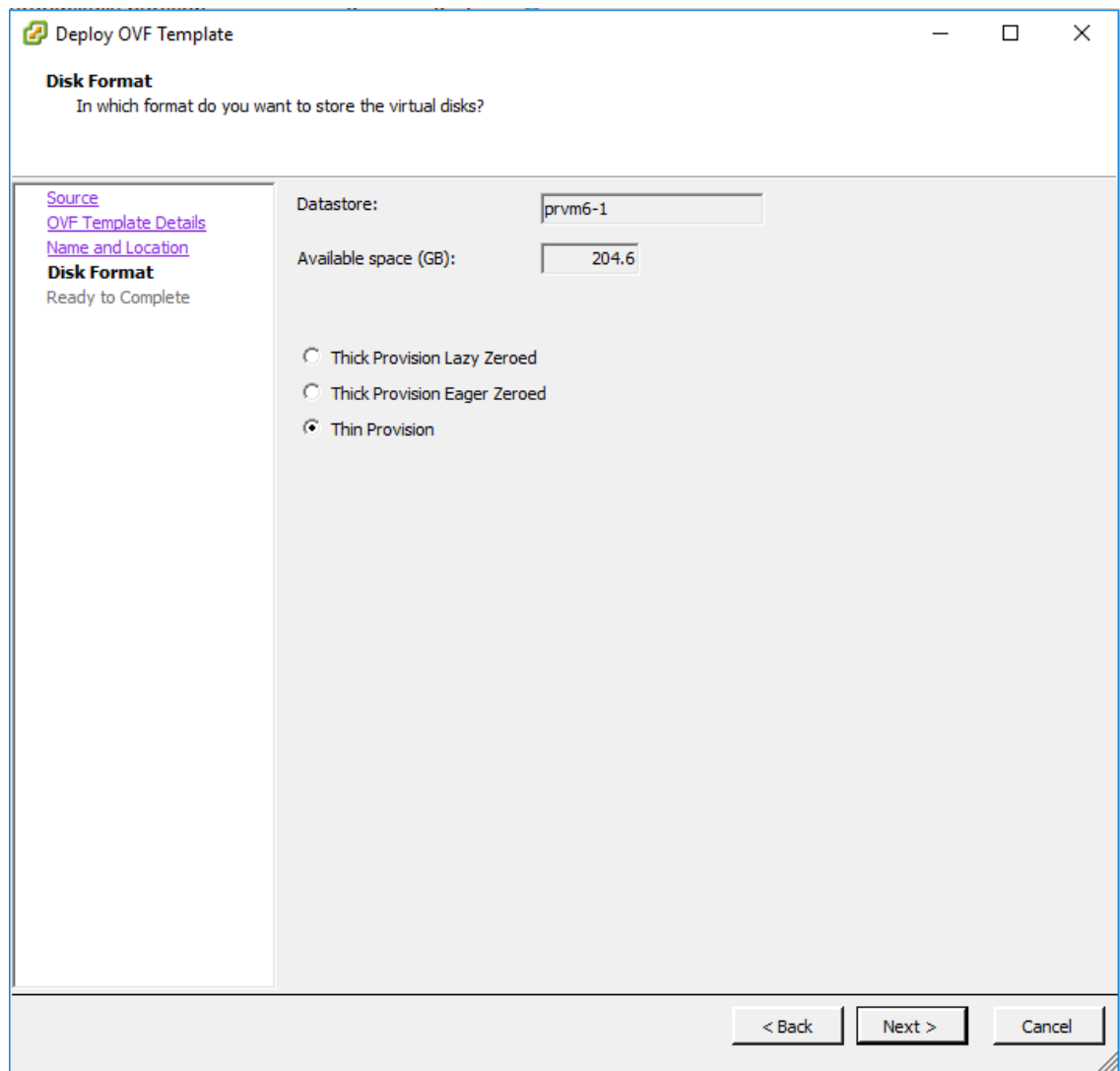
2. Template Details are displayed. These are the requirements of the system and are not changeable here. Ensure that the host system has plenty of space and power to handle these requirements.



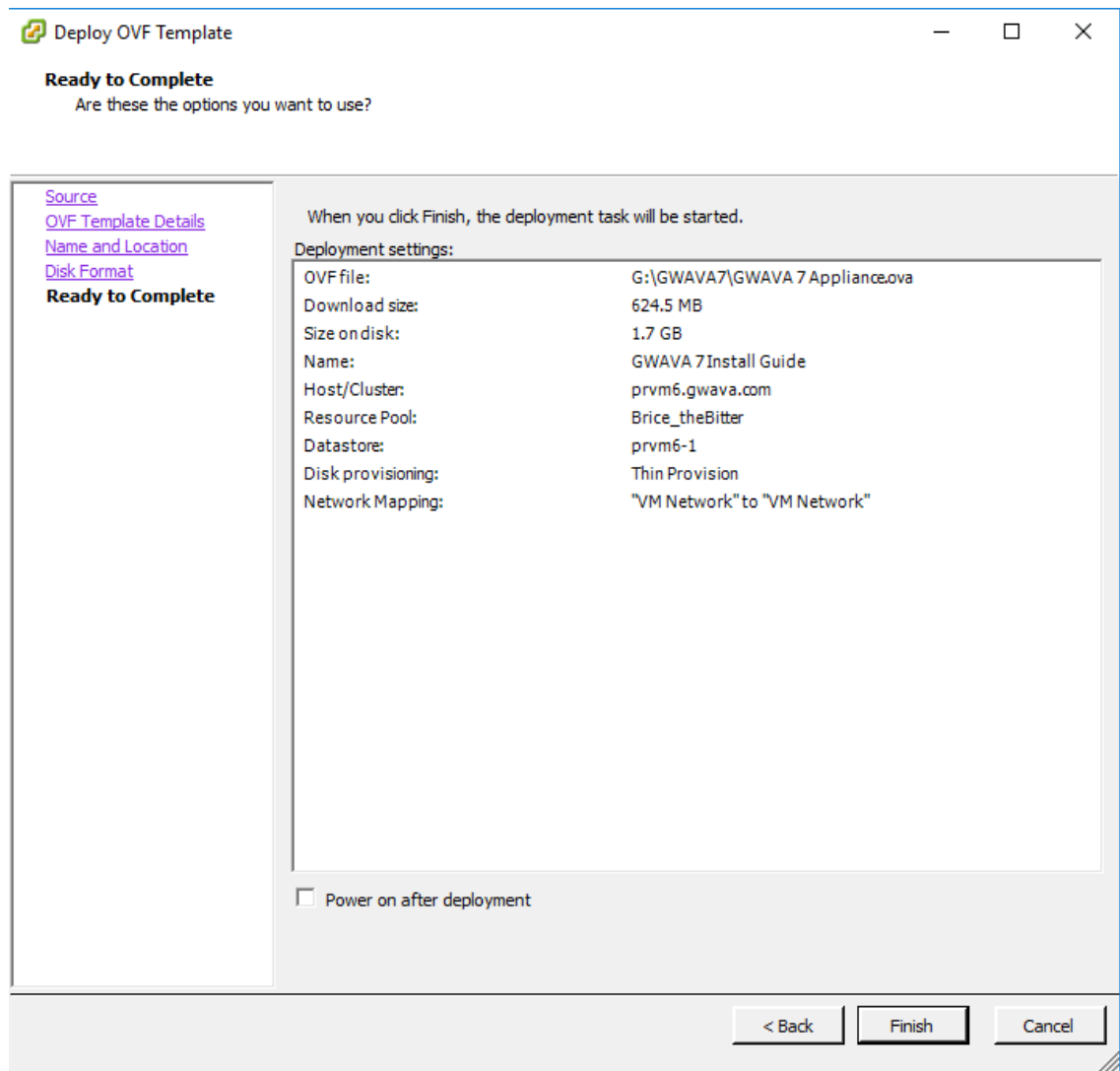
3. Give the VM a name. This can be any name suitable for the system. There is no requirement for any specific name, but it is useful to create one which is easily recognizable as the Secure Messaging Gateway 7 system.



4. If possible, select the Resource Pool for the Appliance.
5. Select the desired disk format. The recommended setting is shown. Remember that the required space is only 60 GB.



6. The settings for deployment are displayed for confirmation. Make sure that the settings are correct and then select 'Finish' to perform the deployment.



7. If desired, check the box to power on after deployment
8. Once powered on, connect to the new Secure Messaging Gateway VM.

Secure Messaging Gateway Installation

Once the VM has been deployed, the Secure Messaging Gateway software must be installed.

1. If not already running, start the machine. Open the machine console and log in. Default credentials to log in with will be displayed.
2. After logging in, you will be prompted to run the pre-install script. Issue the following command:

```
sudo /opt/gwavapreinstall.sh
```

```
Ubuntu 16.04 LTS gwava tty1

gwava login: gwava
Password:
Last login: Mon Jul 24 12:04:57 MDT 2017 from 137.65.64.201 on pts/0
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

132 packages can be updated.
31 updates are security updates.

#####

Please run the following command:

sudo /opt/gwavapreinstall.sh

#####

gwava@gwava:~$ sudo /opt/gwavapreinstall.sh
```

3. The EULA will be displayed. Enter 1 to accept.

```
RE ABOUT TO DOWNLOAD.

BEFORE CLICKING THE "ACCEPT" BUTTON OR USING THE SOFTWARE, PLEASE READ THE FOREGOING TERMS AND CONDI
TIONS CAREFULLY. BY CLICKING ACCEPT, YOU WILL BE DEEMED, FOR ALL LEGAL PURPOSES, TO HAVE READ, UNDER
STOOD AND ACCEPTED, UNCONDITIONALLY AND WITHOUT QUALIFICATION, THE TERMS SET OUT HEREIN AND YOU WILL
BE SIGNIFYING YOUR LAWFUL AND BINDING CONSENT TO BE BOUND THEREBY.

CLICKING ON ACCEPT AND/OR THE USE OF THE SOFTWARE WILL COMPLETE AND THEREAFTER CONSTITUTE A LEGAL C
ONTRACT, BETWEEN YOURSELF AND Micro Focus THAT SHALL, FOR ALL LEGAL PURPOSES, BE GOVERNED BY THE TER
MS AND CONDITIONS AS HEREINAFTER SET OUT.

IF, FOR ANY REASON, YOU DO NOT AGREE WITH ANY OF THE TERMS HEREIN OR DO NOT WISH TO BE BOUND BY THEM
, YOU MAY CLICK THE BUTTON DISPLAYING THE "NO" ELECTION AND IT IS UNDERSTOOD THAT NO CONTRACTUAL REL
ATIONSHIP WILL BE CREATED AND YOU WILL NOT ACQUIRE THE RIGHT TO DOWNLOAD OR USE THIS SOFTWARE.

1. Definitions
Where used in the present Agreement the following terms shall have the meaning as hereinafter set ou
t:

"Agreement" when used herein shall mean the EULA entered into between yourself and Micro Focus gover
ning the issuance to You of a license to use Micro Focus software

"Software" when used herein shall mean computer software and/or computer code and/or associated medi
a and/or printed materials and/or, where applicable, 'online' and/or electronic documentation

"Maintenance" when used herein shall mean technical support in conjunction with upgrade protection (
the modification of the software after delivery to correct faults, improve performance or add functi
onality or other attributes).

"Subscription" when used herein shall mean the usage of a term license in conjunction with technical
support and upgrade protection (the modification of the software during the term to correct faults,

Choose one of these options:
1) You agree to this license agreement
2) You DO NOT agree to this license agreement
3) You want to re-read the license agreement
Choose (1-3):
```

This will start the Secure Messaging Gateway installation. The Secure Messaging Gateway installation starts with networking configuration.

4. The Secure Messaging Gateway server needs to know the network settings for the machine. Select the network interface to configure it.

```
Getting a list of all interfaces to configure networking
List of available interfaces:
1) ens160
Which Interface would you like to set? _
```

5. Set each setting for the system by inputting them in turn. When the settings are correct, input 'y' to continue.

```
Getting a list of all interfaces to configure networking
List of available interfaces:
1) ens160
Which Interface would you like to set? 1
SET_INTERFACE = ens160
Backing up existing interfaces file
IP address (example: 192.168.1.2): 151.155.183.156
Subnet Mask (example: 255.255.255.0): 255.255.255.0
Gateway (example: 192.168.1.1): 151.155.183.1
Primary DNS (example: 192.168.1.254): 137.65.247.1
Secondary DNS (example: 192.168.1.253): 207.171.3.65

Please verify that these values are correct:
IP address: 151.155.183.156
Subnet Mask: 255.255.255.0
Gateway: 151.155.183.1
Primary DNS: 137.65.247.1
Secondary DNS: 207.171.3.65

Finish setting up the server with these values? (y\n): y_
```

6. Set the hostname and domain for the server. When correct, press 'y' to continue when prompted.

```
What is the hostname for this machine (eg gwava?): sga157
What is the domain for this machine (eg gwava.com): doc.mf.net
Hostname: sga157
Domain: doc.mf.net
Finish setting up the server with these values? (y\n): y_
```

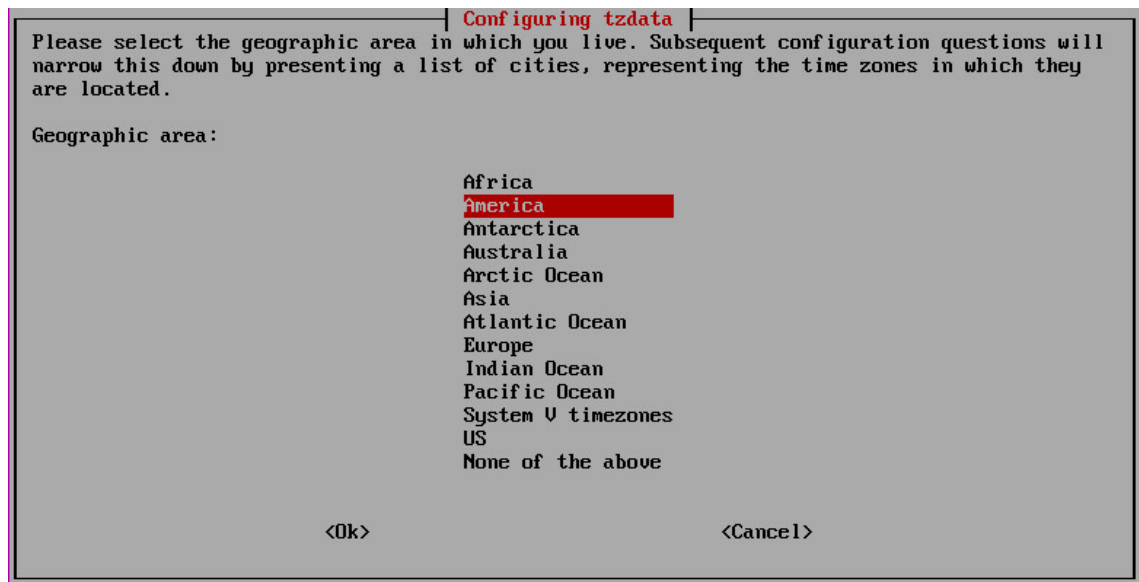
7. Set the Proxy settings. If a proxy is required input it into this section.

```
#####
Proxy Setup
#####
Does this server require a proxy server? (y\n): n_
```

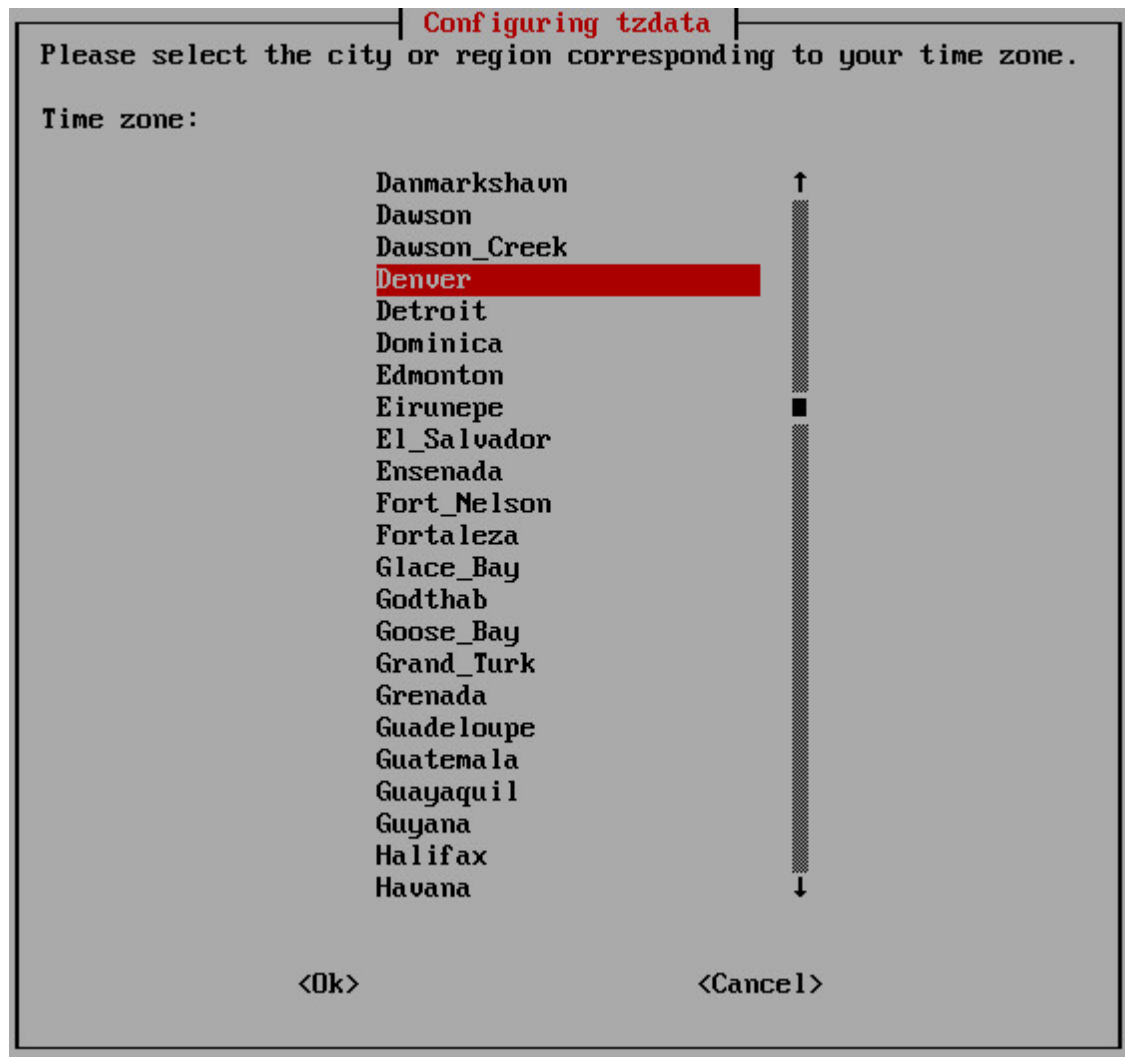
- 8. After setup, the network connection is tested.
- 9. Root user password creation. Do not forget this password. This is the root password for the appliance. This is not the user or password used in the administration console, that is configured later.

```
#####
Update Password for Linux User: gwava
#####
Enter new UNIX password: _
```

- 10. Select the geographical area for the Secure Messaging Gateway Server. This is used for the time zone.



- 11. Select your city, or the closest city to your location in your time zone.



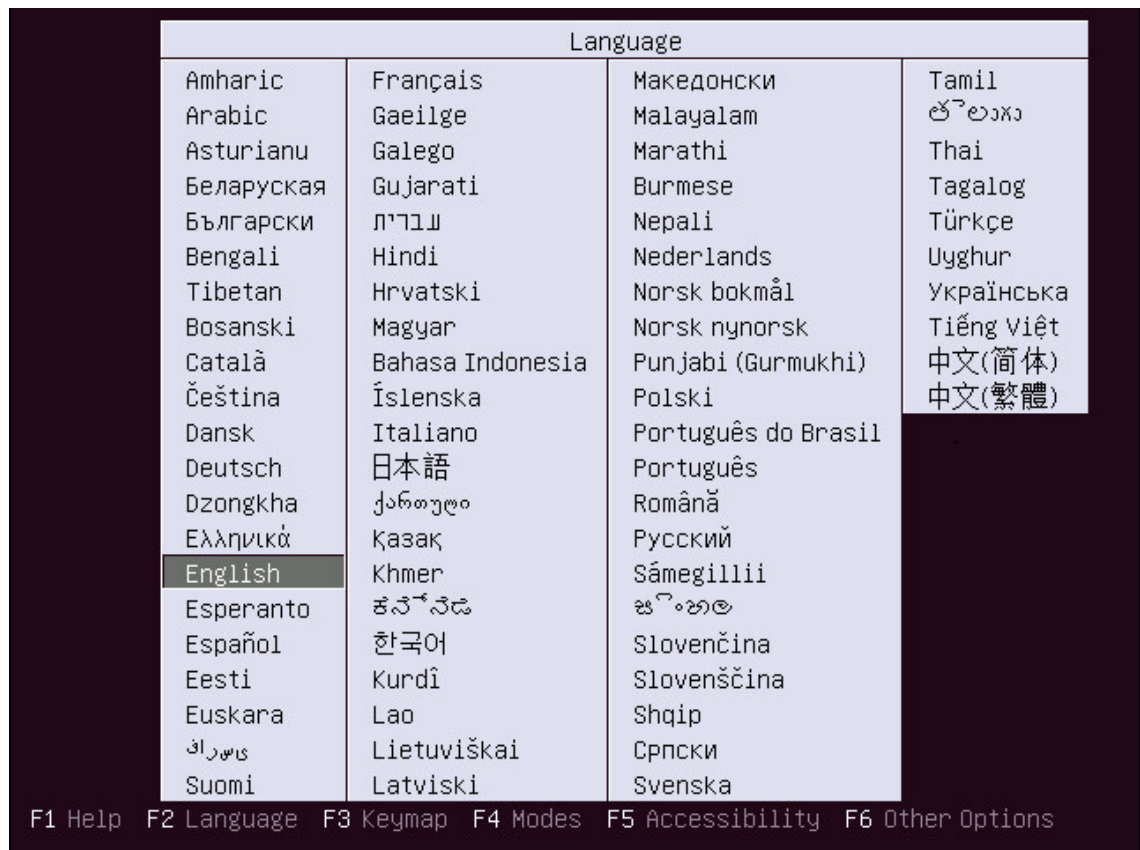
12. Once all the settings are complete, Secure Messaging Gateway will automatically download the latest security patches and then install the system.

Once installation is complete, the initialization and configuration of the Secure Messaging Gateway system is ready. To access the web console, open a browser and go to the hostname.domain specified in step 3, or use the IP address to connect to the server. The initialization will automatically be displayed.

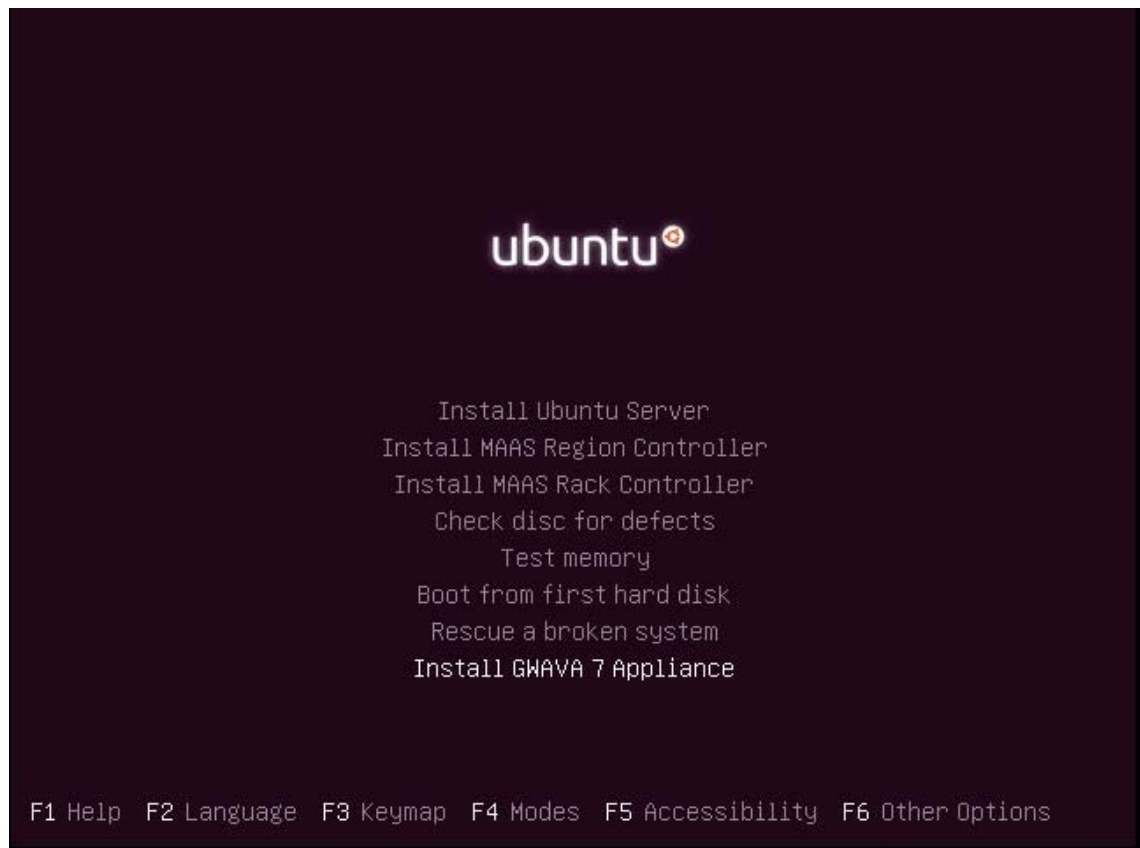
ISO Installation

Secure Messaging Gateway can be setup from an .ISO file.

1. Create an Ubuntu 16 LTS VM that meets the [system requirements \(System_Requirements.htm\)](#) and load the ISO.
2. Select the desired language



3. Select "Install Secure Messaging Gateway Appliance"



4. The keyboard layout needs to be specified. Either select the keyboard layout from a list or select auto-detect, which will ask you to press certain keys or ask if other keys are present.

The appliance will be installed, then the server can be [configured \(Post-Install_Tasks.htm\)](#).

Configuration

After installation is complete, there are a number of configuration tasks to complete.

Set up the domain, quarantine self-provisioning, authentication, policies, digests and inserting Secure Messaging Gateway into the system.

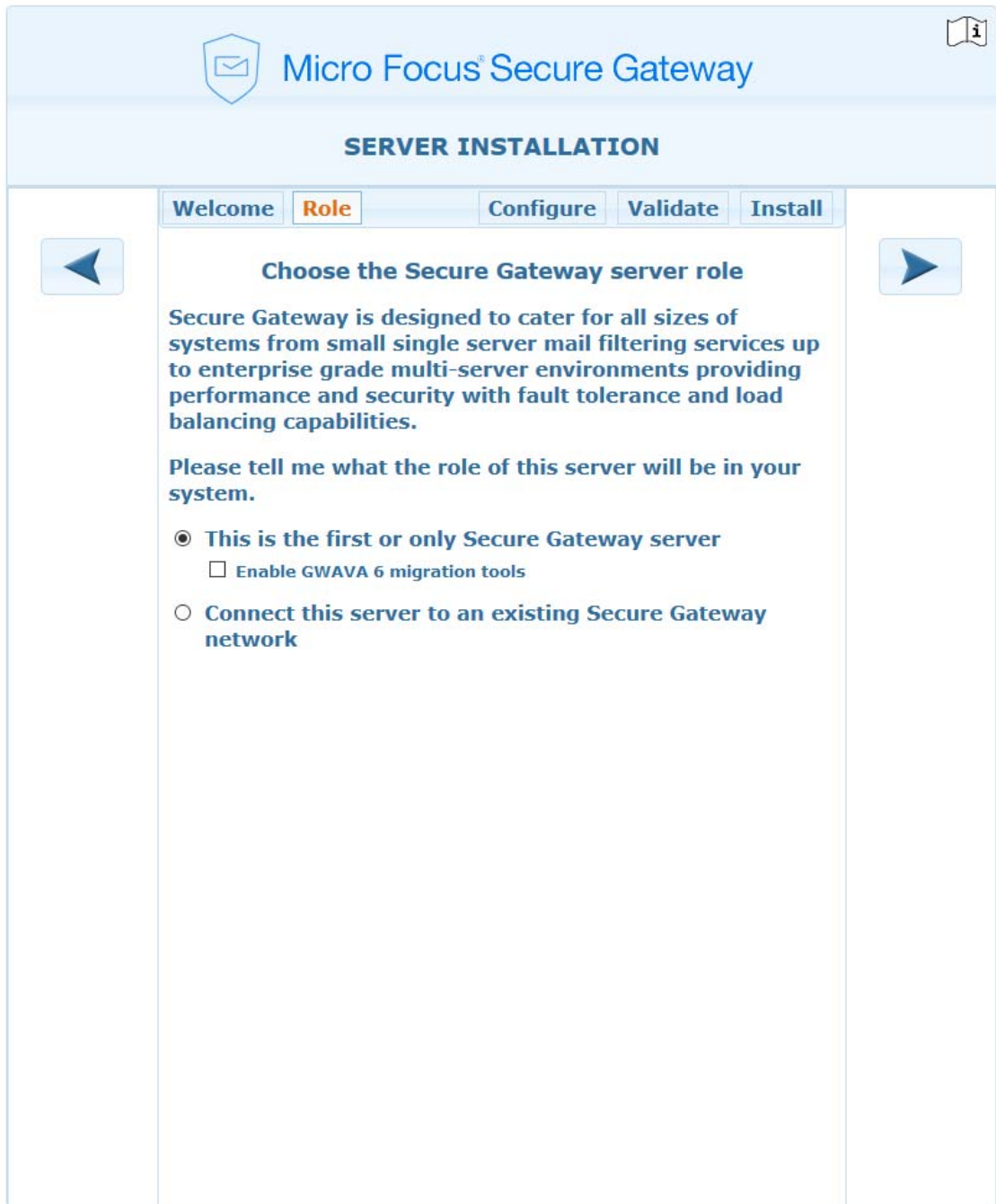
1. Browse to the Secure Messaging Gateway server hostname or IP Address. You will be welcomed by the server installer. Select the forward arrow on the right to go to the next page, or the back arrow on the left to return to the previous page.



2. Select the Role this Secure Messaging Gateway server will have.

If this is the first or only server and you have an existing GWAVA 6 system, you may migrate the GWAVA 6 settings with the [migration tools \(GWAVA_6_to_Secure_Gateway_Migration.htm\)](#).

If adding to an existing Secure Messaging Gateway network, see how to connect with an [existing network \(Installing_into_an_Existing_Secure_Gateway_Network.htm\)](#).



3. Configure the server.

Update the Server name and address.



Add a password for the admin user.

Enter the primary domain.

Enter a contact email, optional.

Enter the mail relay server hostname or IP address and credentials, if required.

Enable Setup default system.

 **Micro Focus® Secure Gateway** 


SERVER INSTALLATION

Welcome Role Configure Validate Install

Configure new Secure Gateway server

Provide all of the details in preparation for configuring your Secure Gateway server.

Server name	<input type="text" value="sg156.sf.gwava.net"/>
Connection address	<input type="text" value="151.155.183.156"/>
Description	<input type="text"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Re-type password	<input type="password" value="••••••••"/>
Primary domain	<input type="text" value="sf.gwava.net"/>
Contact email	<input type="text"/>
Mail relay server	<input type="text" value="151.155.183.142"/>
Mail relay username	<input type="text"/>
Mail relay password	<input type="password"/>
Setup default system	<input checked="" type="checkbox"/>

Postgres Database Configuration 

Config	Quarantine	Statistics	Tracker
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGateway"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="••••••••"/>		

Postgres Database Configuration

If using a external databases, they can be configured here.

Config

Postgres Database Configuration

Config	Quarantine	Statistics	Tracker
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGateway"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="●●●●●●"/>		

Quarantine

Postgres Database Configuration

Config	Quarantine	Statistics	Tracker
Create this database	<input checked="" type="checkbox"/>		
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGatewayQuarantine"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="●●●●●●"/>		

Statistics

Postgres Database Configuration

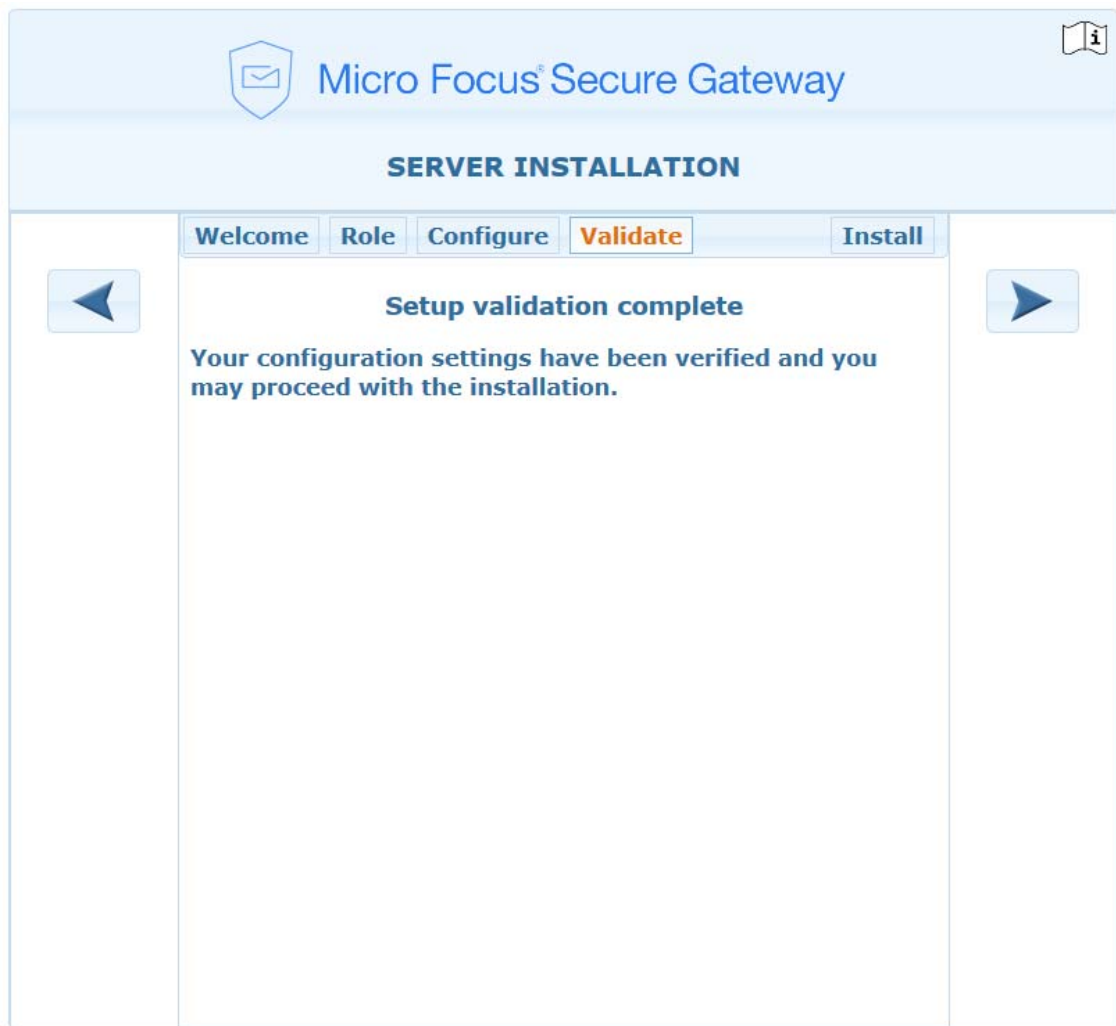
Config	Quarantine	Statistics	Tracker
Create this database	<input checked="" type="checkbox"/>		
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGatewayStats"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="●●●●●●"/>		

Tracker

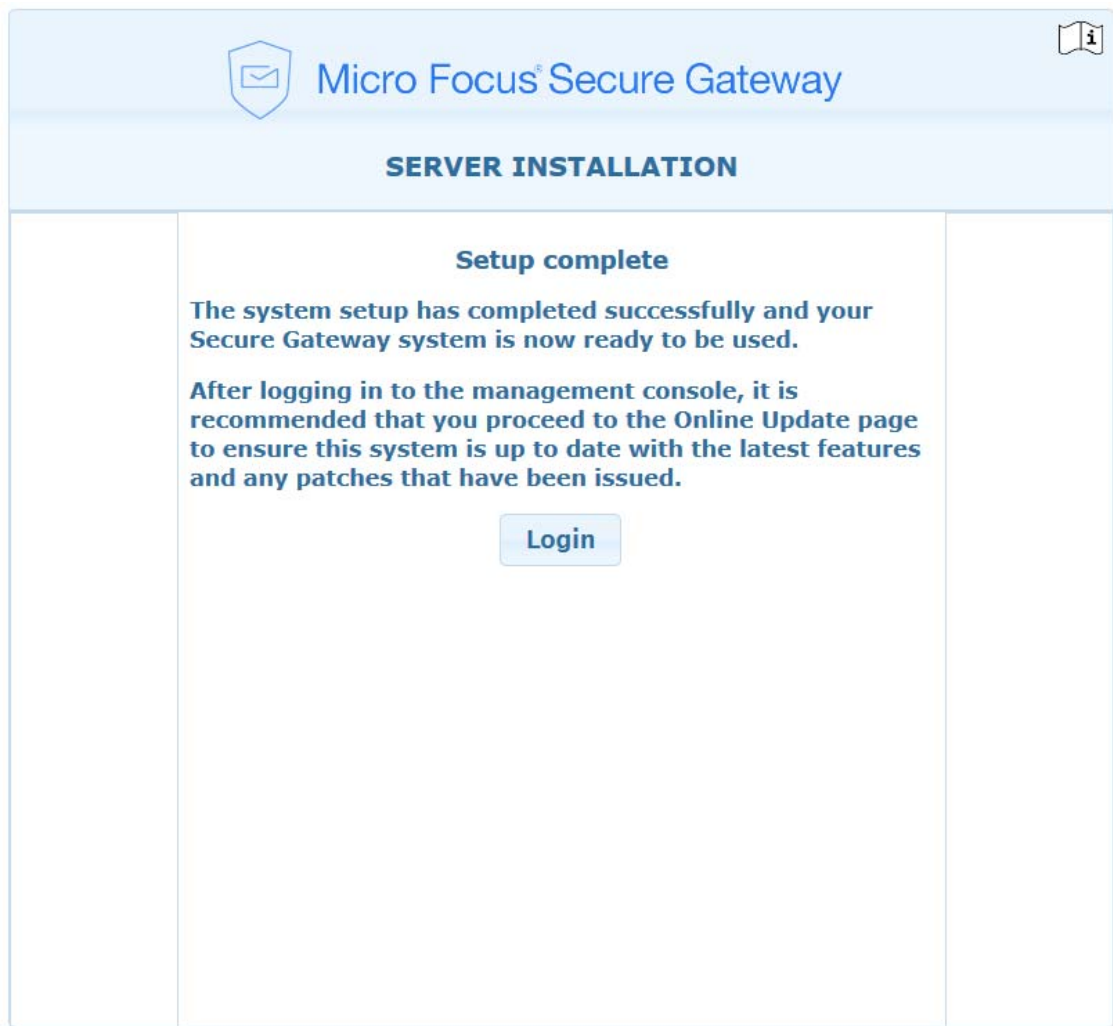
Postgres Database Configuration

Config	Quarantine	Statistics	Tracker
Create this database	<input checked="" type="checkbox"/>		
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGatewayTracker"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="●●●●●●"/>		

4. Validate. The installer will validate the entered settings.



5. Install. Selecting the forward arrow will install the Secure Messaging Gateway server. This may take a few minutes. When complete log in to configure the server with the post install tasks.



6. Log into the Secure Messaging Gateway Server.

Micro Focus® Secure Gateway

The screenshot shows the login page for the Micro Focus Secure Gateway. It features the Micro Focus logo (a shield with an envelope) on the left. To the right of the logo are two input fields: 'Login name' and 'Password'. Below these fields is a blue 'Login' button. In the bottom right corner of the login box, there is a link labeled 'Login help'.

Post-Install Tasks

Once Secure Messaging Gateway is configured, there are some post-install tasks that need to be completed to fully set up the system.

1. Adding the domain.
2. Create a policy.
3. Set up a digest .
4. Set Secure Messaging Gateway as the outbound SMTP server.
5. Add the new Secure Messaging Gateway server as a trusted relay.

On the Secure Messaging Gateway server

1. Set up your domain under *Organization/Policy Management | Domain Management*.
 - a. Add new.
 - b. Under *SMTP Hosts* enter the Target host of your email server.
 - c. Setup User Quarantine Self-Provisioning so that users can manage their own quarantine.
 - i. Select *Enable user auto-provisioning*
 - ii. Enable the Auto-provision roles *QMS User*
 - iii. If using GroupWise, enable *auto* Authentication so users can login into the QMS to manage their quarantines

The screenshot shows the 'Manage Domains' web interface. At the top, there are buttons for 'Add new', 'Delete selected', 'Instructions', and 'Move selected'. Below this, the domain 'doc.mf.net' is selected. The configuration options include:

- Enable user auto-provisioning**:
- Auto-provision roles**:
 - System Administrator
 - OU Supervisor
 - Policy Administrator
 - Policy User
 - QMS Administrator
 - QMS User
 - Message Tracker
- Additional Host Pattern Matches**: An empty text input field.
- SMTP Hosts**: A table with columns for Target host, Priority, Security, Authentication, Username, Password, Mail, Auth, and Line limit. The 'Target type' is set to 'SMTP server'.

Target host	Priority	Security	Authentication	Username	Password	Mail	Auth	Line limit
151.155.183.147	1	none	auto			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000
	1	none	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000

- iv. If using LDAP authentication, enter the *LDAP target host*, set the *Scope* to sub tree, and enter the *DN template/DN search base*, for example, DN=company,DC=com

sf.gwava.net

Enable user auto-provisioning

Auto-provision roles

- System Administrator
- Group 1
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- Message Tracker

Additional Host Pattern Matches

SMTP Hosts

Target type: SMTP server

Target host	Priority	Security	Authentication	Username	Password	Mail Auth	Line Limit
151.155.183.142	1	auto	auto			<input checked="" type="checkbox"/>	1000
	1	none	none			<input checked="" type="checkbox"/>	1000

LDAP Hosts

Target host	Priority	Security	Username	Password	Auth	Validate	Scope	DN template / DN search base	Search pattern
151.155.183.142	1	none	CN=dapple ldap,CN=l	*****	<input checked="" type="checkbox"/>	<input type="checkbox"/>	sub tree	dc=sf,dc=gwava,dc=net	
	1	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	template		

Notes

2. Create a Policy:

Create at least one [policy \(Policy_Management.htm\)](#) with Block and Quarantine Services under *Organization/Policy Management | Policy Management*. The wizard can create a default that will handle most cases.

3. Set up Digest:

- a. Log out of the System Administration console and log into the QMS console as admin.
- b. Select the *Digest* tab and under the *Settings* sub tab, confirm that *Enable global digest services* is enabled.

Enable global digest services

Contact email address

Digest Template


Preferred digest language

Maximum digest rows

Release button address

Digest recipients

Custom address list

Remove selected 

Add new 

- c. Under the *Schedule* sub tab select a day or time for the digests to be sent to users with quarantined messages. Click on the Time row to select the entire row, click on the Day column to select an entire day, or the top corner for all.

Quarantine	Options	Digest	Users	Groups	Settings		
Settings		Schedule		Manual Release			
	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Midnight	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8:00am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Midday	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

On the Email Server

1. In the email server set outbound messages to go to GWAVA/Secure Messaging Gateway.

GroupWise

In *GroupWise Administration* | *Internet Agents* | *SMTP/MIME* | *Settings* | *Relay Host for outbound messages*: set to the GWAVA/Secure Messaging Gateway server.

Exchange

In *Exchange Admin Center | Mail flow | Send connectors* set the send connector to route to the GWAVA/Secure Messaging Gateway server.

2. A new SMTP IP address won't be trusted. Add to [trusted relays \(Interfaces.htm#Allowed_relay_sources\)](#).

Installing into an Existing Secure Messaging Gateway Network

If the Secure Messaging Gateway server is being deployed into an existing Secure Messaging Gateway network, there are a few settings which need to be configured. The Secure Messaging Gateway Network shares the databases to keep the configuration, quarantine, and statistics up to date and common across the whole system. A Secure Messaging Gateway Network is utilized when multiple servers are required to handle the load or must be separated due to the host network and design where multiple Secure Messaging Gateway appliances at multiple locations are required.

Overview

First, setup the main Secure Messaging Gateway server for Postgres to have the database installed and created. Then, the following steps must be completed. All Postgres steps must be completed as 'root' user:

1. Configure Postgres to allow remote connections.
2. Determine and set the connection addresses allowed.
3. Restart Postgres.
4. Complete the initialization of the remaining Secure Messaging Gateway servers.

Setup

In order for the databases to be accessible to all Secure Messaging Gateway servers, Postgres must be configured to allow remote connections.

1. Configure Postgres to allow remote connections.

To configure Postgres to allow remote connections a file must be modified.

NOTE: The file must be modified as root user.

The file which must be modified is: (replace the 9.x directory with the running version of Postgres. Likely 9.5)

```
/etc/postgresql/9.x/main/pg_hba.conf
```

As the root user, open the *pg_hba.conf* file with the preferred editor and locate the line: # IPv4 local connections:

```
host all all 127.0.0.1/32 md5
```

This line only specifies connections from the localhost. Add new connection addresses to this line to allow for multiple and remote connections.

Modify the line to make it look similar to this:

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5
host all all 10.1.29.0/24 md5
```

2. Determine and set allowed connection addresses.

Modifying the *pg_hba_conf* file correctly requires that the IP addresses of the remaining Secure Messaging Gateway servers are known. The addresses may be specified individually or they may be specified in a range.

For example, the above specified address setting of "10.1.29.0/24" will allow connections from any address of 10.1.29.x.

If a subnet of addresses is desired, it may also be specified as such:

10.0.0.0/8 Will allow any connection from addresses 10.x.x.x

172.16.0.0/16 Will allow any connection from addresses 172.16.x.x

192.168.1.0/24 Will allow any connection from addresses 192.168.1.x

Or if a specific IP is to be specified: 192.168.1.20/32

Once the file has been modified to allow connections from the desired addresses, save the file.

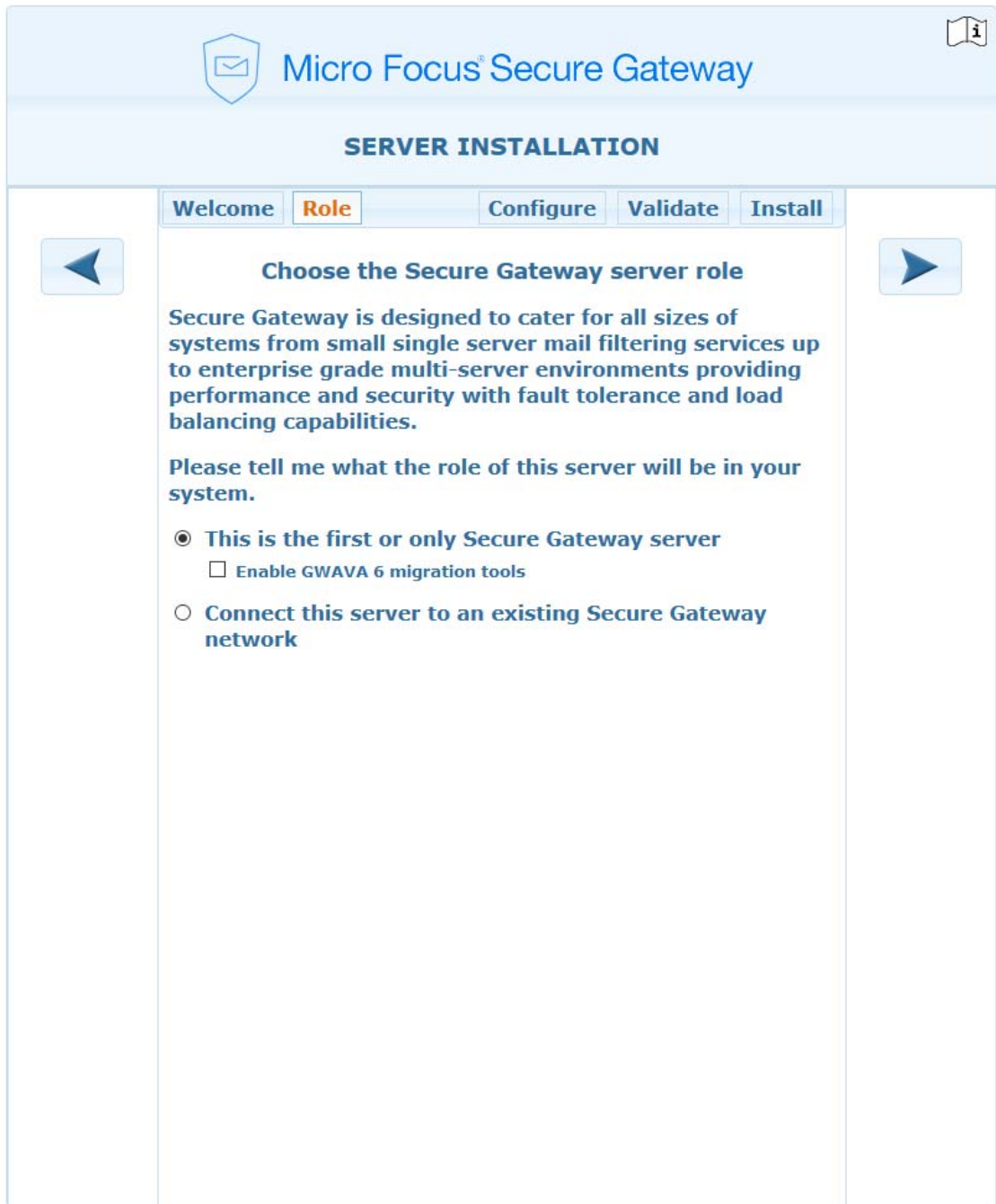
3. Restart Postgres.

Postgres must be restarted to load the new configuration. Once Postgres has been restarted, the rest of the Secure Messaging Gateway servers may be deployed and initialized.

```
/etc/init.d/postgresql restart
```

With Postgres now configured to allow multiple connections, the initialization of the rest of the Secure Messaging Gateway servers may be completed. Make sure that the address for the newly configured Postgres server is used for configuring the remaining servers

4. Install next Secure Messaging Gateway server. Select "Connect this server to an existing Secure Messaging Gateway network"



5. Configure next Secure Messaging Gateway server.

SERVER INSTALLATION

Welcome Role **Configure** Validate Install

Connect to existing Secure Gateway network

Provide all of the details in preparation for configuring your Secure Gateway server.

Additional server configuration may be necessary prior to running this process. Click the information icon in the upper right corner of this page to view the online guide for full details.

Server name

Connection address

Description

System key 

Postgres Database Configuration

DB server address

DB name

DB user name

DB password

Server name: The name of this server will use.

Connection address: The IP address of this server.

Description: An optional field to describe this server.

System key: The system key is a unique value used to secure your Secure Messaging Gateway system, that is shared across all servers. Due to its sensitive nature, it is not stored in the system database.

Typically you can leave this entry blank, and an existing gwavaman program will be contacted to acquire the key during the validation step.

If the validation process cannot obtain this key from another server, you will need to access the config/system.xml file inside the Secure Messaging Gateway directory on an existing server and enter the <privatekey> entry here manually.

Please note that entering an invalid key will cause secure data to be incompatible between servers and will very likely lead to system instability.

DB server address: The address of the database server configured in Setup above on the first Secure Messaging Gateway server.

DB name: The name of the database from above.

DB user name: The username for the database.

DB password: The password for the database.

6. Validate and install the server.
7. Login and [configure \(Post-Install_Tasks.htm\)](#) the server.

GWAVA 6 to Secure Messaging Gateway Migration

The migration tools can migrate your data from GWAVA 6 to Secure Messaging Gateway. The migration tool can be run multiple times so a piecemeal strategy is possible for the migration. For example, one recommended strategy is to setup Secure Messaging Gateway and import the exceptions from GWAVA 6.

Pre-migration Tasks

Open port 5432 in the firewall, if necessary.

Secure Messaging Gateway can be added to an existing GWAVA network and the settings migrated from GWAVA 6.

If the GWAVA server is being deployed into an existing GWAVA network, there are a few settings which need to be configured.

The GWAVA Network shares the databases to keep the configuration, quarantine, and statistics up to date and common across the whole system. A GWAVA Network is utilized when multiple servers are required to handle the load or must be separated due to the host network and design where multiple GWAVA appliances at multiple locations are required.

First, setup the main GWAVA server for Postgres to have the database installed and created. For SQLite databases download them and skip to the Migration. Then, the following steps must be completed. All Postgres steps must be completed as 'root' user:

1. Configure Postgres to allow remote connections.
2. Determine and set the connection addresses allowed.
3. Restart Postgres.
4. Complete the initialization of the remaining GWAVA servers.

In order for the databases to be accessible to all GWAVA servers, Postgres must be configured to allow remote connections.

1. Configure Postgres to allow remote connections.

To unlock the databases, configure Postgres to allow remote connections.

Telnet into the server.

A configuration file must be modified as root user. Make a copy as a backup before modifying the file. The file which must be modified is:

```
/opt/beginfinite/gwava/postgres/pg_hba.conf
```

As the root user, open the *pg_hba.conf* file with the preferred editor and locate the line:

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5
```

This line only specifies connections from the localhost. Add new connection addresses to this line to allow for multiple and remote connections.

Modify the line to make it look similar to this:

```
# IPv4 local connections:
host all all 127.0.0.1/32 md5
host all all 10.1.29.0/24 password
host all all <Secure Messaging Gateway IP Address>/<Subnet mask> password
```

2. Determine and set allowed connection addresses.

Modifying the `pg_hba_conf` file correctly requires that the IP addresses of the remaining GWAVA servers are known. The addresses may be specified individually or they may be specified in a range. For example, the above specified address setting of “10.1.29.0/24” will allow connections from any address of 10.1.29.x.

If a subnet of addresses is desired, it may also be specified as such:

```
10.0.0.0/8 Will allow any connection from addresses 10.x.x.x
172.16.0.0/16 Will allow any connection from addresses 172.16.x.x
192.168.1.0/24 Will allow any connection from addresses 192.168.1.x
```

Or if a specific IP is to be specified:

```
192.168.1.20/32
```

Once the file has been modified to allow connections from the desired addresses, save the file.

3. Restart Postgres.

Postgres must be restarted to load the new configuration. Once Postgres has been restarted, the rest of the GWAVA servers may be deployed and initialized.

```
rcpostgresql-9.1 restart
```

or

```
/etc/init.d/postgresql restart
```

4. Complete the initialization and deployment of the remaining GWAVA servers.

With Postgres now configured to allow multiple connections, the initialization of the rest of the GWAVA servers may be completed. Make sure that the address for the newly configured Postgres server is used for configuring the remaining servers.

5. Revert Secure Messaging Gateway installation to default state by renaming or removing the configuration files from two locations.

Telnet into the Secure Messaging Gateway server.

a. Rename or remove the files in `/opt/gwava/config`

```
root@gwava153:/opt/gwava/config# ll
total 4
drwxrwx--- 2 root gwava 24 May 26 10:48 ./
drwxr-xr-x 14 root root 179 May 26 10:48 ../
-rwxr----- 1 root gwava 407 May 26 10:48 system.xml*
```

b. Rename or remove the files in `/opt/gwava/gwavaman/http_local/security`

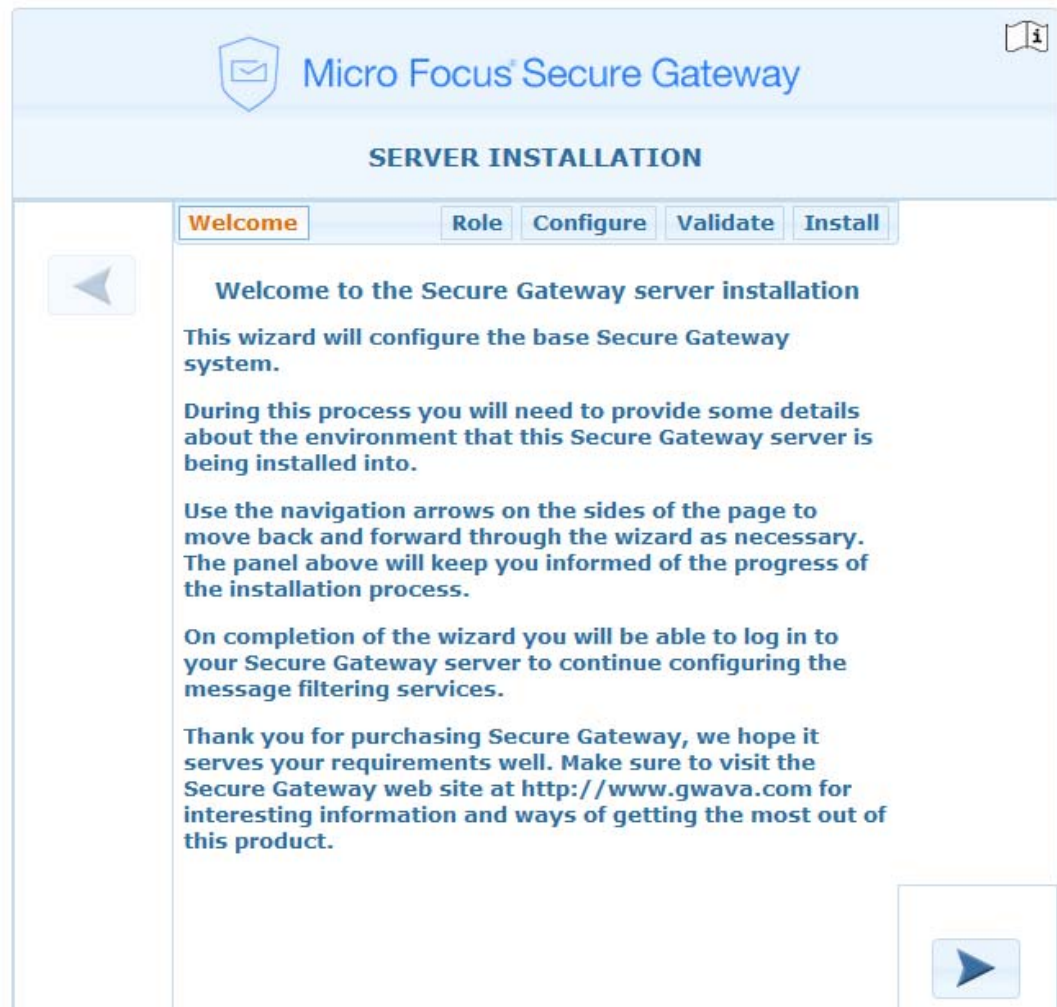
```
root@gwava153:/opt/gwava/gwavaman/http_local/security# ll
total 8
drwxrwx--- 2 root gwava 67 May 26 10:48 ./
drwxrwx--- 4 root gwava 36 May 26 10:48 ../
-rw-r--r-- 1 www-data www-data 0 May 26 10:48 install.lock
-rw-r--r-- 1 www-data www-data 108 May 26 10:48 pg_auth.php
-rw-r--r-- 1 root gwava 62 May 26 10:48 privatekey.php
```

c. Restart apache

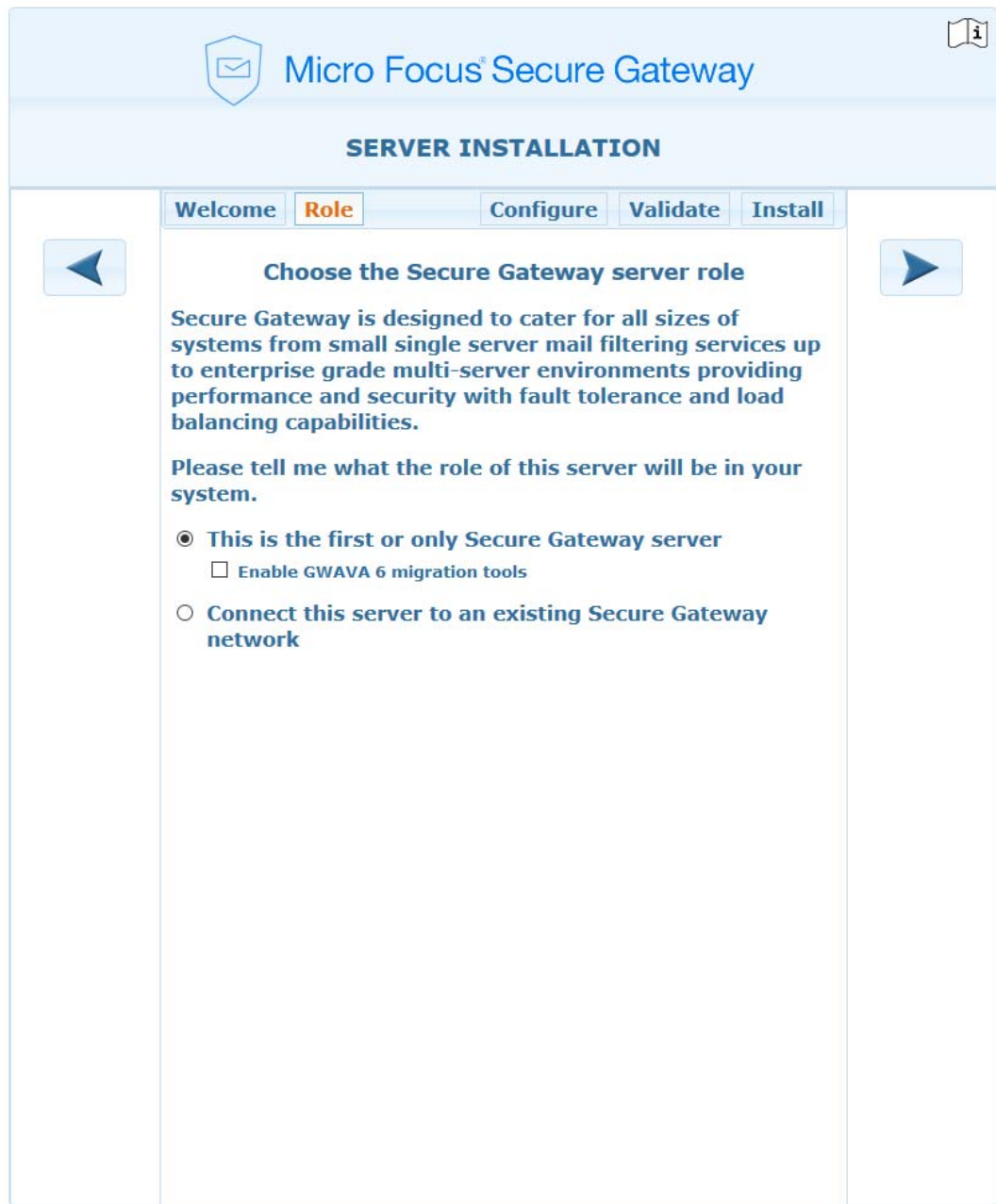
```
service apache2 restart
```

d. Browse to Secure Messaging Gateway

e. Setup Secure Messaging Gateway



f. Setup the Server Role and enable *Enable GWAVA 6 migration tools*.



g. Configure the Secure Messaging Gateway server



SERVER INSTALLATION

Welcome Role **Configure** Validate Install



Configure new Secure Gateway server

Provide all of the details in preparation for configuring your Secure Gateway server.

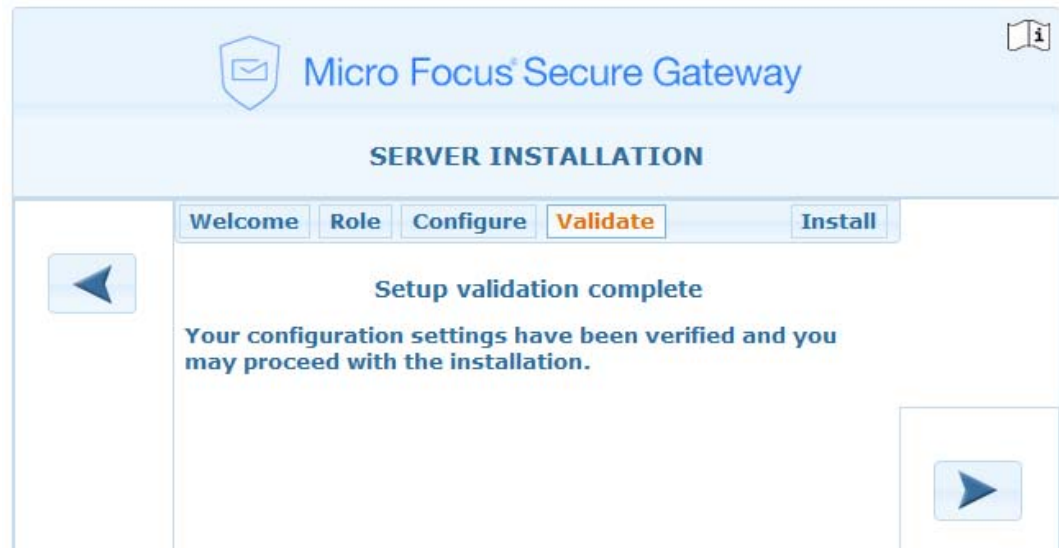
Server name	<input type="text" value="gwava153"/>
Connection address	<input type="text" value="151.155.183.153"/>
Description	<input type="text"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="•••••"/>
Re-type password	<input type="password" value="•••••"/>
Primary domain	<input type="text" value="doc.mf.net"/>
Contact email	<input type="text" value="aiden@doc.mf.net"/>
Mail relay server	<input type="text" value="151.155.183.147"/>
Mail relay username	<input type="text"/>
Mail relay password	<input type="password"/>
Setup default system	<input checked="" type="checkbox"/>

Postgres Database Configuration ⓘ

Config	Quarantine	Statistics	Tracker
DB server address	<input type="text" value="127.0.0.1"/>		
DB name	<input type="text" value="SecureGateway"/>		
DB user name	<input type="text" value="postgres"/>		
DB password	<input type="password" value="••••••••"/>		



h. Validate the server installation

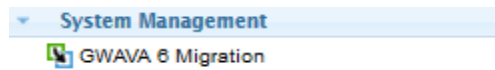


Migration

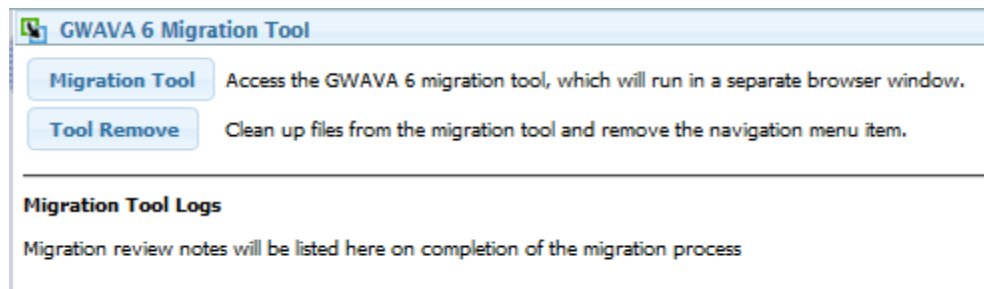
GWAVA 6 Migration Tool

Log into Secure Messaging Gateway System Administration.

Select *System Management | GWAVA 6 Migration*



You'll have two choices



Migration Tool will open a new window to begin the process.

Tool Removal will clean up the migration files and remove the menu item.

By selecting the migration tool you will be given an instruction page.

The migration tool *will* migrate:

GWAVAMAN database

Quarantine Management System Database(s)

and/or User Exceptions Database.

The migration tool *will not* migrate:

SSL certificates

QMS data

IP Settings

Custom notifications

Message Tracker data

Interfaces

Connection drop settings

Spam reporting

Conversation tracking

SMTP relay configuration

Proxy configuration

Reporting

Click on the next arrow (>>) to continue

Configure GWAVA 6 Database Connections

Enable a database to reveal its settings. The migration tool can be run as often as desired, so piecemeal migrations are acceptable.

For SQLite, upload the database files downloaded from GWAVA 6.

For postgres, provide the required information

Overview

GWAVA 6 is comprised of several major components. The toolkit can be used to selectively import these parts of a GWAVA 6 system, or even multiple GWAVA 6 systems into Secure Gateway.

If you choose to only import some settings from GWAVA 6 at this time, you may return to the toolkit at a later time to continue importing additional data.

During this toolkit some information about your GWAVA 6 installation will be required. The information can be located from the System management section of your GWAVA 6 management console.

Configure GWAVA 6 Database Connections

- GWAVAMAN Database

Select database type

- External (postgres)
- Internal (sqlite)

Server address

Database name

Database login name

Database login password

Test connection

Database test succeeded

Press *Test connection* to determine if the database can be accessed by Secure Messaging Gateway.

Press next (>>) to continue. If not all databases are filled in then a warning will appear.

Import Filter Setup

The migration tool can inspect the GWAVA system before importing the data.

Import Filter Setup

Select the categories of data to inspect for import.

Press the start button below when you are ready to run the inspection process.

Start Inspection

This panel lists issues found with the migration process that are discovered with your system.

Import Components

- System configuration**
- Admin Accounts**
- Domains**
- Interfaces**
- Policies**
- QMS System Configuration**
- QMS Digest Configuration**

Review the resulting report. The panel at the top right provides detailed information about each section of this migration.

Review Import Data

Inspection of components is complete. Select the actions to be taken for each item. Expandable items provide finer control of individual import items allowing directed import of individual items into existing configuration.

The default action for imported items that are not individually controlled will be to create new items in the system. This is a good option to use for first time migration.

When you are happy with the selection of items to migrate, press the next page button to start the migration process.

Import Components**System configuration**

- Number of days to retain logs
- Agent restart setting

Admin Accounts

Import into OU [root] v

- Admin (account already exists)

Domains

Import into OU [root] v

- qa.gwava.com
- suzdom.com

Interfaces

- (SMTP_INTERFACE) smtp
(GWMTA_AGENT) mta scan
(GWPOA_AGENT) poa scan

Policies

- smtp Import as new policy [root] v
 - Enable bypass mode
 - Match message direction
 - Scan inbound mail
 - Scan outbound mail
 - Scan internal mail
 - Scan collected mail
 - Scan composed mail
 [click here to customize imported data]
- poa scan Import as new policy [root] v
 - Enable bypass mode

This panel lists issues found with the migration process that are discovered with your system.

- **System Configuration Notes**

- Most of the system and server configuration settings have been preconfigured on this system. Due to relocation and enhancements to most of these settings, migrating many of these options is unlikely to be correct. Please review the items below for settings that may need to be reviewed for consistency with your previous system.
- SSL configuration is no longer centrally configured. Please read the documentation for instructions on how the web interface and SMTP interfaces are configured.
- IP address configurations must be manually redefined. Please read the documentation for instructions on IP interface settings.
- The SMTP relay module has different settings. Review the relay module configuration to ensure it is compliant with your network infrastructure.
- Proxy configuration is currently not implemented for any services, and has no configuration setting available.
- Proxy configuration is currently not implemented for any services, and has no configuration setting available.
- **Interface Configuration Notes**
- One or more interfaces configured in your GWAVA 6 system cannot be imported. Secure Gateway only directly supports SMTP email traffic. Please refer to the GWAVA knowledgebase for information on the status of other interfaces.
- Imported interfaces will not be automatically assigned to a server on systems that have multiple servers, or have an existing interface of the imported type. After migration, you should review the imported interface and assign it to a server to activate it. Any conflicts with existing interfaces need to be resolved by adjusting relevant settings or disabling the existing interface.
- **Policy: smtp**
- This policy has an interface limit imposed. Interface assignment is now provided at the interface level and will need to be reconfigured to achieve an equivalent

Start the Migration

Click next (>>) to begin the migration. A warning will appear.

This action will start the migration process. Are you sure you want to begin?

OK

Cancel

Migration Complete. This will provide a log of the actions taken including the pre-migration inspection.

Status: Migration finished

Help

Migration Complete

The migration tool is now complete.

If you performed a partial migration, you may reuse the migration tool at any time to import more data into this Secure Gateway system.

Any information that was logged during the migration process, which is listed below, can be reviewed from the main system administration interface from the GWAVA 6 Migration page.

If you no longer have a need for the migration tool, it is recommended that it is removed from the menu system. The main entry page to the migration tool provides the option to clean up the files and menus associated with the migration tool. It can be added back into the system if necessary by running a script that is documented in the GWAVA knowledgebase.

If errors or warnings are listed in the migration log, please check whether the associated component has been imported correctly into the Secure Gateway system. Some system features may cause data collisions which will not affect your system. In these cases, particularly when running the migration multiple times, it may simply be a case where duplicate data tried to be inserted. The system is correctly rejecting these.

Migration Tool Log

Migration log was not found

Post Migration

Check that the items were migrated correctly. Migrated data will be marked as (Migrated). For example mta scan (Migrated):

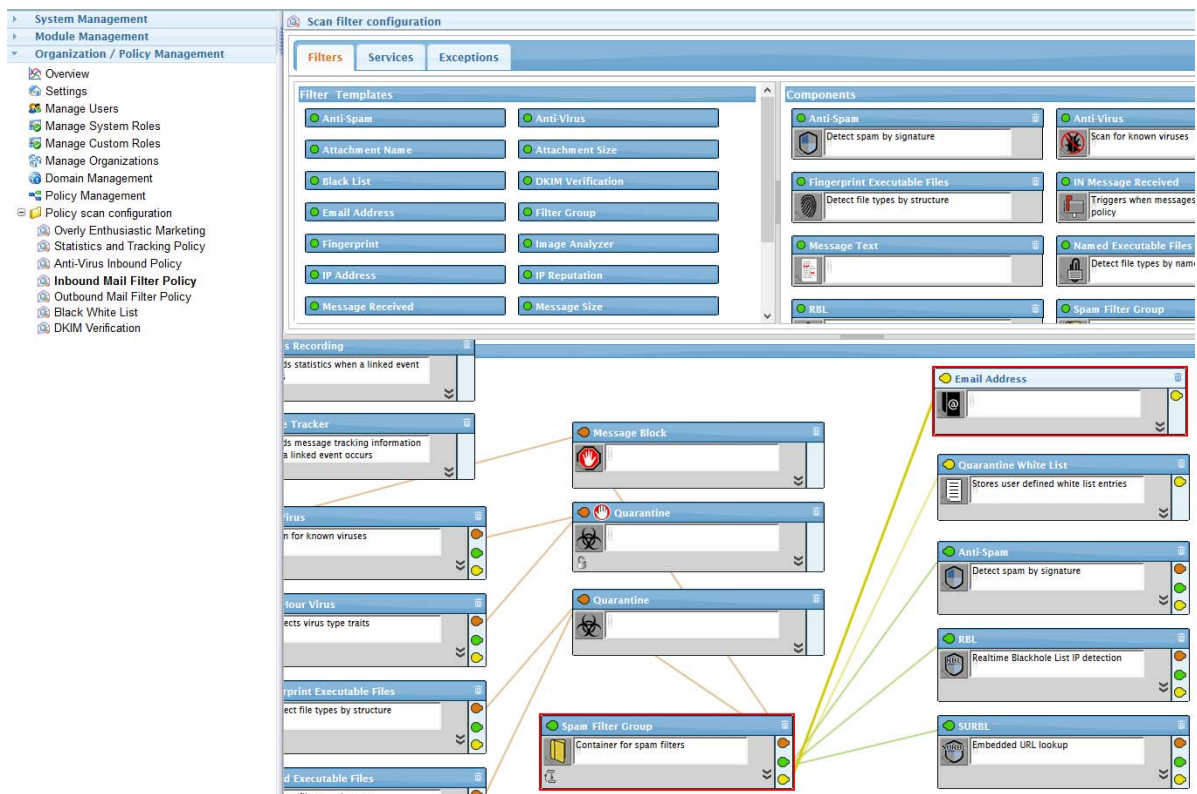
The screenshot displays the 'Scan filter configuration' window. On the left, a navigation pane shows 'System Management' > 'Module Management' > 'Organization / Policy Management' > 'Policy scan configuration', with 'mta scan (Migrated)' selected. The main area is divided into 'Filters' and 'Components' sections. The 'Filters' section lists various filter templates like 'Anti-Spam', 'Anti-Virus', and 'Attachment Name'. The 'Components' section lists migrated components such as 'Antivirus (G6 import)', 'Attachment name (G6 import)', 'Bulk spam (G6 import)', and 'Confirmed spam (G6 import)'. Below this is the 'Deployment Workbench', which shows a visual representation of the configuration. It features two columns of nodes. The left column contains nodes for 'Attachment name (G6 import)', 'Antivirus (G6 import)', 'Zero Hour Virus (G6 import)', 'Confirmed spam (G6 import)', and 'Inbound mail (G6 import)'. The right column contains nodes for 'Block (G6 import)', 'Quarantine (G6 import)', 'Block forced on (G6 import)', and 'Quarantine forced off (G6 import)'. Lines connect the nodes between the two columns, indicating the relationships and actions defined in the configuration.

Manual Migration

If you are migrating from another message processing product or an older version of GWAVA, you can migrate your settings manually. It is recommended that you study the Policy Scan Configuration “Policy Scan Configuration” on page 148 section before you begin.

1. Begin by creating a list of exceptions from your old program. These are the email addresses you are allowing/disallowing system-wide.
2. Then create an Inbound Mail Filter Policy “New Policy Wizard” on page 169 or a Block and Quarantine with Exceptions policy “Creating a Block and Quarantine with Exceptions Policy” on page 180.

You can migrate the settings you have built up in the other program. For example, you want to import the email address exceptions that should be allowed through. In this case, you can add an email address exception to the Spam Filter Group.

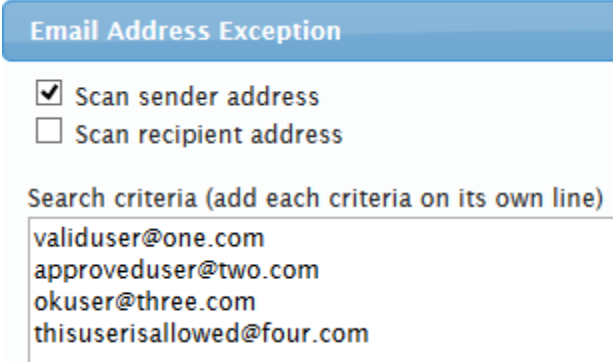


In this example, you will use an inbound mail filter policy and modify it to act as a system whitelist, which is different from a user's personal whitelist.

1. Begin by creating a list of whitelist exceptions for this filter. Go to your old filter program and gather the list of system-wide allowed emails. Copy them to a text file, one email address on each line with no leading or trailing spaces, and no blank lines.
2. Create an inbound mail filter policy using the wizard, under System Administration | Policy Management.
3. Add an exception by going to the Exception tab and dragging down the Email Address exception to the workbench. Connect the exception to the filter by clicking and dragging the yellow pin. In this example, to the Spam Filter Group.

4. Click on the Exception Icon (the little black book with an @ sign) to edit the search criteria. This is where you paste a copy of the exceptions from the other program.

NOTE: Make sure there are no leading or trailing spaces around the email addresses, and that there are no blank lines.



Email Address Exception

Scan sender address
 Scan recipient address

Search criteria (add each criteria on its own line)

validuser@one.com
approveduser@two.com
okuser@three.com
thisuserisallowed@four.com

5. Press Ok to save the search criteria.

6. Press Save (the little floppy disk icon at the top-right) to save and activate the filter.

This same logic applies to creating a IP address, or message text exception. In the case of message text exceptions, interior spaces are allowed but a line should not begin or end with a space and no lines may be completely blank..

Setting up a Multi-Tenant System

If you are running a system with multiple tenants, for example as an ISP, you can set up Secure Messaging Gateway to handle the messages for each domain separately without having a separate server for each domain.

A default system and Organizational Unit (OU) will need to be created then a URI Association for tenant-admins to sign up through. Then tenant-users can log on to view their quarantine.

Setting Up a Multi-tenant System

Configure the following:

1. Interface. [“Interfaces” on page 101](#)
2. Scan engine. [“Scan Engine Manager” on page 108](#)
3. QMS. [“QMS Module Manager” on page 113](#)
4. Message tracker. [“Message Tracker Module Manager” on page 116](#)
5. Statistics. [“Stats Module Manager” on page 115](#)
6. Mail Relay module. [“Mail Relay Module Manager” on page 110](#)
7. Default OU to contain the tenant units. [“Manage Organizations” on page 132](#)
8. Default Policy within the default OU, new tenants will use this policy. [“Policy Management” on page 144](#)
9. URI Association. Create a URI association for tenant-admins to sign up with. This requires a captcha key to be generated. Select the OU to assign new tenants to. [“URI Association” on page 84](#)

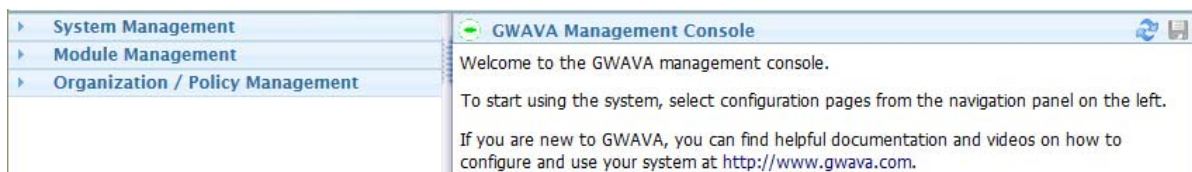
10. Confirm each module can service the default OU.

3 System Administration

Log into the Micro Focus Secure Messaging Gateway server and select System Administration.



This takes you to the Micro Focus Secure Messaging Gateway Management Console

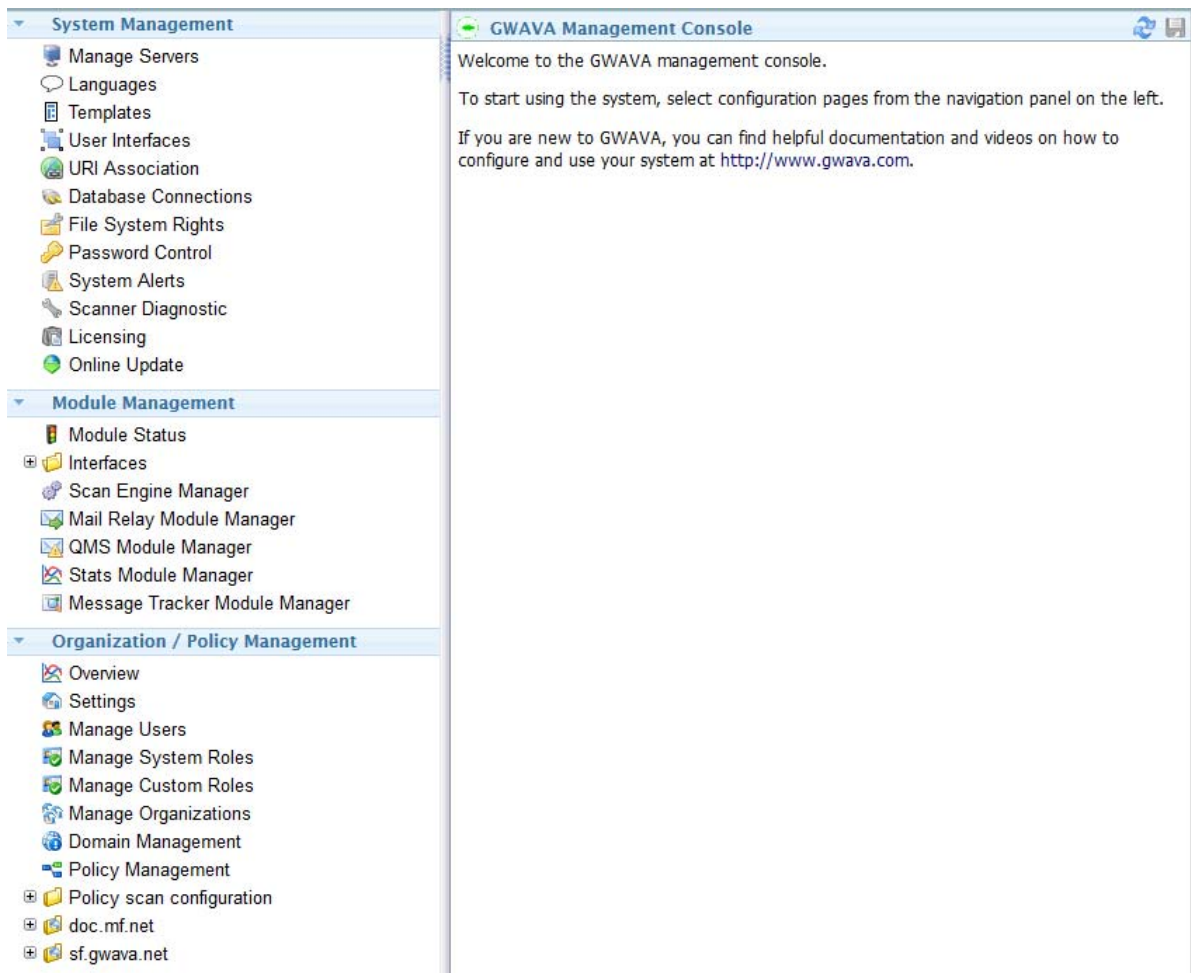


From here you can access the administrative functions of Micro Focus Secure Messaging Gateway.

They are grouped into three primary sections:

- ♦ *System Management*: Deals with servers, templates, databases and other system-wide items.
- ♦ *Module Management*: Deals with scanners installed on the system.
- ♦ *Organization / Policy Management*: Deals with users, roles, organizations and policies.

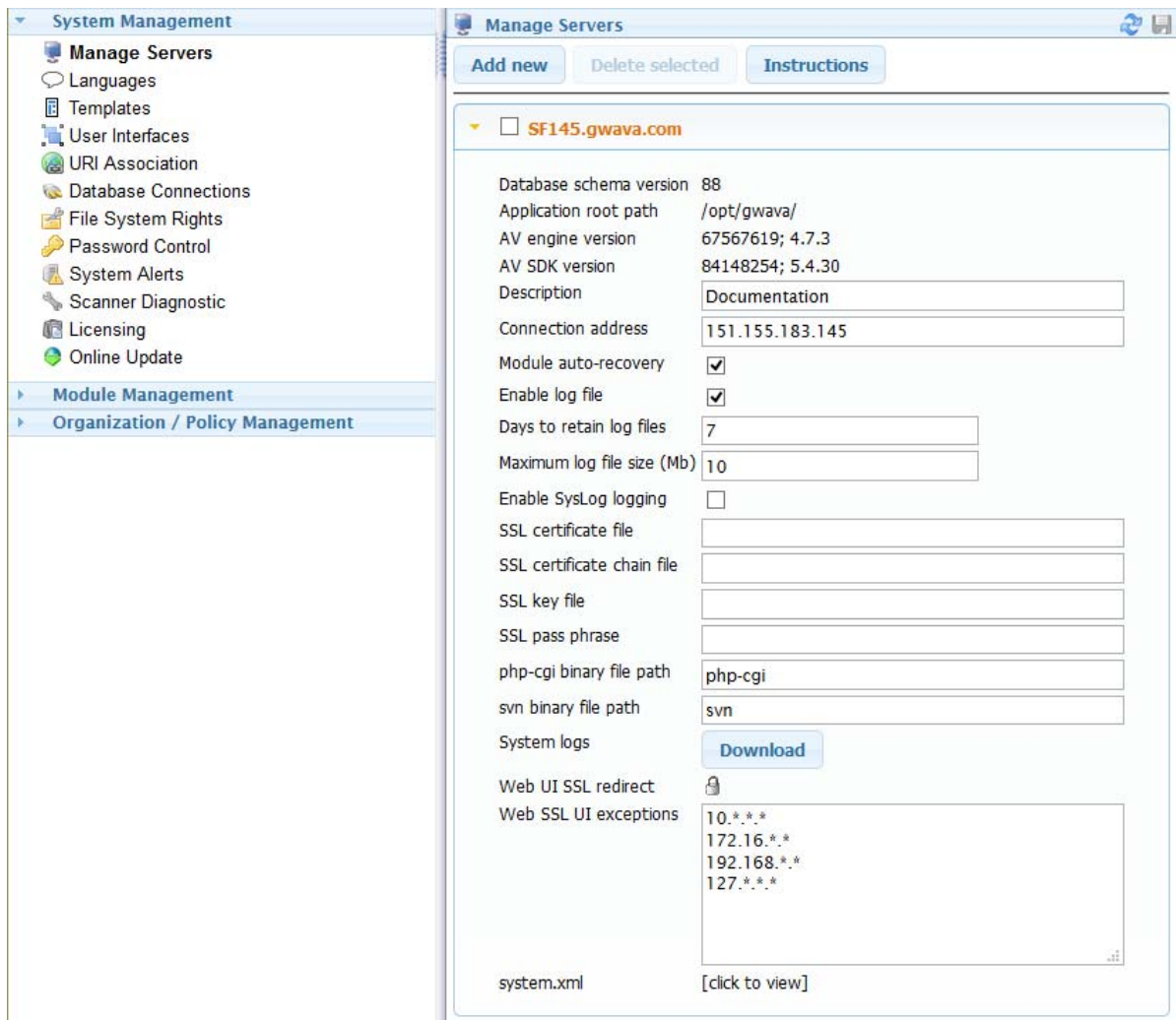
Click on the titles or reveal triangles to open each section.



System Management

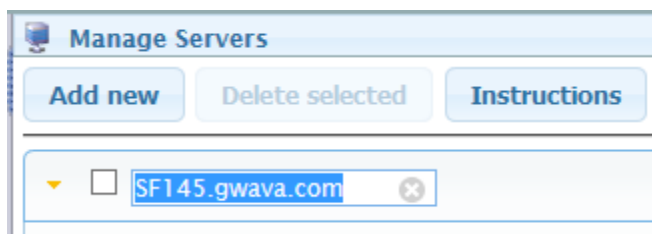
Manage Servers

Each server in your Micro Focus Secure Messaging Gateway network requires some information specific to its instance. If, for some reason, a server fails and needs to be reconstructed, the necessary setup files can easily be regenerated from the information provided on this page.



- ◆ To recover a server, install a new Micro Focus Secure Messaging Gateway server as a single standalone server. Once the installation is complete, edit the system.xml file which is located in the config folder of the installation directory. Replace the contents with the XML file displayed under the server information panel, adjusting the highlighted information for your system.
- ◆ The database password entry in the file will be encrypted once gwavaman has run for the first time.
- ◆ Once complete, restart the Micro Focus Secure Messaging Gateway programs.

You can rename the server by clicking on the name of the server.



Enabling SSL on Secure Messaging Gateway

There are two ways to configure SSL with Secure Gateway: With Secure Messaging Gateway and enabling SSL in apache. Both methods require that you have already obtained from your registrar.

Prerequisites

- ◆ SSL certificate file
- ◆ SSL certificate chain file
- ◆ SSL key file
- ◆ SSL pass phrase

Method 1: Within Secure Gateway

- ◆ Log into the Secure Gateway server via TTY and upload the files to the server.
- ◆ Log into Secure Gateway web console as admin and go to System Administration.
- ◆ Under System Management | Manage Servers open the server panel.
- ◆ Enter the file locations for each file and the SSL pass phrase.
- ◆ Save the configuration.
- ◆ Logout.
- ◆ Change the URL to begin with "https".
- ◆ Log into the Secure Gateway web console.
- ◆ If you want the web UI to redirect to SSL, under System Management | Manage Servers open the server panel and click on the lock for Web UI SSL redirect. Warning: You MUST be logged in with the https URL or you will no longer be able to connect to the Secure Gateway server.

Method 2: Enabling SSL in apache

SSL may be enabled directly in apache. See the [apache documentation \(https://httpd.apache.org/docs/2.4/ssl/\)](https://httpd.apache.org/docs/2.4/ssl/).

Callouts

Database schema version: The version of the schema the server database is using.

Application root path: The location of the application on disk.

AV engine version: The version of the anti-virus engine.

AV SDK version: The version of the anti-virus software development kit.

Description: You may enter a description of this server here.

Connection address: The IP address or hostname of the Micro Focus Secure Messaging Gateway server.

Module auto-recovery: With this option checked, the modules will attempt to recover themselves if they lose connection. Default checked.

Enable log file: With this option checked, a log file will be kept. Default checked.

Days to retain log files: How long to keep log files on the server. Default 7.

Maximum log file size (Mb): How large log files are allowed to become before being cycled. Default 10.

Enable SysLog logging: With this option checked, a SysLog is kept. Default unchecked.

SSL certificate file: Copy the file here.

SSL certificate chain file: Copy the file here.

SSL key file: Copy the file here.

SSL pass phrase: Enter the pass phrase here.

php-cgi binary file path: Default: php-cgi

svn binary file path: Default: svn

System logs: Click the button to download the logs.

Web UI SSL redirect: The web UI can be redirected to a secure address. **WARNING:** Access to the system administration console may be lost if this option is not configured correctly.

- ◆ Forcing SSL connections to the web interface requires SSL to be configured in the Apache web server that hosts the Micro Focus Secure Messaging Gateway system.
- ◆ The Apache configuration is not managed within this administration interface. Please follow the guides on how to customize the web server for your site specific needs for SSL security, and test that SSL is functional before enabling this option.
- ◆ If SSL connectivity is disabled at a later date with this setting turned on, users and administrators will not be able to access the system.
- ◆ To prevent careless misuse of this option, it has been disabled due to the current connection not being SSL secure. To unlock the option, reconnect with a secure connection and navigate back to this page.

Web SSL UI exceptions: exceptions to the SSL UI redirect.

system.xml: To recover a server, install a new Micro Focus Secure Messaging Gateway server as a single standalone server. Once the installation is complete, edit the system.xml file which is located in the config folder of the installation directory. Replace the contents with the XML file displayed under the server information panel, adjusting the highlighted information for your system.

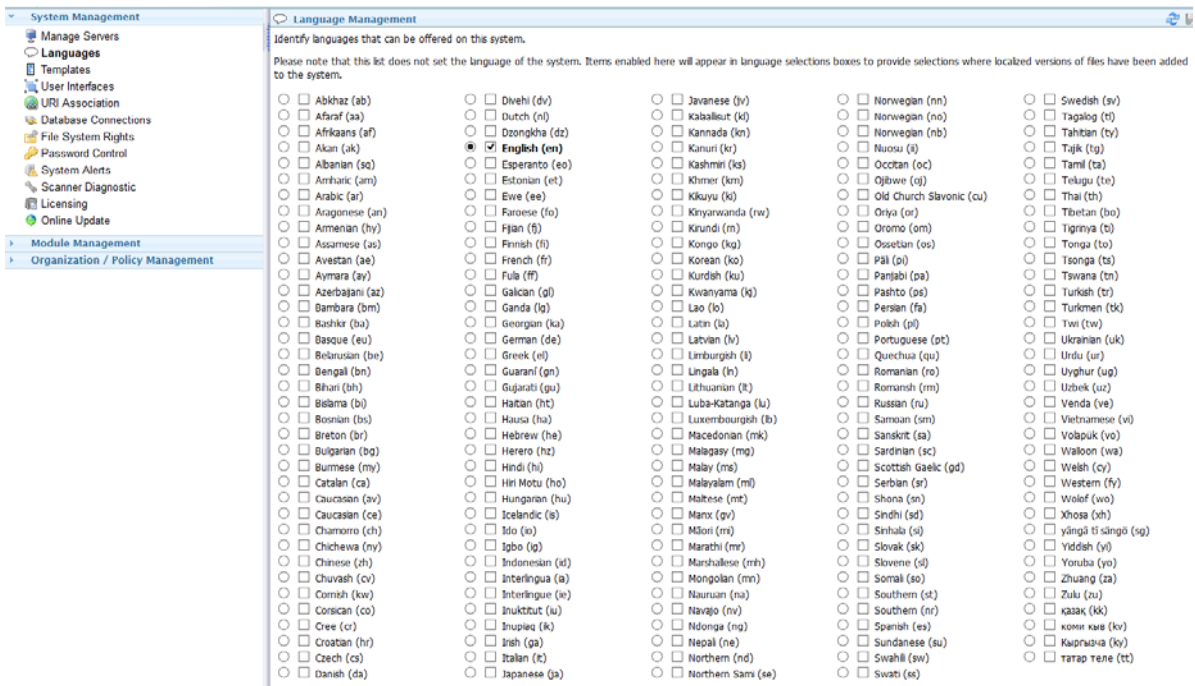
system.xml

Review the page instructions for details on usage of this information

```
<gwava>
<serverid>1</serverid>
<privatekey>copy this value from an existing server</privatekey>
<module name="gwavaman" id="1" />
<dbhost>database_host_address</dbhost>
<dbname>database_name</dbname>
<dbuser>database_username</dbuser>
<dbpass encrypted="no">database_password</dbpass>
</gwava>
```

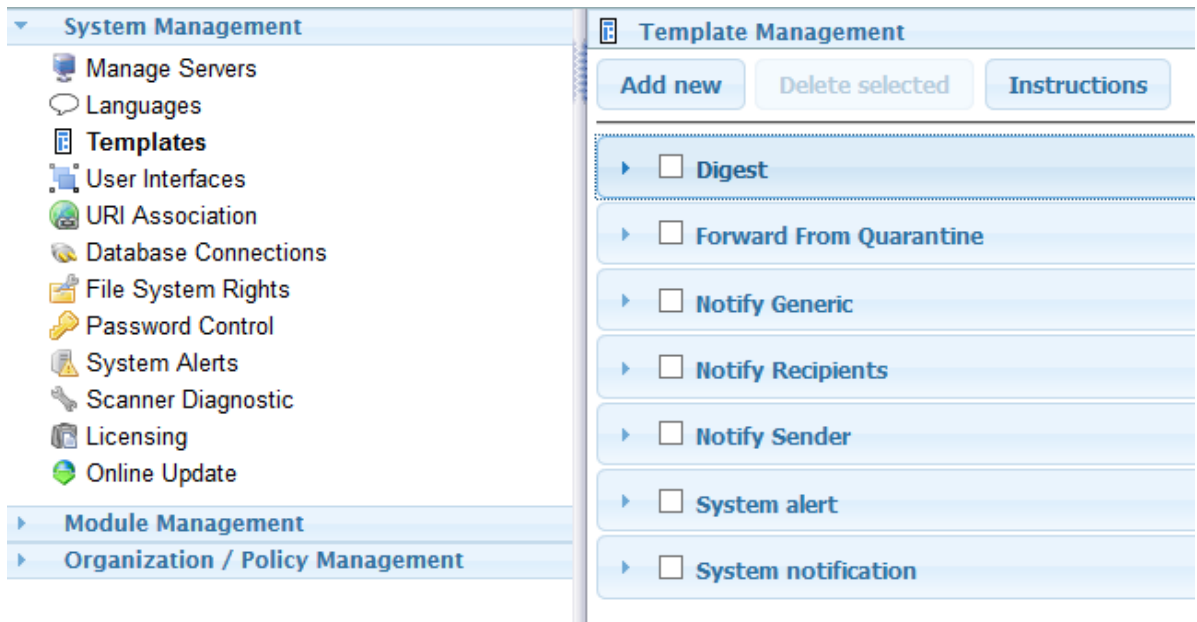
Languages

Select the languages that the system will make available in the interface.



Templates

The Template Management provides access to the template pages for all the notifications, digests, and alerts that GWAVA may send.

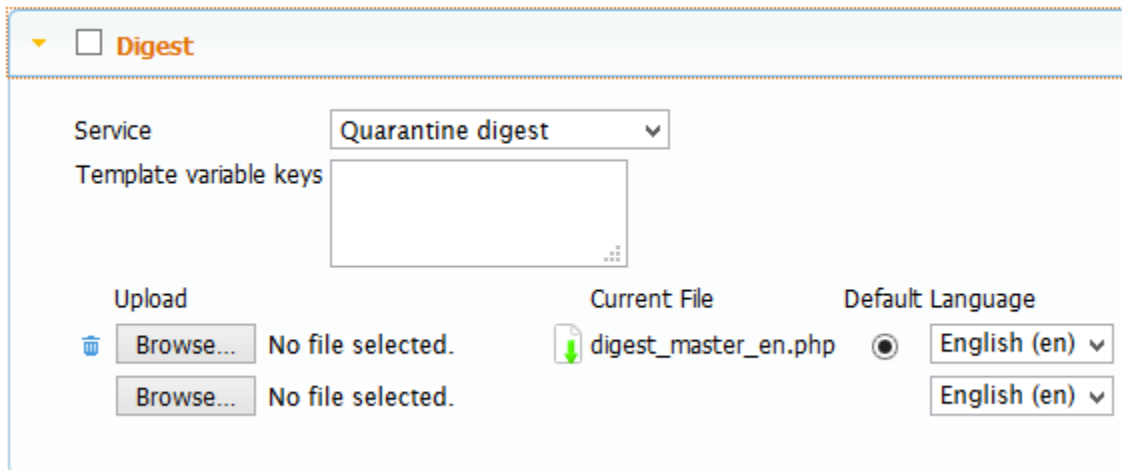


Always create custom templates if changes need to be made. Default templates should never be modified. When there is an update to any default template, any changes will be overwritten.

Custom Templates

Each template has a default master file. Never modify this file, any modifications will be overwritten when default templates are updated by the upgrade system.

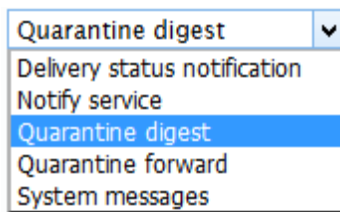
To customize these templates with a new icons, names, or layout, either create a new, custom template, or download and modify an existing template. It is highly recommended to name the modified template names something different than the existing template. While remote, there is a chance that the existing templates may be updated and custom changes overwritten if the name is left as default.



The screenshot shows a configuration panel for a 'Digest' service. At the top, there is a dropdown menu for 'Service' with 'Quarantine digest' selected. Below it is a text input field for 'Template variable keys'. Underneath, there are three sections: 'Upload' with two 'Browse...' buttons and 'No file selected.' text; 'Current File' with a file icon, a dropdown showing 'digest_master_en.php', and a radio button; and 'Default Language' with two dropdown menus, both showing 'English (en)'.

Service Dropdown menu

Select the service that will trigger the digest



The screenshot shows a dropdown menu with the following options: 'Quarantine digest' (selected), 'Delivery status notification', 'Notify service', 'Quarantine digest', 'Quarantine forward', and 'System messages'.

Delivery Status notification

Notify service

Quarantine digest

Quarantine forward

System messages

Template variable keys

Available keys for personalizing digest messages are:

SenderName

Subject

MessageText

AlertSeverity

AlertDetail

MessageText

MessageHTML

Upload: A new template may be uploaded to the system. This must be a PHP file.

Current File: Lists the current template being used by the service. The file can be downloaded by clicking on the download file icon.

Default Language: The languages made available in this drop down are determined by the languages selected in *System Management | Languages*.

To create a custom digest template

1. Go to the Digest panel and Download the Current File: `digest_master_en.php` to your workstation.
2. Rename the template to something straightforward such as `digest_custom_en.php`.
3. Open the template in a text editor, customize the template as needed, and save when complete.
4. Upload the new template to the next available Upload and select the Default radio button.
5. Press Save to make it available.

The screenshot shows the 'Template Management' interface. At the top, there are three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below this is a section for 'Digest' with a dropdown arrow and a checkbox. The 'Service' is set to 'Quarantine digest'. The 'Template variable keys' field is empty. There are three 'Upload' rows, each with a 'Browse...' button and the text 'No file selected.'. The 'Current File' column shows 'digest_master_en.php' and 'digest_custom_en.php'. The 'Default Language' column has three radio buttons and three dropdown menus, all set to 'English (en)'. The second radio button is selected.

Creating a template in a different language

For example, to create a German version of the digest template.

1. Go into the Languages tab and select German as an available language.
2. Go to the Digest panel and Download the Current File: `digest_master_en.php` to your workstation.
3. Rename the template to something straightforward such as `digest_master_de.php`.
4. Open the template in a text editor, translate it into German, and save when complete.

5. Upload the new template to the next available Upload and change the language to German.
6. Press Save to make it available.

Template Management

Add new
Delete selected
Instructions

Digest

Service
Quarantine digest

Template variable keys

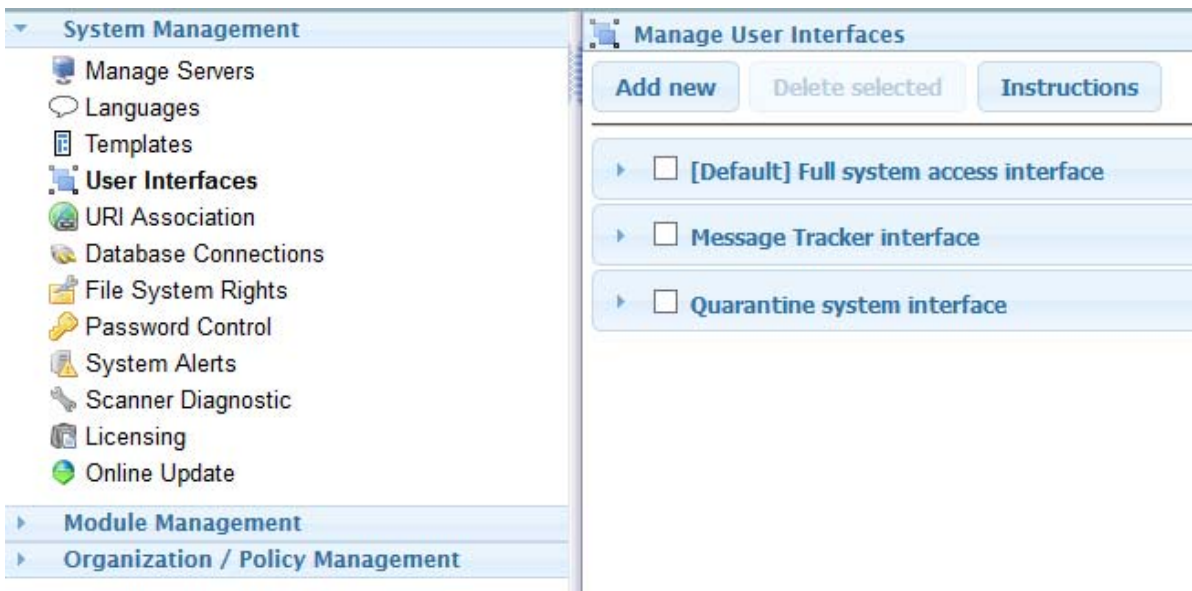
Upload	Current File	Default Language
Browse... No file selected.	digest_master_en.php	<input type="radio"/> English (en)
Browse... No file selected.	digest_custom_en.php	<input checked="" type="radio"/> English (en)
Browse... No file selected.	digest_master_de.php	<input type="radio"/> German (de)
Browse... No file selected.		<input type="radio"/> English (en)

User Interfaces

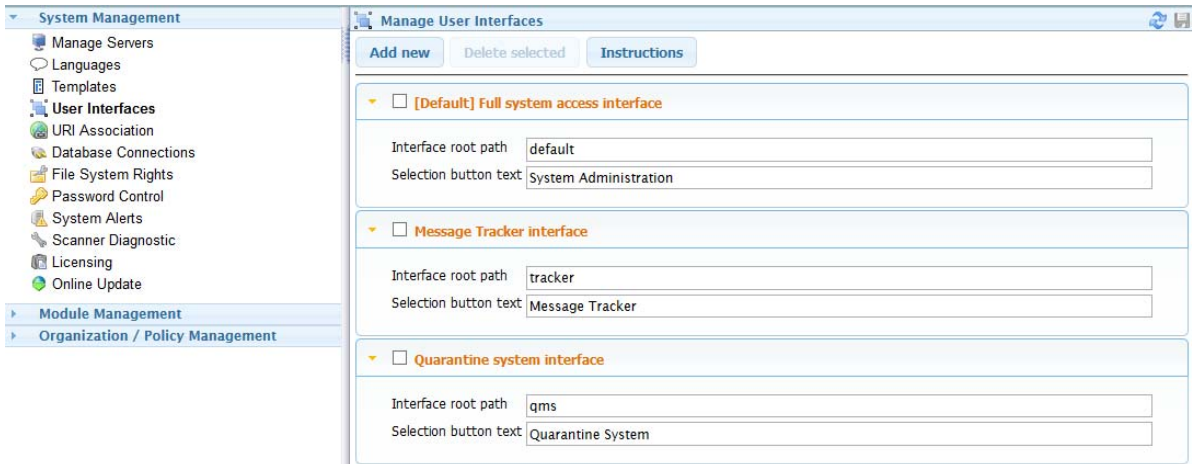
The Manage User Interfaces window allows administrators the ability to control the look and the login options of users for each interface.

If an administrator wants to modify or customize the login pages and text for either the management console or the qms interface, this is where the pages and text would be specified.

The text seen here is shown at the login page, and the root path holds the web pages to which the user would be directed.



Use the reveal triangle to expand the panel you wish to change.



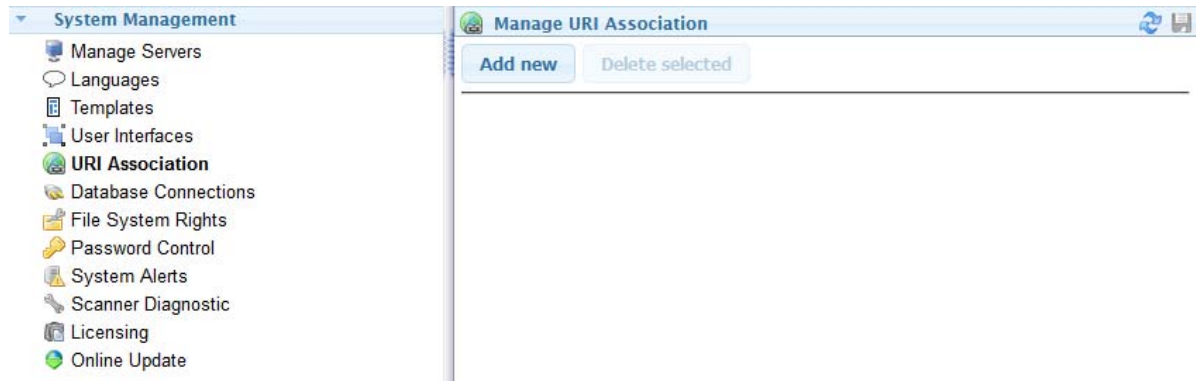
The *Interface root path* changes which section (default for system administration, tracker for message tracker and qms for quarantine management system) of GWAVA the button logs the user into.

The *Selection button text* changes the Select Interface dialog box button text.

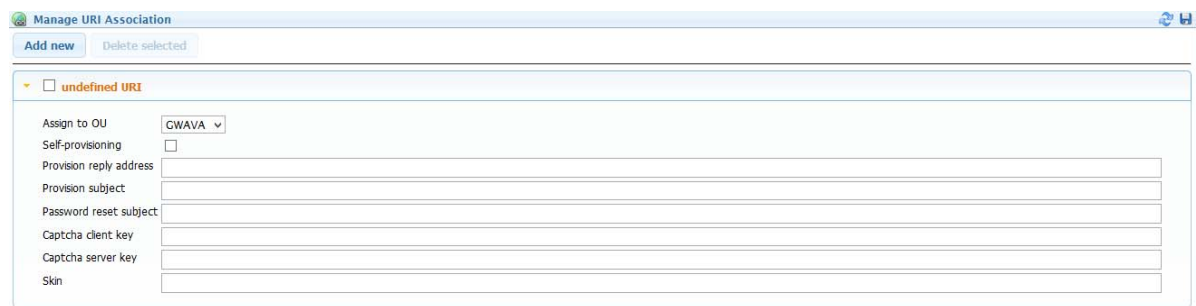


URI Association

If you are setting up a multi-tenant deployment in a cloud infrastructure and want to enable auto-provisioning of organizations this is where that is setup.



Click on *Add New* to provision a new URI for an organization.



Assign to OU: Select the OU to provision. Setup an OU in *Organization/Policy Management | Manage Organizations*.

Self-provisioning: Enable this to allow users to set themselves up.

Provision reply address: Enter the reply address of the provisioning email.

Provision subject: Enter the subject of the provisioning email.

Password reset subject: Enter the subject of the password reset email.

Captcha client key: Enter the Captcha client key. Setup the captcha so bots will not be able to set themselves up in the system.

Captcha server key: Enter the Captcha server key. Setup the captcha so bots will not be able to set themselves up in the system.

Skin: A branded template can be created for each OU.

For captcha API

[reCAPTCHA \(https://www.google.com/recaptcha/admin#list\)](https://www.google.com/recaptcha/admin#list)

Accessibility and captcha:

[Accessible CAPTCHA \(https://www.section508.gov/blog/CAPTCHA\)](https://www.section508.gov/blog/CAPTCHA)

[The accessibility of Google's No CAPTCHA \(http://simplyaccessible.com/article/googles-no-captcha/\)](http://simplyaccessible.com/article/googles-no-captcha/)

Database Connections

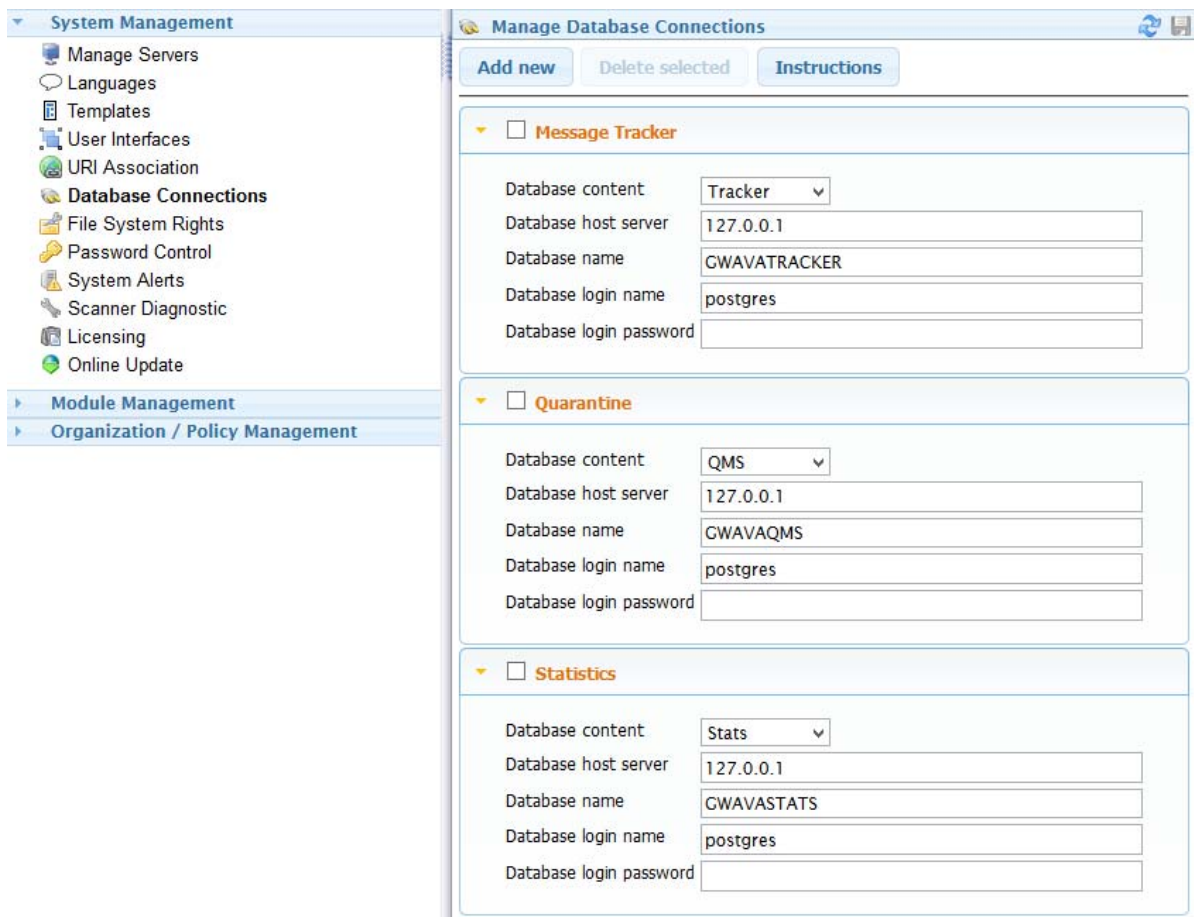
The Database Connections manager allows for the configuration of, management of, or removal of QMS and Stats databases for the system. This is designed for use with multiple organization to allow for separate databases for clients or organizations. If multiple organizations do not exist on the system, this feature will not be useful and should be left alone.

To create a new database for Micro Focus Secure Messaging Gateway to connect to: the intended content, host server, database name, and login credentials must be provided.

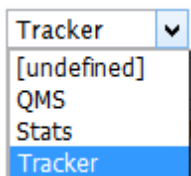
Supported databases:

Postgres 9.5 or higher

After creation, the new database will appear in the different module managers, (qms or stats), under the name specified here.



Database content drop down menu: Select the type of database to deploy



QMS

Stats

Tracker

Database host server: Enter the server that will host the database.

Database name: Enter the name of the database. Must be unique.

Database login name: Enter a database user login name.

Database login password: Enter a password for the database user.

File System Rights

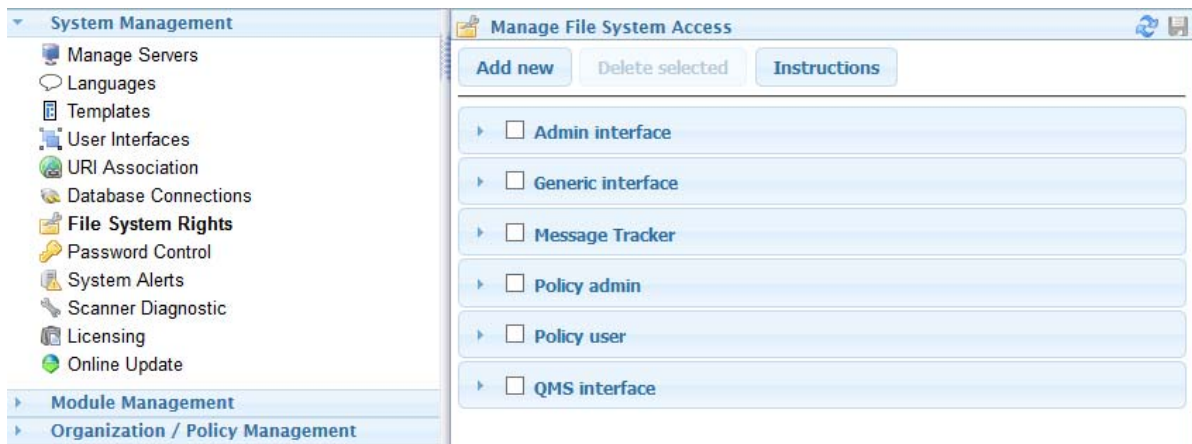
In Micro Focus Secure Messaging Gateway, roles define what abilities and rights any user has. The File Access Manager is the method by which the roles are fine tuned. File access determines which web pages any specific role can access.

If you do not know what you are doing in this interface, leave it alone; roles and rights of users can be messed-up quickly.

The Allow and Deny file path lists have the locations of the web pages in the interface. Allowing or Denying pages based on their path in the Micro Focus Secure Messaging Gateway file system allows administrators to fine-tune the interfaces that users have access to. If a page is to be modified, it is highly recommended to copy the page and modify the copy instead of potentially breaking a current interface file.

Unless you are comfortable writing and modifying PHP, this is an area which should not be changed.

File System Rights Interface



Admin interface

Admin interface

Allow file path list

Deny file path list

Role Assignment

- Message Tracker
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- System Administrator

Generic interface

Generic interface

Allow file path list

Deny file path list

Role Assignment

- Message Tracker
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- System Administrator

Message Tracker

Message Tracker

Allow file path list:

Deny file path list:

Role Assignment

- Message Tracker
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- System Administrator

Policy admin

Policy admin

Allow file path list:

Deny file path list:

Role Assignment

- Message Tracker
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- System Administrator

Policy user

Policy user

Allow file path list

Deny file path list

Role Assignment

Message Tracker
 OU Supervisor
 Policy Administrator
 Policy User
 QMS Administrator
 QMS User
 System Administrator

QMS interface

QMS interface

Allow file path list

Deny file path list

Role Assignment

Message Tracker
 OU Supervisor
 Policy Administrator
 Policy User
 QMS Administrator
 QMS User
 System Administrator

Allow file path list. The file paths the role is allowed access to.

Deny file path list. The file paths the role is denied access to.

Role Assignment. Which roles the file system access applies to.

Message Tracker

OU Supervisor

Policy Administrator

Policy User

QMS Administrator

QMS User

System Administrator

Password Control

Passwords stored on this system must be encrypted before use. This prevents data leakage when data is viewed from a web browser.

Password Control

Passwords stored on this system must be encrypted before use. This prevents data leakage when data is viewed from a web browser.

Processing server: SF145.gwava.com

Password: [Hidden]

3/bs64FELYIvbS5QmSuqW8JeGw98sDAX

Processing server. Which server will process the request

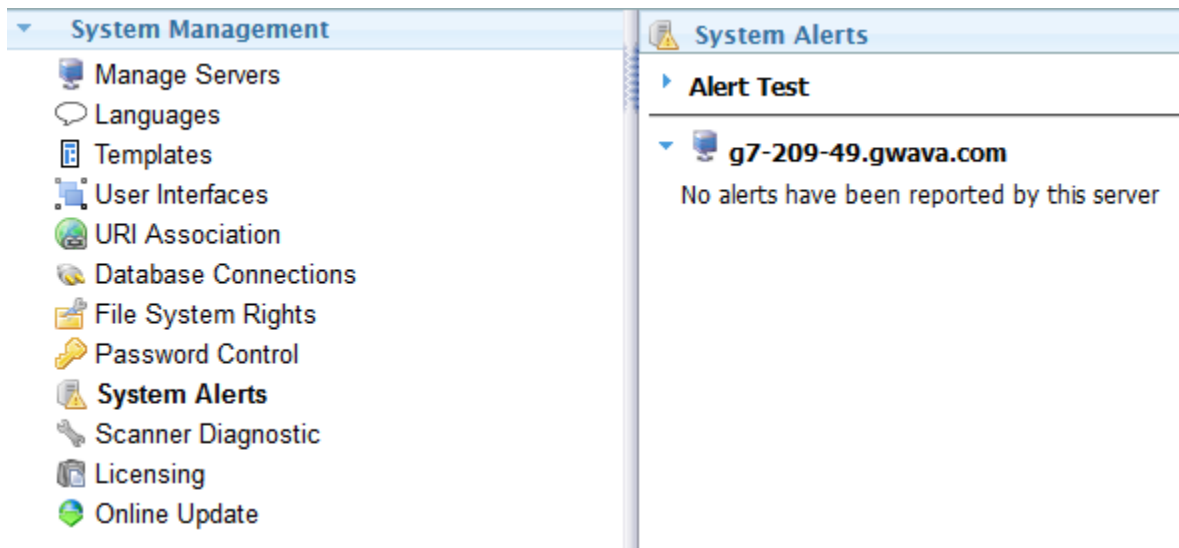
Password:

1. Enter the password text in the upper text box, the password will be hidden.
2. Press *Encrypt*.
3. The encrypted password will appear in the lower text box.

System Alerts

System alerts will list issues that have come up within the GWAVA system that need your attention.

Alerts are shown by server and module



Alert Test

The alert system can be tested.

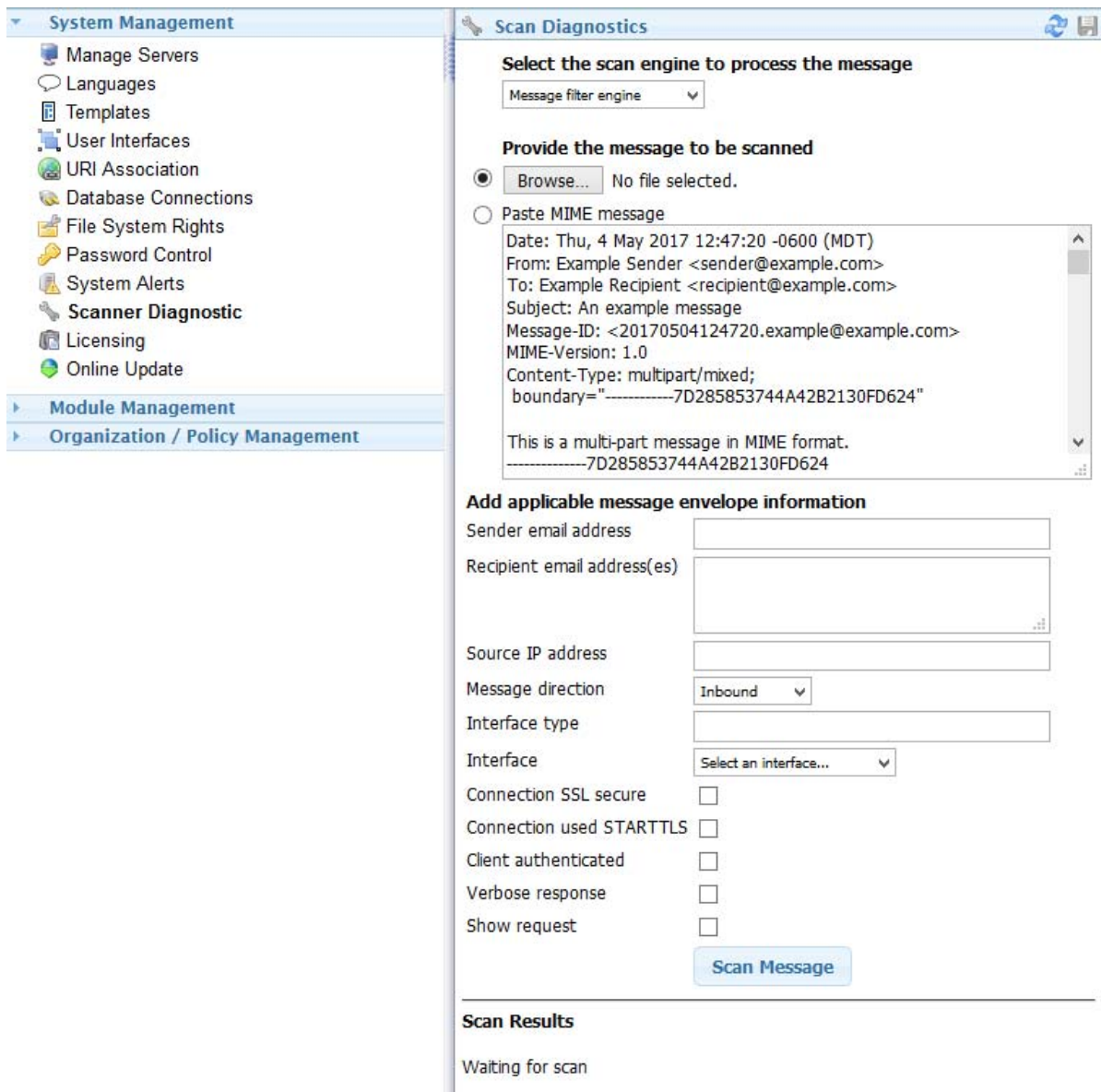


Select running module to test: Select the module on a particular server to test

Raise Alert: Press the button to begin the test.

Scanner Diagnostic

If a message is not filtered as you expect, it can be tested under Scan Diagnostics.



Select the scan engine to process the message: from the drop down menu

Provide the message to be scanned: by browsing to and uploading the file

Paste MIME message: paste the MIME.822 in the text box

Add applicable message envelope information:

Sender email address

Recipient email address(es)

Source IP address

Message direction

Inboard

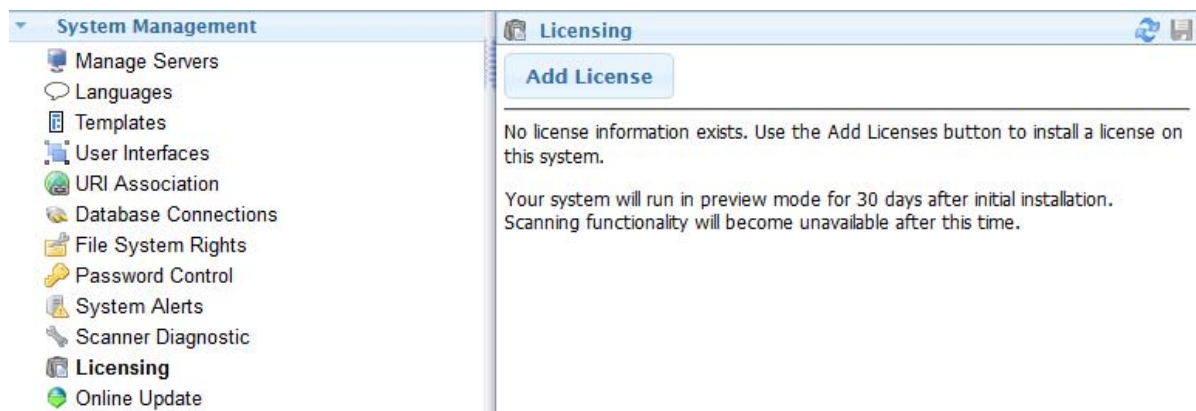
Outboard

- Internal
- Interface type
- Interface SMTP interface
- Connection SSL secure
- Connection used STARTTLS
- Client authenticated
- Verbose response
- Show request

Press *Scan Message* to begin the process. The results will appear under Scan Results.

Licensing

The license is checked every day and every time Micro Focus Secure Messaging Gateway is restarted. .



Before a license is installed you will receive the following message:

No license information exists. Use the Add Licenses button to install a license on this system.

Your system will run in preview mode for 30 days after initial installation. Scanning functionality will become unavailable after this time.

Click on *Add License* to enter your Customer ID (the email address your organization registered with) and Validation key.

License Lookup
✕

Enter your customer details

Customer Id

Validation key

Online Updates

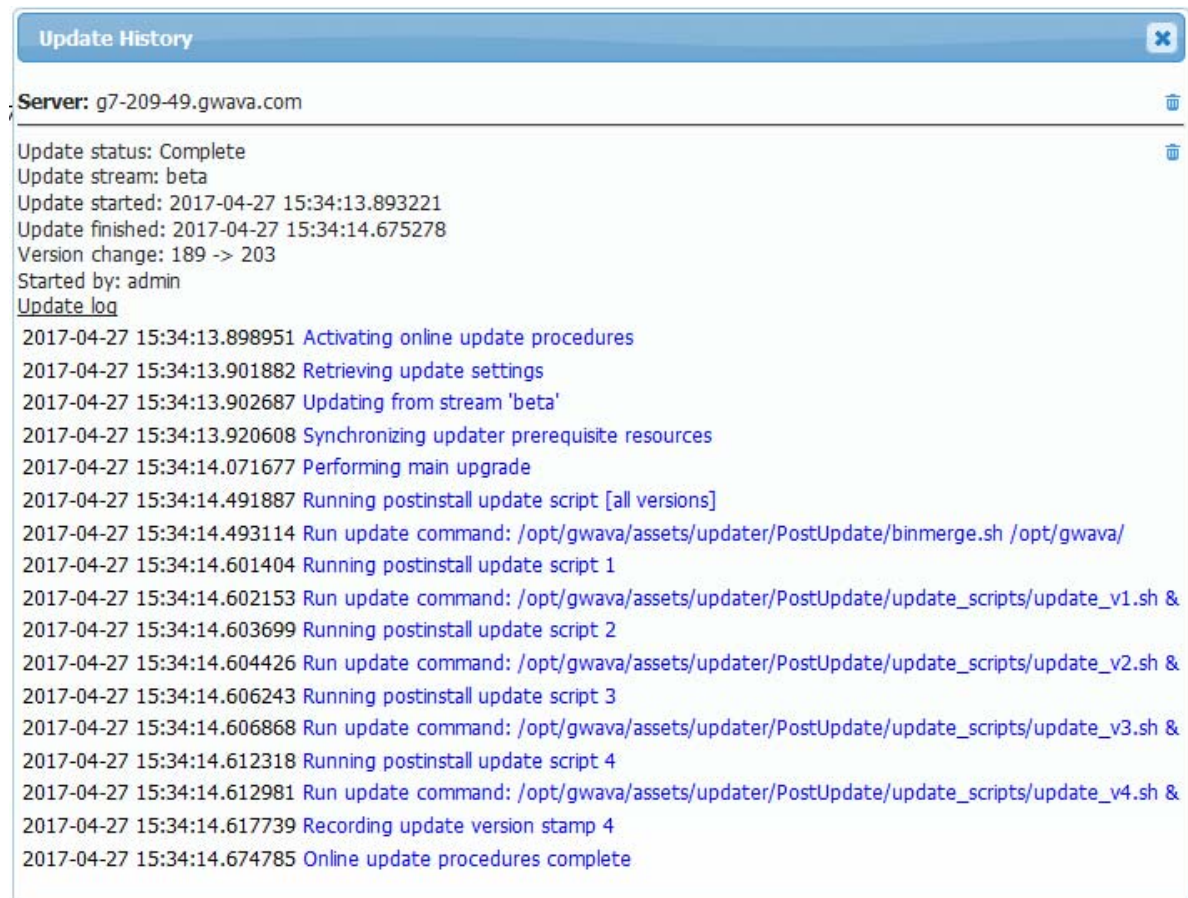
Micro Focus Secure Messaging Gateway is updated online. Virus and spam signatures are updated daily automatically.

To update the server click *Start Update*.

Once the update is complete the modules must be [restarted \(Module_Status.htm\)](#) manually.



Update History will show when the updates were installed on the server.



View Updates will show the versions installed on the server.

Version History

release beta

Revision: 200 - created 27-Apr-2017
 Fix custom user digest setting not displaying correctly when set to EXCLUDED
 Fix qms prune data/info options not displaying the correct state when items are disabled
 Fix custom roles not able to be removed
 Merge GWAV-1830 - Override EHLO/HELO host
 Fix Message Tracker role ID causing custom role creation issue on first attempt
 Add missing test harness files
 Modify wording of "View HTML Messages" to "View Message HTML" in QMS rights
 GWAV-1845 - Fix invalid path error in browser console when loading admin UI
 GWAV-1499 - Upload large files through PHP

Revision: 189 - created 30-Mar-2017
 Fix issue with HTTP upload process mapping source data type to incorrect method
 Fix HTML signature populating TEXT signature in UI when reloading node
 Add option to disable multi-threaded filters within an engine module
 GWAV-1689 - Custom Roles
 GWAV-1815 - Add move object button to domains management page
 GWAV-1771 - Policies created with wizard can now be deleted/moved/cloned immediately after creation
 Implement cipher list support for SMTP module SSL
 GWAV-1502 - Alter user last login info for users that have no login data recorded
 GWAV-1773 - Add exception handling to filter calls and fix possible usage of nullptr if MIME message cannot extract root entity during fingerprint tests
 Merge GWAV-1810 - Staggered DB sequences
 Add missing icon to notes box on workbench
 GWAV-1482 - Fix filters not saving in Chrome
 GWAV-1701 - Fix issue when parent events of events are removed, causing cascade deletes of attached events
 GWAV-1770 - New policies created with the wizard are suffixed with a number if a duplicate name would occur to

Module Management

Module Status

The status of each module by server, including uptime* is displayed on this page.

Server	Id	Description	Type	Status	Control	Up time*	Status received time
g7-209-49.gwava.com 1							
	10	Message filter engine	gwava	Up	Stop All Start All Restart All	6 days	2017-05-04 12:50:13.622264 (6 seconds ago)
	1	g7-209-49.gwava.com	gwavaman	Up	Stop Start Restart	6 days	2017-05-04 12:50:19.506705 (0 seconds ago)
	11010	SMTP Interface	gwvsmtp	Up	Stop Start Restart	6 days	2017-05-04 12:50:18.660846 (1 second ago)
	14010	Quarantine service	qms	Up	Stop Start Restart	6 days	2017-05-04 12:50:12.026557 (7 seconds ago)

* For modules that are down, up time displays the amount of time the module was previously active for. Systems that have not reported their health status provide the time since start, plus the known up time before the last heartbeat was received.

Green indicates a module that is up and has recently reported its status.
 Red indicates a module that is not running and/or was purposely shut down.
 Amber indicates a module that has not reported its health status within the expected timeframe, likely caused by a failure in the module.

* For modules that are down, up time displays the amount of time the module was previously active for. Systems that have not reported their health status provide the time since start, plus the known up time before the last heartbeat was received.

- ♦ Green indicates a module that is up and has recently reported its status.

- ♦ Red indicates a module that is not running and/or was purposely shut down.
- ♦ Amber indicates a module that has not reported its health status within the expected time frame, likely caused by a failure in the module.

Module Management

Modules are managed on this page. After an update the modules need to be restarted.

- ♦ Individual modules may be stopped, started or restarted.
- ♦ All modules may be stopped, started or restarted simultaneously.

Interfaces

Interfaces Overview

The interface managers are how Secure Messaging Gateway connect to the email system.

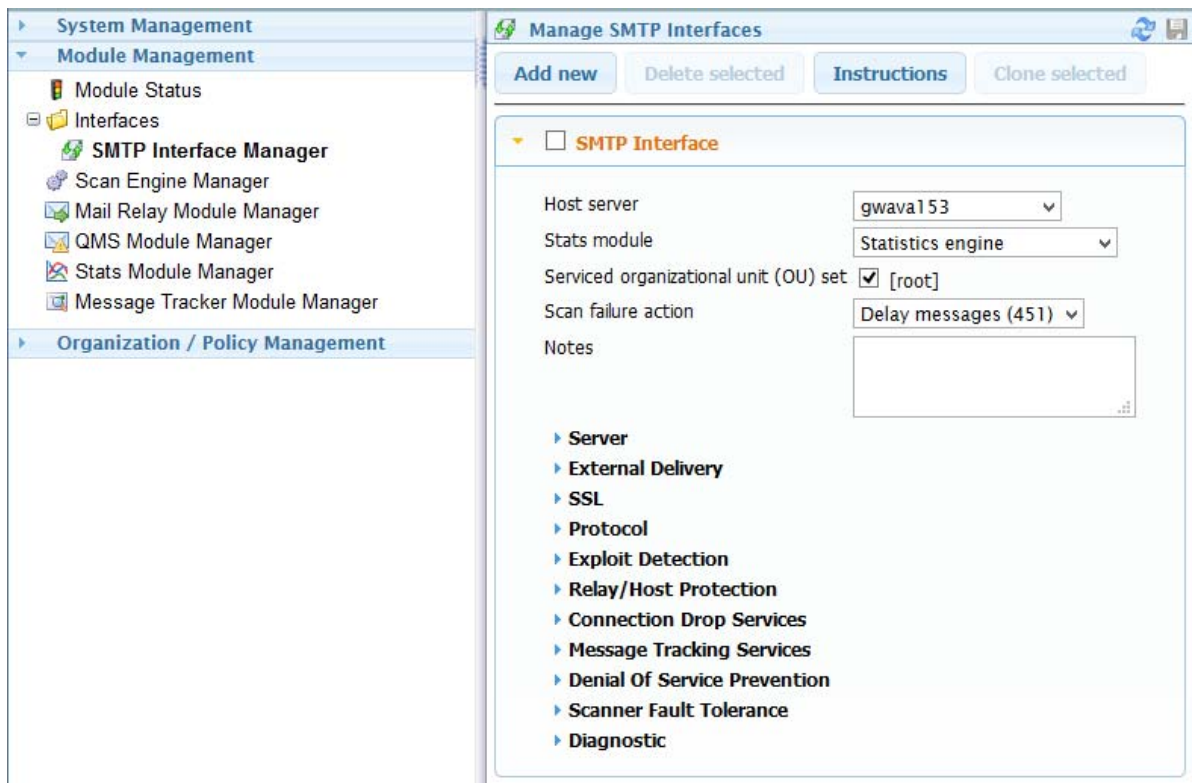
The SMTP interface defines the connection to an SMTP server.

SMTP Interface

The SMTP Interface Manager is used to configure and manage the SMTP interfaces in the Micro Focus Secure Messaging Gateway system. This interface controls the configuration of the SMTP for capturing messages to be scanned. Mainly, this is designed for use with multiple organizations and should not be changed if only running a single organization system.

If a serviced organization needs an exclusive SMTP, this is where to add and configure the new interface and tie it to the organization.

While configuring the new SMTP system, be sure to configure all desired fields. Before an organization can be selected to be tied to the SMTP, the organization must be created and configured on the 'Manage Organizations' page.



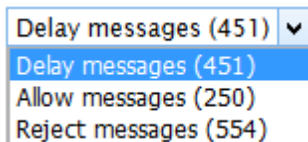
Create a new Interface by clicking *Add New*.

Host server: Select the host server

Stats module: Select the Statistics engine

Serviced OU set: Select the OU to service

Scan failure action: Select the action to take on failure



Delay messages (451)

Allow messages (250)

Reject messages (554)

Notes: Enter notes about the module, if desired.

Server

Enable SMTP server (plain): The SMTP server can be disabled here. Default, enabled.

SMTP server listen address: What IP address the SMTP server will listen on

SMTP source bind address: What IP address the SMTP server will bind to

Max inbound connections: Limit the number of inbound connections. Default, 256.

DSN template file: Delivery Status Notification template file location. The template can be created in *System Management | Templates*

Keep spool files: For support use. Save spool files to disk in /opt/gwava/gwsmtp/private/ Need to clean up manually. Default, disabled.

External Delivery

Connection Security: Set the security protocol.

None (Default)

auto

tls

ssl

Line Limit: How many lines to allow. Default, 1000.

Use relay server: Enable to use a SMTP relay server.

Relay targets:

SMTP Host Server: Enter the IP address or Hostname of the SMTP to use.

Priority: Enter the priority, 1 is highest.

Security: Select the security protocol used by the SMTP relay.

none

auto

tls

ssl

Authentication: Select the authentication protocol used by the SMTP relay.

None

auto

plain

login

cram-md5

Username: Enter the SMTP relay username, if needed.

Password: Enter the SMTP relay password, if needed.

Line Limit: Limit the number of lines to send, default 1000.

SSL

Enable TLS: Use TLS for security. Default disabled.

Enable SMTP server (SSL): Use SSL for SMTP. Default disabled.

SMTP server listen address (SSL): Enter the IP address of the SMTP server.

Max inbound connections: Limit the number of inbound connections. Default, 256.

SSL certificate file: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

SSL certificate chain file: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

SSL key file: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

SSL cipher list: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

SSL pass phrase: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

Protocol

Enable inbound timeouts: Default enabled.

Client connection timeout (sec): Default 15 seconds.

Client protocol timeout (sec): Default 5 seconds.

Enable outbound timeouts: Default enabled.

Server connection timeout (sec): Default 60 seconds.

Server protocol timeout (sec): Default 60 seconds.

SMTP banner: Enter the path to the file on the Micro Focus Secure Messaging Gateway server.

SMTP host domain: This will be pre-populated with the domain of the SMTP server is associated with.

Postmaster email: Enter the email address of the SMTP domain postmaster.

Custom EHLO responses: Enter custom EHLO responses, if desired.

Forwarded EHLO/HELO domain: Enter the forwarded domain.

Enable SIZE limit: Default enabled.

SIZE limit (bytes): Default 40000000.

Exploit Detection

Enable drop on invalid commands: Default enabled.

Max allowable invalid commands: Default 5.

Enable address hiding on dictionary attack: Default enabled.

Max failed addresses before hiding: Default 3.

Relay/Host Protection

Restrict relaying: Default enabled.

Allowed relay sources: Add the system's SMTP relay. Default "127.0.0.1", "10.*", "172.16.0.0/12", "192.168.*".

Allow Relay: Enable to allow relaying. Default, enabled.

Skip Connection Tests: Enable to skip the connection test. Default enabled.

Allow relay if authenticated: Default disabled.

Connection Drop Services

Delayed rejection state: Default No delay. In a multi-tenant system, it is especially important that this be set to DATA so that all recipient OUs are received and tracked in Message Tracker.

No delay

HELO/EHLO: Wait until the HELO/EHLO command is sent.

STARTTLS: Wait until the STARTTLS command is sent.
MAIL FROM: Wait until the MAIL FROM command is sent.
RCPT TO: Wait until the RCPT TO command is sent.
DATA: Wait until the DATA command is sent.

Report rejections to SMTP: Default enabled.

Enable RBL: Default enabled.

RBL server configuration

RBL Server

sbl-xbl.spamhaus.org (Default)

bl.spamcop.net (Default)

Skip Local IP: Default enabled.

RBL hit action

Reject connection (554)

Delay connection (421) (Default)

Enable IP reputation service: Default enabled.

Reject IP reputation match: Default enabled.

4xx on IP reputation tmpfail: Default enabled.

IP reputation host address: Default 127.0.0.1.

Enable SPF: Default disabled.

Treat ~all as -all: Default disabled.

IP address rejection: Enter IP address(es) to be rejected. One address per line.

Message Tracking Services

A storage location **must** be selected when this feature is enabled. Data may be stored in the default OU or in the owning (sender and/or recipient) OU.

At least one Message Tracking filter must be configured in the Policy Manager for this to work or only SMTP tracking data will be able to be gathered.

Enable message tracking: Default disabled.

Store in default OU: Default disabled.

Default OU for message tracking: Set to root, or if in a multi-tenant system to the default OU.

Store in owning OU: Default disabled. If enabled, the Connection Drop Services "Delayed rejection state" **must** be set to DATA to insure that all recipients are received.

Track only if NOT tracked by the scan engine: Default disabled.

Track only if connection dropped: Default disabled.

Denial of Service Protection

Enable DoS functionality: Default enabled.

Scanner Fault Tolerance

Priority influence: Influence Priority Message filter engine: 1 is highest.

Diagnostic

Enable client IP address override: Default disabled.

Client override IP address: Enter the IP address to override.

Retain decoded message files: For support use. When enabled copies of the message files will be saved to /opt/gwava/gwvsmpt/./tmp. For troubleshooting use only. If left enabled the hard drive will be filled. Default, disabled.

Retain raw message files: For support use. When enabled copies of the message files will be saved to /opt/gwava/gwvsmpt/./tmp For troubleshooting use only. If left enabled the hard drive will be filled. Default, disabled.

Average session time (seconds): Statistics about the sessions.

Average scan time (seconds): Statistics about the scans.

Scan Engine Manager

The Scan Engine manager contains the connection address, host server, and OU settings for a scanner.

The screenshot shows the 'Manage Scan Engines' configuration page in the Micro Focus Secure Gateway. The left sidebar contains a navigation tree with 'System Management' and 'Module Management' expanded. Under 'Module Management', 'Scan Engine Manager' is selected. The main content area is titled 'Manage Scan Engines' and includes buttons for 'Add new', 'Delete selected', and 'Instructions'. A 'Message filter engine' is listed with a checkbox. Below this, there are several configuration fields: 'Notes' (empty text area), 'Enable REST Service' (checked), 'Host server' (dropdown menu showing 'jgibbs-PC'), 'Connection address' (text input 'g7trunk'), 'Bind address' (text input '0.0.0.0'), 'Fault tolerance priority' (text input '1'), 'Multi-threaded scanning' (checked), and 'OpenDKIM services' (text input '127.0.0.1:4932'). At the bottom, there are statistics for 'Serviced OU set' (checked, '[root]'), 'Average message size (bytes)' (0 (past min), 3530 (past hr), [no data] (past 24hr)), and 'Average scan time (seconds)' (0 (past min), 0.033 (past hr), [no data] (past 24hr)).

Load Balancing

If dealing with very high load factors, additional servers can be joined to the network and the load balanced between the various servers in a round robin model.

Fault Tolerance

For fault tolerance, an additional server would need a lower priority and would be waiting until the higher priority is unable to fulfill more requests.

Organizational Units

Scan engines may be created to service specific organization units. A [new organization \(Manage_Organizations.htm\)](#) must be created before it can be selected for a scanner. Once created, the Organization will appear in the 'Serviced OU set' at the bottom of the configuration window.

If the scanner is to be hosted on a separate server in the network, the connection address should be specified.

Message Filter engine

Notes: Enter notes about the filter engine, optional.

Enable REST Service: Default enabled.

Host server: Select the server to run the engine on.

Connection address: Enter the IP address of the server.

Bind address: Default 0.0.0.0.

Fault tolerance priority: Default 1. 1 is highest.

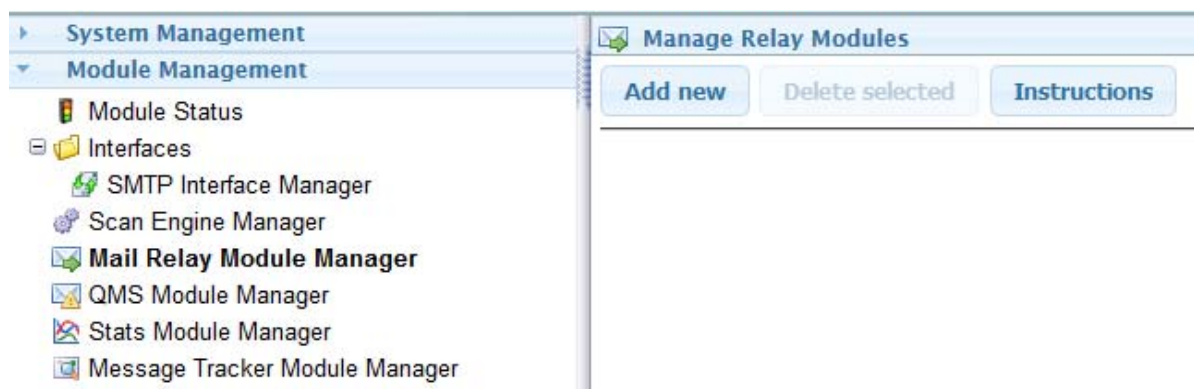
Multi-threaded scanning: Default enabled.

OpenDKIM services: OpenDKIM service list can have a list of multiple servers to be used. Each server can also have *,n* added (where n is a number) to provide for ordered failover and fault tolerance. Default 127.0.0.1:4932

Serviced OU set: Default enabled.

Mail Relay Module Manager

Micro Focus Secure Messaging Gateway can send many types of notifications depending on settings in the system. It may be desired to send the notifications to a separate system or SMTP relay. The Micro Focus Secure Messaging Gateway Relay will send all notification from the system to the target SMTP server.



To add a new SMTP relay, select 'Add new' and then configure the relay as desired. Save changes.

A *Host server* is required for the message queue. Specify a custom queue location if desired - it should be on the local machine.

Manage Relay Modules

[Add new](#) [Delete selected](#) [Instructions](#)

▼ **Relay to 151.155.183.142**

Send test message [Message test](#)

Host server

Message queue location

Maximum SMTP threads

Delivery targets

- Defined domains
- Relay targets
- MX targets

SMTP Relay Target List

Host Address	Auth	Auth Username	Auth Password	Security	Priority
<input type="text" value="151.155.183.142"/>	<input type="text" value="none"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="text" value="1"/>
<input type="text"/>	<input type="text" value="none"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="none"/>	<input type="text" value="1"/>

Send test message: Click button to send test message.

Mail Relay Test Message [X]

This test will send a message from the mail relay agent with the email addressing information supplied. Please ensure the addresses are valid to prevent delays in processing.

Please ensure that the relay module is assigned to a server and is running. Testing against an inactive module will have no effect.

Results of the message test can be reviewed in the gwvrelay log files.

Sender address

Recipient address

[Send](#) [Cancel](#)

Host server: Select the server to host the module.

Message queue location: Enter directory of the message queue. Created by default.

Maximum SMTP threads: Default 32.

Delivery targets

Defined domains: Domains defined in Secure Messaging Gateway will have mail routed to their SMTP server. Default disabled.

Relay targets: The relay targets defined in SMTP Relay Target List below. Default enabled.

MX targets: Lookup the MX for the domain and use that. Default disabled.

SMTP Relay Target List

Host Address: Enter the IP address of the SMTP relay target server.

Auth: Select the authorization required by the SMTP relay:

none

auto

plain

login

cram-md5

Auth Username: Enter the SMTP username, if required.

Auth Password: Enter the SMTP password, if required.

Security: Select the security protocol:

none

auto

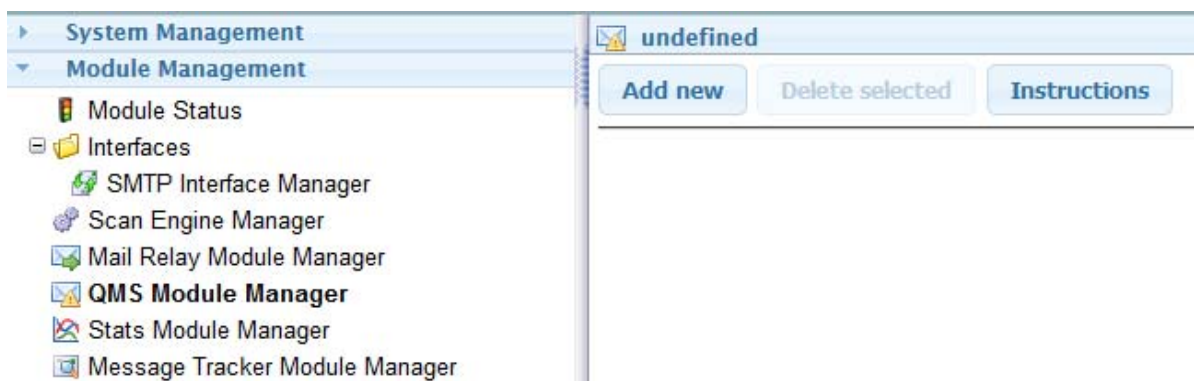
tls

ssl

Priority: 1 is highest priority. Default 1.

QMS Module Manager

The QMS manager allows for the configuration of multiple QMS systems. This is designed for use with multiple organizations.



The 'Enable Processing' option must be activated or the QMS module will not function.

If a separate Quarantine system is needed for a separate organization, a new QMS may be created to service that organizational unit. To assign a new organization to a new QMS module, the organization must be created first. Once created, the new organization will be available under the 'Serviced OU set' option at the bottom of the configuration window.

A contact address for notifications of the new QMS and notes may be added. If none is added, the default administrator will receive the notifications.

The screenshot shows the 'Manage QMS Modules' interface. At the top, there are three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below these is a section for 'Quarantine service' with a dropdown arrow and a checkbox. The configuration fields are as follows:

Enable processing	<input checked="" type="checkbox"/>
Contact email address	<input type="text"/>
Database	Quarantine
Module root path	qms/data_store/
Notes	<input type="text"/>
Host server	g7-209-49.gwava.com
Fault tolerance priority	1
Serviced OU set	<input checked="" type="checkbox"/> [root]

Enable processing: Default enabled.

Contact email address: Enter an email address. Default, the default administrator will receive notifications.

Database: Select the database. Default Quarantine. Databases can be defined in *System Management | Database Connections*.

Module root path: Default, qms/data_store/

Notes: Enter description of the service.

Host server: Select the host server.

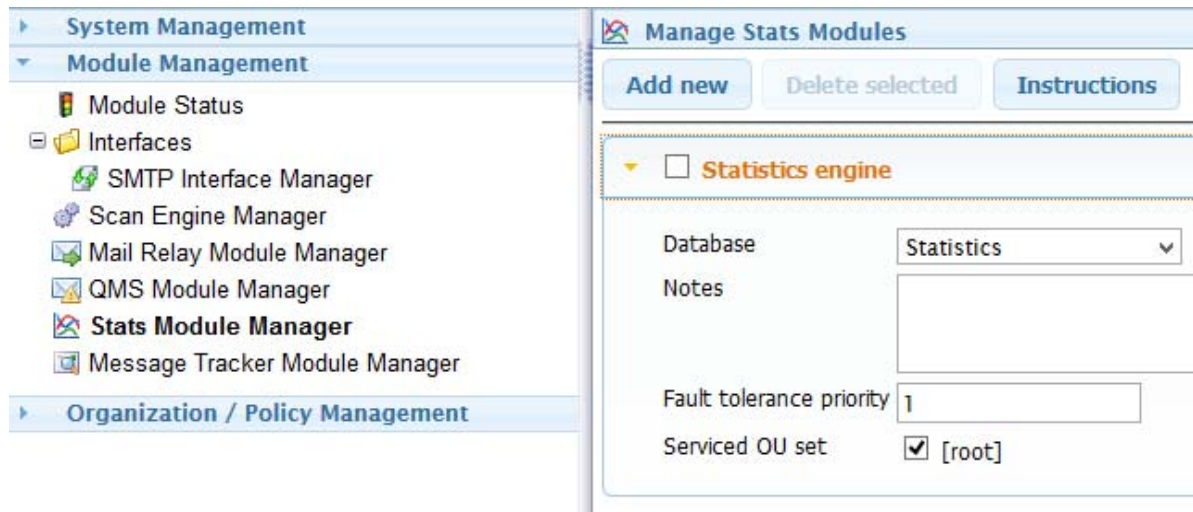
Fault tolerance priority: If there are multiple GWAVA servers if all are at the same priority they will share through round-robin. If at different priorities they are utilized from highest to lowest as they are fully loaded. Highest 1. Default 1.

Serviced OU set: Enable OUs to be serviced.

Stats Module Manager

The Stats Module Manager provides options to configure the statistics engine. This is designed for use with multiple organizations.

If statistics are to be kept separate from different Organizations, the Stats Module Manager provides that option. Before a different organization can be configured to record statistics separately, the organization must first be created. Afterwards, a new statistics module can be created and the organization selected from the 'Serviced OU set' option.



The screenshot shows the 'Stats Module Manager' configuration window. On the left, a navigation pane lists 'System Management' > 'Module Management' > 'Stats Module Manager'. The main area is titled 'Manage Stats Modules' and has three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below these is a section for 'Statistics engine' with a checkbox. The configuration fields are: 'Database' (dropdown menu set to 'Statistics'), 'Notes' (text area), 'Fault tolerance priority' (input field with '1'), and 'Serviced OU set' (checkbox checked, with '[root]' next to it).

Database: Select database to use. Default Statistics. Databases can be defined in *System Management | Database Connections*.

Notes: Enter description.

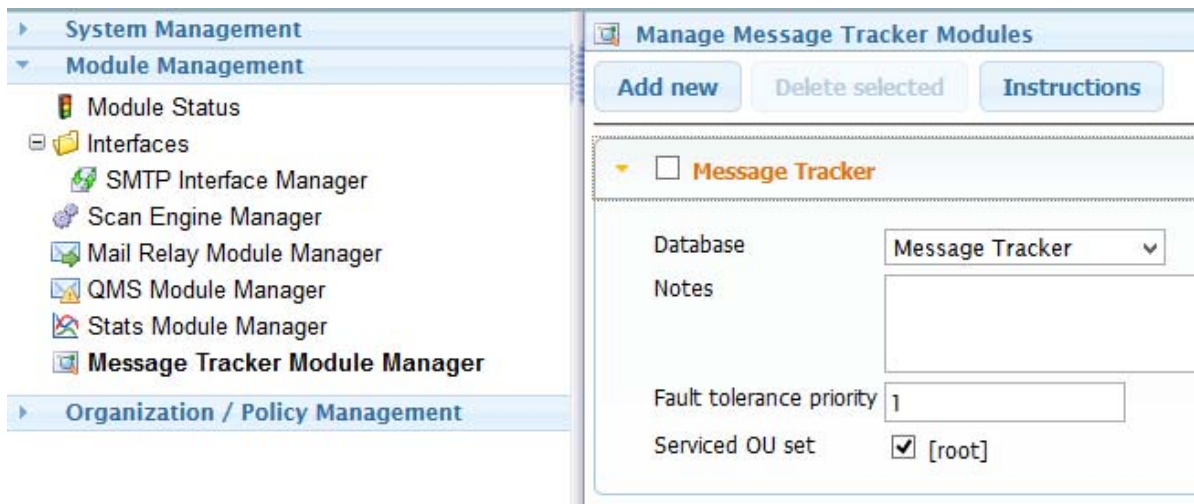
Fault tolerance priority: If there are multiple GWAVA servers if all are at the same priority they will share through round-robin. If at different priorities they are utilized from highest to lowest as they are fully loaded. Highest 1. Default 1.

Serviced OU set: Enable OUs to be serviced.

Message Tracker Module Manager

The Message Tracker Module Manager provides options to configure the message tracker service. This is designed for use with multiple organizations.

If message tracking information should to be kept separate from different Organizations, the Message Tracker Module Manager provides that option. Before a different organization can be configured to record message tracker information separately, the organization must first be created. Afterwards, a new message tracker module can be created and the organization selected from the 'Serviced OU set' option.



Database: Select database to use. Default Message Tracker. Databases can be defined in *System Management | Database Connections*.

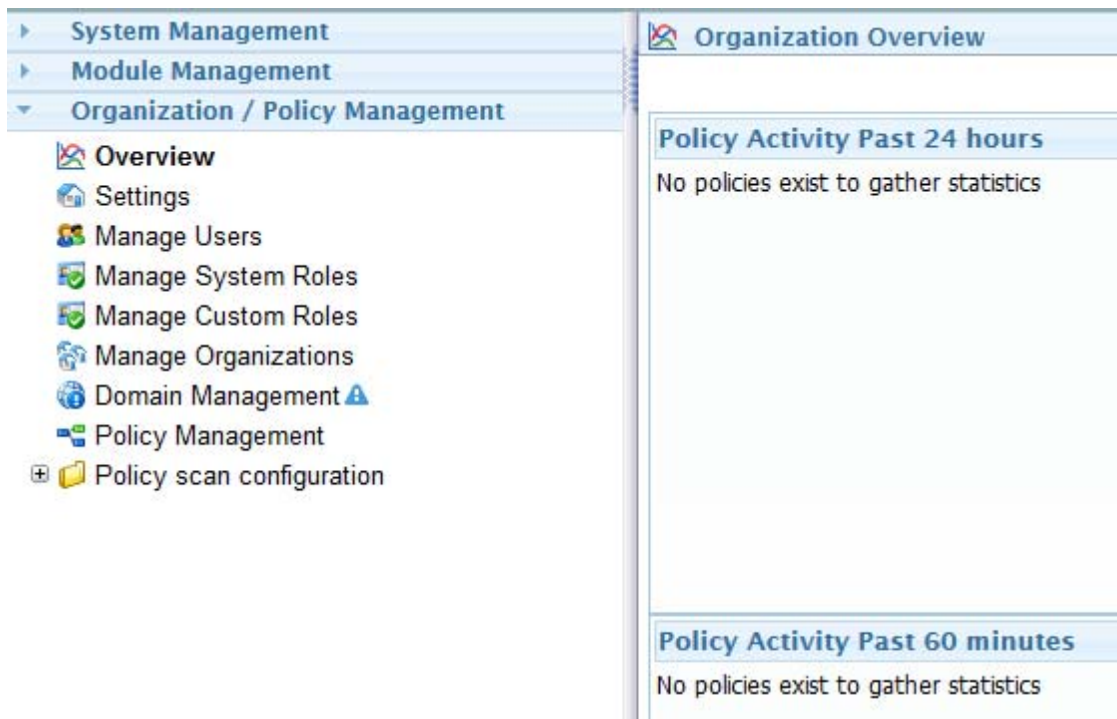
Notes: Enter description.

Fault tolerance priority. If there are multiple Micro Focus Secure Messaging Gateway servers if all are at the same priority they will share through round-robin. If at different priorities they are utilized from highest to lowest as they are fully loaded. Highest 1. Default 1.

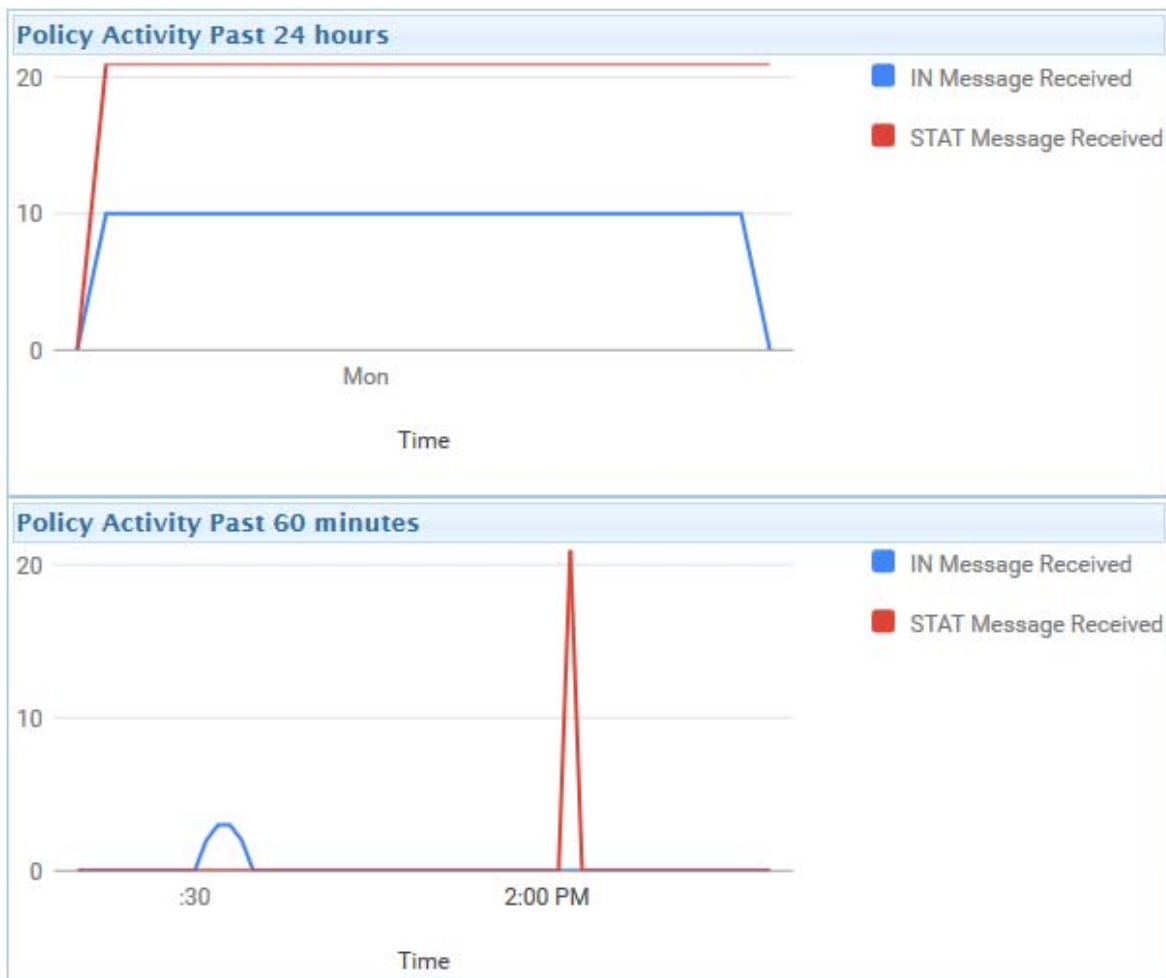
Served OU set: Enable OUs to be serviced.

Organization / Policy Management Overview

If you have a statistics policy enabled you will be able to see policy activity over the past 60 minutes and 24 hours. Initially there will be no statistical information until a policy with statistics recording services is created.



Once a domain, at least one policy with [statistics recording \(Creating_a_Statistics_and_Tracking_Policy.htm\)](#) configured, and mail flowing through the system, then data will be gathered and displayed in the Overview panel.



Settings

Organizational unit settings can be set or viewed here.

<ul style="list-style-type: none"> System Management Module Management Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management Policy Management Policy scan configuration 	<p>Organization Settings</p> <p>Administrator email address <input type="text"/></p> <p>New child OU template <input type="text" value="[no template]"/></p> <p>Message tracking data retention days <input type="text" value="30"/></p> <p>Attached interfaces SMTP Interface</p> <p>Attached scan engines Message filter engine</p> <p>Attached statistics service Statistics engine</p> <p>Attached quarantine service Quarantine service</p> <p>Account details are not configured for this organizational unit.</p>
--	---

Administrator email address: Enter the Administrator's email address for receiving messages.

New child OU template: Select a template for new child organizational units. Templates are defined under *System Management | Templates*.

Message tracking data retention days: Enter the number of days to keep message tracking data. Default, 30.

Attached interfaces: List of interfaces attached to this organization.

Attached scan engines: List of scan engines attached to this organization.

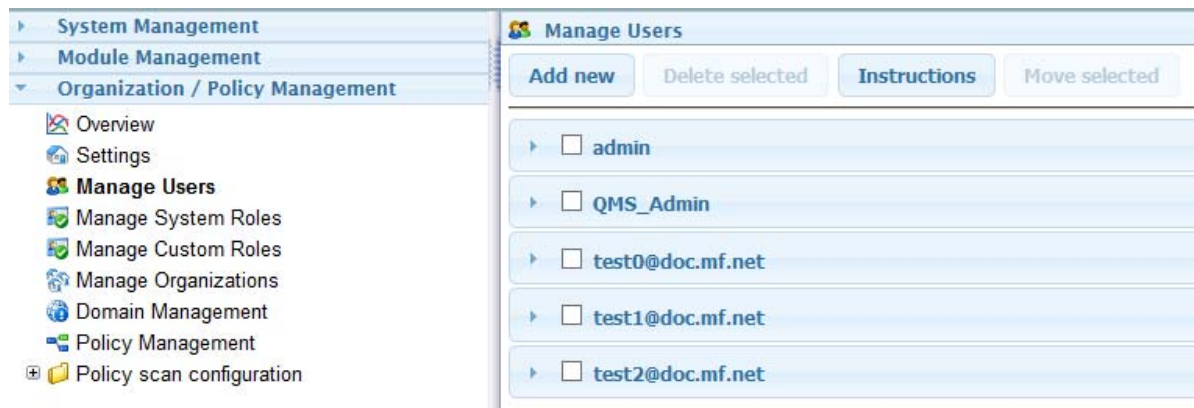
Attached statistics service: The statistics service attached to this organization.

Attached quarantine service: The quarantine service attached to this organization.

Manage Users

The Manage Users window allows administrators to manage users in the system. User creation, removal, roles, and moving between organizational units etc. is accomplished here.

The user list will popular with users that have logged into their quarantine. These users can also be granted additional rights.



Role membership defines what a User is allowed to do. For example, user test1 has showed themselves to be responsible and are granted the role QMS Administrator to manage the quarantine while the system administrator takes a much deserved vacation.

Manage Users

admin
 QMS_Admin
 test0@doc.mf.net
 test1@doc.mf.net

Last login: Tue, 13 Jun 2017 15:55:07 -0600 from 137.65.60.85
Enabled:
Management:
Password:
Contact email:

Role Membership

Message Tracker
 OU Supervisor
 Policy Administrator
 Policy User
 QMS Administrator
 QMS User
 System Administrator

Last login: Shows the last login with date stamp and IP address.

Enabled: Login for this user can be disabled. Default, enabled.

Management: Set the level the user can manage: *System* or *Domain provisioning*. Default, system.

Password: To change a password, specify the new password in the field provided and then save the changes.

Contact email: Enter the email address used for this user.

Role Membership: Select the role memberships the user will be able to access when the user logs in.

Message Tracker: Allows access to message tracker interface.

OU Supervisor: Allows management of organizational units..

Policy Administrator: Allows management of policies.

Policy User: Allows use of policies.

QMS Administrator: Allows management of quarantine management system and access to others quarantines.

QMS User. Allows access to their own quarantine mailbox.

System Administrator. Allows full access.

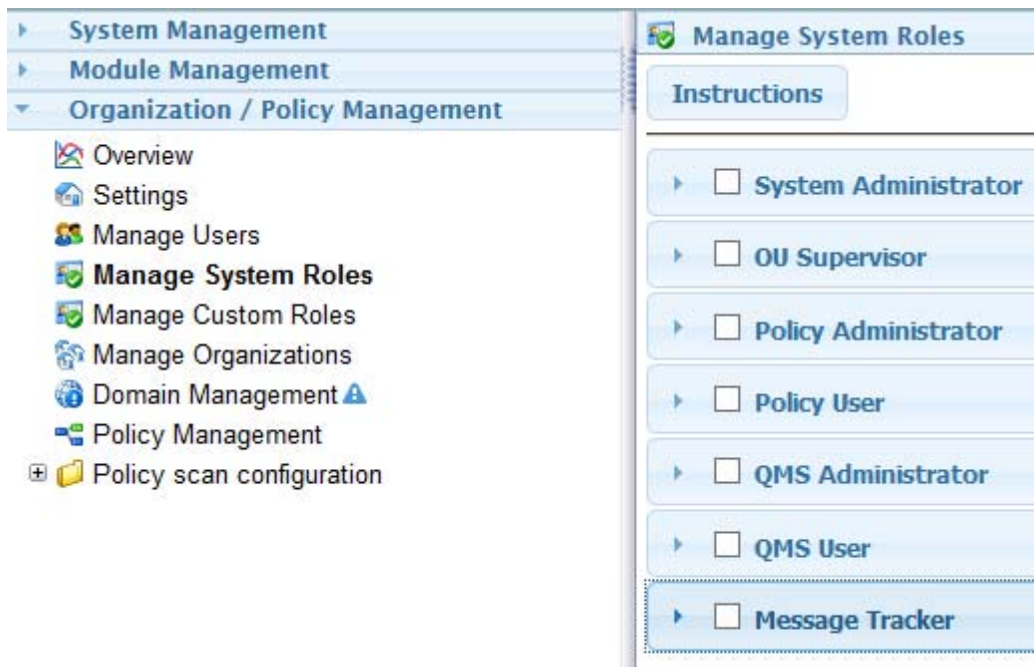
Manage System roles

Roles provide access to features of the Micro Focus Secure Messaging Gateway system to users, and controls the actions of role dependent features found throughout the system. System roles are predefined and cannot be edited, added or removed.

Importantly for systems that utilize the multi-tenant functionality of Micro Focus Secure Messaging Gateway, system roles must be inherited from the root level of the system. If a role is not made available to a child OU, none of the deeper OU's can access the role. See custom roles for this functionality. The main system user interface interacts with these roles to determine which menu items users may access.

Role Members All users within the OU will be listed here. Assign users to the role by selecting the checkbox.

Assigned User Interfaces The available user interfaces for the OU will be listed here. When users log in to the management console, the combined list of user interfaces that are associated by role membership are used to determine how a user will be logged in to the system. If a user is assigned a single user interface, they are automatically presented with that interface. When multiple user interfaces are discovered, the user is presented with an option to select the UI to use.



Roles

There are a number of predefined roles:

System Administrator

OU Supervisor

Policy Administrator

Policy User

QMS Administrator

QMS User

Message Tracker

Within each role, membership and interface is assigned. User interfaces are defined in *System Management | User Interfaces*.

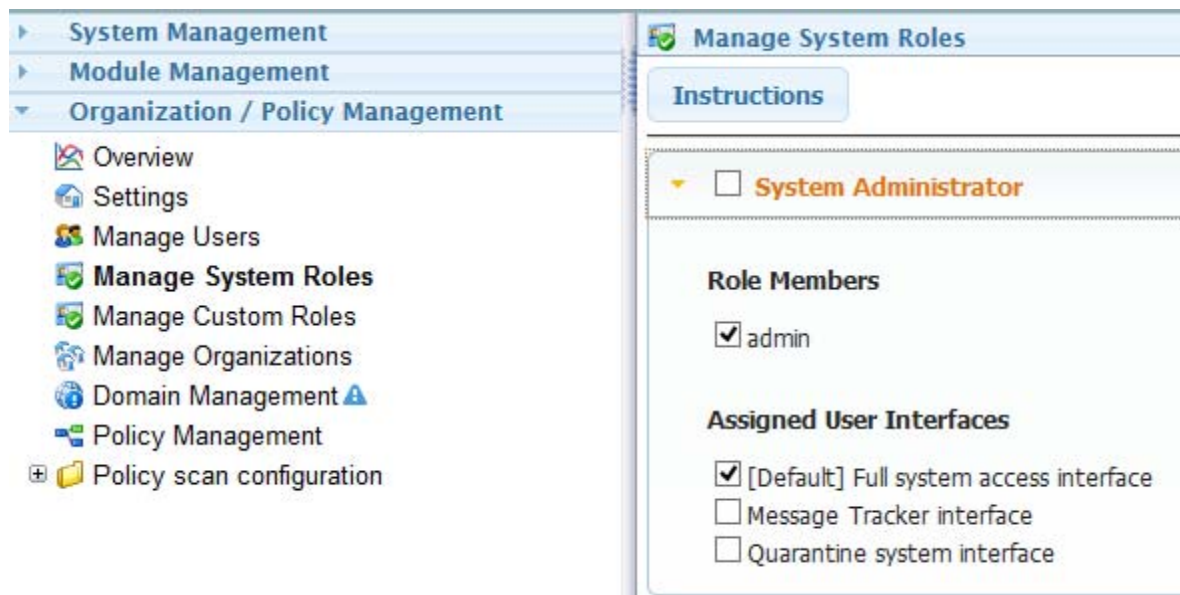
Role Members admin [User]. Added to all by default. Additional users can be enabled after being added in *Organization/Policy Management | Manage Users*.

Assigned User Interfaces [Default] Full system access interface

Message Tracker interface

Quarantine system interface

System Administrator



OU Supervisor

<ul style="list-style-type: none"> ▶ System Management ▶ Module Management ▼ Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management ⚠ Policy Management Policy scan configuration 	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Manage System Roles</p> <p>Instructions</p> <hr/> <ul style="list-style-type: none"> ▶ <input type="checkbox"/> System Administrator ▼ <input type="checkbox"/> OU Supervisor <hr/> <p>Role Members</p> <p><input type="checkbox"/> admin</p> <p>Assigned User Interfaces</p> <p><input checked="" type="checkbox"/> [Default] Full system access interface</p> <p><input type="checkbox"/> Message Tracker interface</p> <p><input type="checkbox"/> Quarantine system interface</p> </div>
--	---

Policy Administrator

<ul style="list-style-type: none"> ▶ System Management ▶ Module Management ▼ Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management ⚠ Policy Management Policy scan configuration 	<div style="border: 1px solid #ccc; padding: 5px;"> <p>Manage System Roles</p> <p>Instructions</p> <hr/> <ul style="list-style-type: none"> ▶ <input type="checkbox"/> System Administrator ▶ <input type="checkbox"/> OU Supervisor ▼ <input type="checkbox"/> Policy Administrator <hr/> <p>Role Members</p> <p><input type="checkbox"/> admin</p> <p>Assigned User Interfaces</p> <p><input checked="" type="checkbox"/> [Default] Full system access interface</p> <p><input type="checkbox"/> Message Tracker interface</p> <p><input type="checkbox"/> Quarantine system interface</p> </div>
--	--

Policy User

<ul style="list-style-type: none"> ▶ System Management ▶ Module Management ▼ Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management ⚠ Policy Management Policy scan configuration 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #e6f2ff; padding: 2px;">Manage System Roles</div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="background-color: #e6f2ff; padding: 2px; border-radius: 3px;">Instructions</div> <hr/> <ul style="list-style-type: none"> ▶ <input type="checkbox"/> System Administrator ▶ <input type="checkbox"/> OU Supervisor ▶ <input type="checkbox"/> Policy Administrator ▼ <input type="checkbox"/> Policy User <hr/> <p>Role Members</p> <ul style="list-style-type: none"> <input type="checkbox"/> admin <p>Assigned User Interfaces</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> [Default] Full system access interface <input type="checkbox"/> Message Tracker interface <input type="checkbox"/> Quarantine system interface </div> </div>
--	--

QMS Administrator

<ul style="list-style-type: none"> ▶ System Management ▶ Module Management ▼ Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management ⚠ Policy Management Policy scan configuration 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #e6f2ff; padding: 2px 5px;">Manage System Roles</div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="background-color: #e6f2ff; padding: 2px 5px; border-radius: 3px;">Instructions</div> <hr/> <ul style="list-style-type: none"> ▶ <input type="checkbox"/> System Administrator ▶ <input type="checkbox"/> OU Supervisor ▶ <input type="checkbox"/> Policy Administrator ▶ <input type="checkbox"/> Policy User ▼ <input type="checkbox"/> QMS Administrator <hr/> <p>Role Members</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> admin <p>Assigned User Interfaces</p> <ul style="list-style-type: none"> <input type="checkbox"/> [Default] Full system access interface <input type="checkbox"/> Message Tracker interface <input checked="" type="checkbox"/> Quarantine system interface </div> </div>
--	---

QMS User

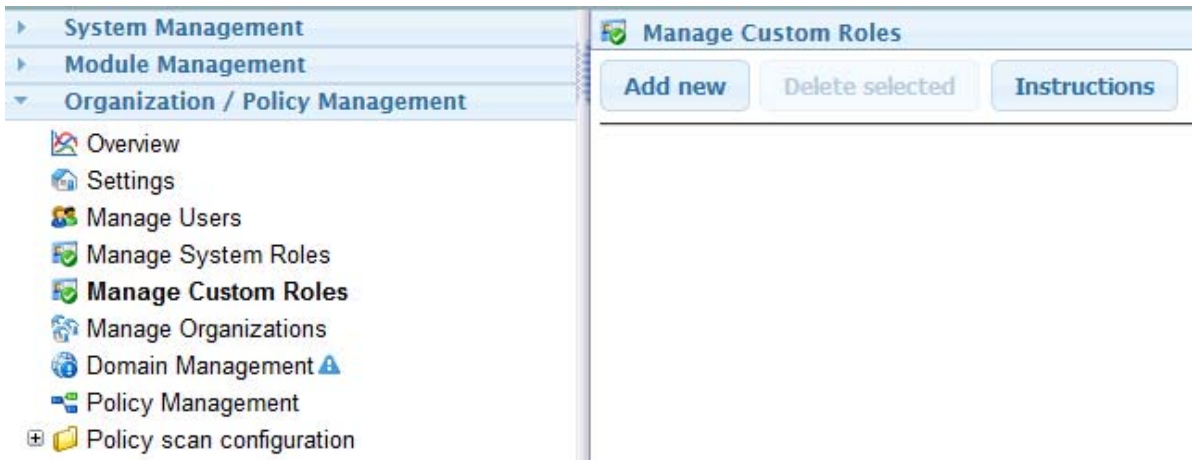
<ul style="list-style-type: none"> ▶ System Management ▶ Module Management ▼ Organization / Policy Management <ul style="list-style-type: none"> Overview Settings Manage Users Manage System Roles Manage Custom Roles Manage Organizations Domain Management ⚠ Policy Management Policy scan configuration 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #e6f2ff; padding: 2px 5px; border: 1px solid #add8e6;"> Manage System Roles </div> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 5px;"> <p style="background-color: #e6f2ff; padding: 2px 5px; border: 1px solid #add8e6; border-radius: 3px;">Instructions</p> <hr/> <ul style="list-style-type: none"> ▶ <input type="checkbox"/> System Administrator ▶ <input type="checkbox"/> OU Supervisor ▶ <input type="checkbox"/> Policy Administrator ▶ <input type="checkbox"/> Policy User ▶ <input type="checkbox"/> QMS Administrator ▼ <input type="checkbox"/> QMS User <hr/> <p>Role Members</p> <ul style="list-style-type: none"> <input type="checkbox"/> admin <p>Assigned User Interfaces</p> <ul style="list-style-type: none"> <input type="checkbox"/> [Default] Full system access interface <input type="checkbox"/> Message Tracker interface <input checked="" type="checkbox"/> Quarantine system interface </div> </div>
--	--

Message Tracker

The screenshot displays the 'Manage System Roles' configuration page. On the left, a navigation menu is expanded to 'Organization / Policy Management', showing options like Overview, Settings, Manage Users, **Manage System Roles**, Manage Custom Roles, Manage Organizations, Domain Management, and Policy Management. The main panel is titled 'Manage System Roles' and contains an 'Instructions' button. Below this is a list of roles, each with a checkbox: System Administrator, OU Supervisor, Policy Administrator, Policy User, QMS Administrator, QMS User, and **Message Tracker** (highlighted in orange). Under the 'Message Tracker' role, there are two sections: 'Role Members' with a checked checkbox for 'admin', and 'Assigned User Interfaces' with checked checkboxes for 'Message Tracker interface' and 'Quarantine system interface'.

Manage Custom Roles

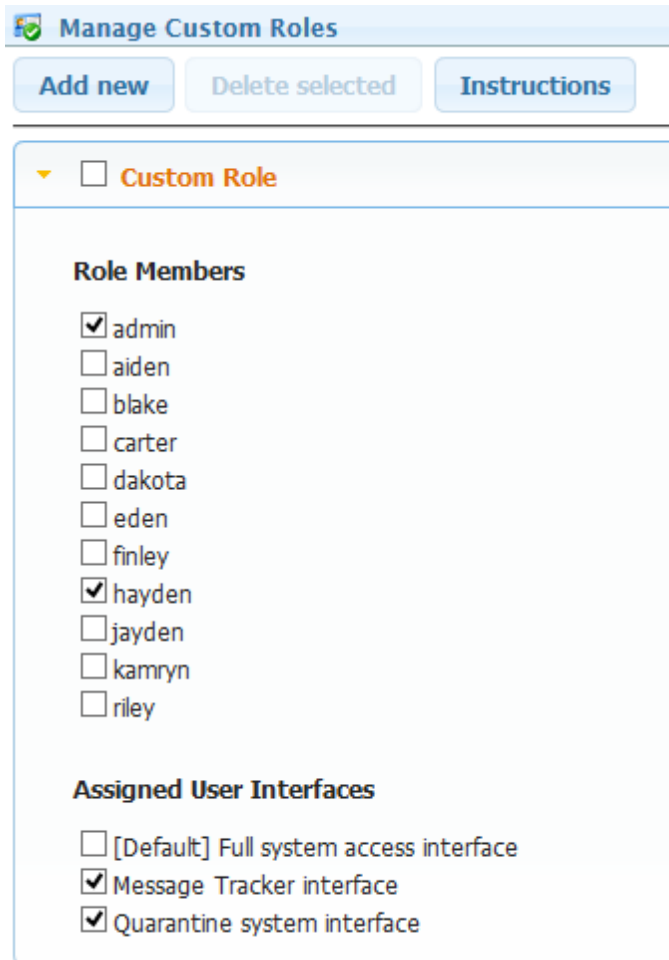
Roles provide access to features of the Micro Focus Secure Messaging Gateway system to users, and controls the actions of role dependent features found throughout the system. Custom roles allow creation of customized roles at any level in the Micro Focus Secure Messaging Gateway OU system. Roles created at sub-levels of a multi-tenant system are limited in scope to that branch of the system, and can be selectively passed down to child OU's.



Create Custom Role

New Roles can be created by pressing *Add new*.

Roles can be renamed by clicking on the role name.



Role Members

All users within the OU will be listed here. Assign users to the role by selecting the checkbox. Additional users can be enabled after being added in *Organization/Policy Management | Manage Users*.

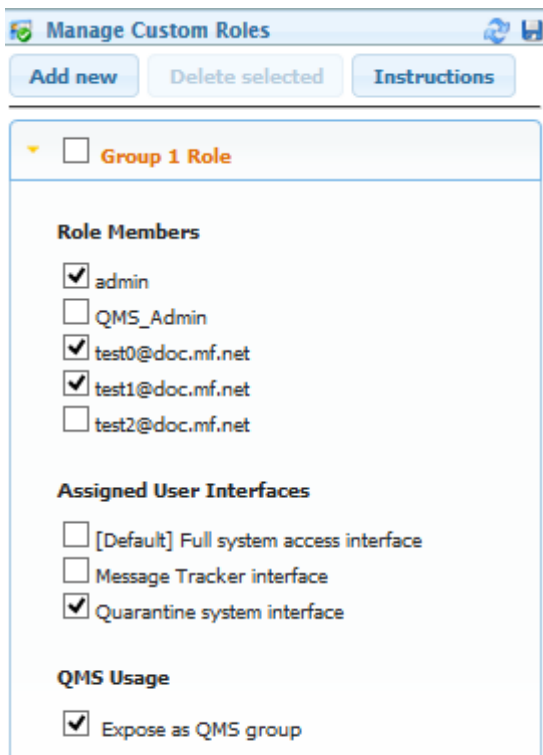
Assigned User Interfaces

The available user interfaces for the OU will be listed here. User interfaces are defined in *System Management | User Interfaces*. When users log in to the management console, the combined list of user interfaces that are associated by role membership are used to determine how a user will be logged in to the system. If a user is assigned a single user interface, they are automatically presented with that interface. When multiple user interfaces are discovered, the user is presented with an option to select the UI to use.

Creating a Group

A Group can be created by adding a new custom role, selecting users and enabling "Expose as QMS group"

1. Select *Add New*
2. Give the new role a name
3. Enable users to be part of the group
4. Enable *Expose as QMS group*



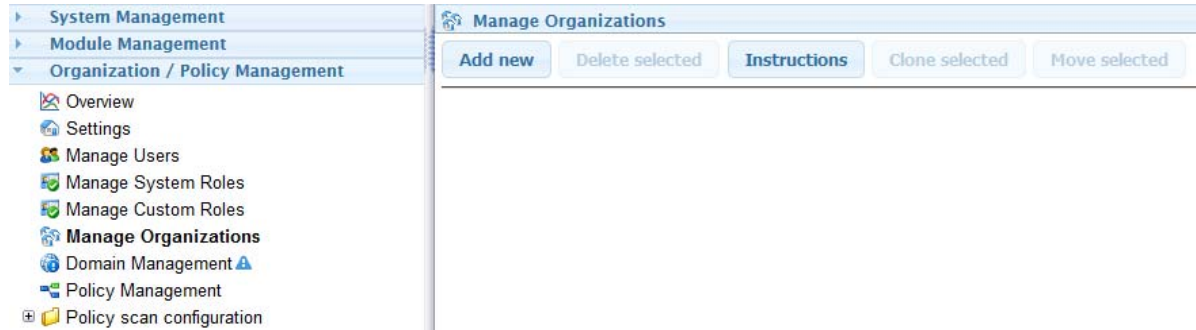
The screenshot shows a web interface titled "Manage Custom Roles" with three buttons: "Add new", "Delete selected", and "Instructions". Below the buttons is a list of roles. The first role, "Group 1 Role", is expanded to show its configuration. The configuration is divided into three sections: "Role Members", "Assigned User Interfaces", and "QMS Usage".

Section	Item	Checked
Role Members	admin	Yes
	QMS_Admin	No
	test0@doc.mf.net	Yes
	test1@doc.mf.net	Yes
	test2@doc.mf.net	No
Assigned User Interfaces	[Default] Full system access interface	No
	Message Tracker interface	No
	Quarantine system interface	Yes
QMS Usage	Expose as QMS group	Yes

Manage Organizations

The Manage Organizations menu is largely for systems that will be filtering mail as a service for other companies, or organizations. This is largely for those who wish to act as an ISP.

Each organization has the ability to be managed with individual policies, interfaces, user limits, expiration dates, roles, exceptions, templates, etc.



To add an organization, select the 'Add New' button and name the organization. Save changes and then configure as desired.

Separate organizations must be created and configured first if scanning is to be provided for a group for which separate quarantine or statistics are to be kept.

Add New

Manage Organizations

▼ **Unnamed organization**

Enabled	<input checked="" type="checkbox"/>
Expires	<input type="checkbox"/>
Expiry date	<input type="text"/>
Enable user limit	<input type="checkbox"/>
User limit	<input type="text" value="1"/>
Force address tracking	<input type="checkbox"/>
Require domain in username	<input type="checkbox"/>
Allow domain patterns	<input checked="" type="checkbox"/>
Require domain validation	<input type="checkbox"/>
Maximum child OU's	<input type="text" value="1000000"/>
Maximum child OU depth	<input type="text" value="100"/>
User interface	<input type="text" value="[Default] Full system access interface"/>
Default child user interface	<input type="text" value="[Default] Full system access interface"/>

▶ **Role Availability**

▶ **Event Availability**

▶ **Service Availability**

▶ **Exception Availability**

▶ **Template Availability**

▶ **User Interface Availability**

Enabled: Default, enabled.

Expires: Default, disabled.

Expiry date: If expiration has been enabled, when the organization will cease to operate.

Enable user limit: Default, disabled.

User limit: Limit number of users. Default 1.

Force address tracking: Default, disabled.

Require domain in username: Default, disabled.

Allow domain patterns: Default, enabled.

Require domain validation: Default, disabled.

Maximum child OUs: Default, 1000000.

Maximum child OU depth: Default, 100.

User interface: Select the main user interface. User interfaces are defined in *System Management | User Interfaces*.

Default child user interface: Select the user interface any child OUs will use by default.

Role Availability

Select the roles available to the OU. Roles are defined in *Organization / Policy Management | Manage System Roles*.

Message Tracker

OU Supervisor

Policy Administrator

Policy User

QMS Administrator

QMS User

System Administrator

Event Availability

Select the events available to the OU.

Anti-Spam

Anti-Virus

Attachment Name

Attachment Size

Black List

Email Address

Filter Group

Fingerprint

Image Analyzer

IP Address

IP Reputation

Message Received

Message Size

Message Text

RBL
SMTP Envelope
SPF
SURBL
Zero Hour Virus

Service Availability

Select the services available to the OU.

Add Header Line
Admin Quarantine
Block
Carbon Copy
Event Writer
Interface Control
Message Signature
Message Tag
Message Tracker
Notify
Quarantine
Quarantine Control
Statistics Recorder

Exception Availability

Select the exceptions available to the OU.

Email Address
Exception Group
IP Address
Message Text
SMTP Envelope
White List

Template Availability

Select the templates available to the OU. User interfaces are defined in *System Management / Templates*.

Digest
Forward From Quarantine

- Notify Generic
- Notify Recipients
- Notify Sender
- System alert
- System notification

User Interface Availability

Select the user interfaces available to the OU. User interfaces are defined in *System Management / User Interfaces*.

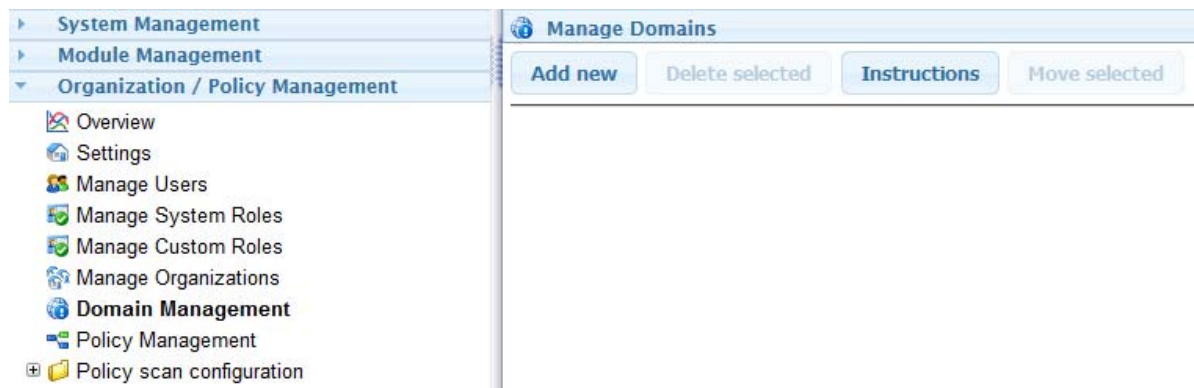
[Default] Full system access interface

Message Tracker interface

Quarantine system interface

Domain Management

Micro Focus Secure Messaging Gateway may manage messages coming from multiple domains. Each domain to be managed by Micro Focus Secure Messaging Gateway must be added to the Domain Management for it to function and have message data scanned by Micro Focus Secure Messaging Gateway.



Adding domains to the Micro Focus Secure Messaging Gateway server is simple: Select the 'Add new' button and input the new domain and select the 'save' disk button at the top right of the Manage Domains page.

Once added, domain options may be configured and managed. The SMTP hosts and any LDAP hosts must be specified for logins and scanning to be completed properly.

Add New

microfocus.com

Enable user auto-provisioning

Auto-provision roles

- (QMS) default (G6 import)
- (QMS) users (G6 import)
- System Administrator
- OU Supervisor
- Policy Administrator
- Policy User
- QMS Administrator
- QMS User
- Message Tracker

Additional Host Pattern Matches

SMTP Hosts

Target type: SMTP server

Target host	Priority	Security	Authentication	Username	Password	Mail	Auth	Line limit
mail.qa.gwava.com	1	none	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8000
*	1	none	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000

LDAP Hosts

Target host	Priority	Security	Username	Password	Auth	Validate	Scope	DN template / DN search base	Search pattern
*	1	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	template		

DKIM Signing

Domain	Selector
*	20171003

Notes

Enabling LDAP for Users Logging into QMS

Using an LDAP browser to confirm that the LDAP server can be successfully accessed is highly recommended. For example, Softerra LDAP Browser.

- ◆ Enter the LDAP server address as the Target Host.
- ◆ Provide the Distinguished Name and password of the user that has access to authenticate the other users.
- ◆ Enable Auth.
- ◆ Enter the DN Search base for the domain.
- ◆ If using proxy addresses or if the users are in a different location than the default, in the Search pattern enter: `((mail=%email%)(proxyAddresses=smtp:%email%))`

LDAP Hosts

Target host	Priority	Security	Username	Password	Auth	Validate	Scope	DN template / DN search base	Search pattern
151.155.183.142	1	none	cn=alpha	*****	<input checked="" type="checkbox"/>	<input type="checkbox"/>	sub tree	dc=sf,dc=gwava,dc=net	((mail=%email%)(prox
	1	none			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	template		

Options

Enable user auto-provisioning: Default, disabled.

Auto-provision roles

Roles are defined in *Organization / Policy Management | Manage System Roles*.

System Administrator

OU Supervisor

Policy Administrator

Policy User

QMS Administrator

QMS User

Message Tracker

Additional Host Pattern Matches

Enter the IP address range or host names with wildcards of appropriate hosts.

SMTP Hosts

Enter the SMTP messages will be directed to.

Target type

SMTP server

Discard

Target host

Priority

Security

Authentication

Username

Password

Mail

Auth

Line limit

LDAP Hosts

Enter the LDAP to authenticate against.

Target host: The IP Address of the LDAP server used for user authentication.

Priority

Security

Username: The username is the Distinguished Name of the user used to allow LDAP access. For example: CN=dapple ldap,CN=Users,DC=sf,DC=gwava,DC=net

Password

Auth

Validate

Scope

DN template / DN search base: The search base is the distinguished name of the domain.

For example: DC=sf,DC=gwava,DC=net

Search pattern: If using proxy addresses or if the users are in a different location than the default, in the Search pattern enter: ((mail=%email%)(proxyAddresses=smtp:%email%))

DKIM Signing

Domain: Enter the domain that emails will be signed from. Once a domain is entered, additional functionality is revealed.

Domain	Selector	
doc.mf.net	20171003	Public Key
	20171003	Create Keys
		Upload Keys

Selector: An identifier that will be used in your DNS for the signing. This can be anything, by default it is today's date.

Public Key button: This button will reveal your public key, once it has been created or uploaded. The public key is provided in a format suitable for inclusion in DNS configuration files. If your DNS is hosted by a 3rd party, you should create a TXT record for your domain and copy the data portion of the record, removing quotes and spacing within the base64 portion of the data.

```
20171003._domainkey IN TXT ( "v=DKIM1; k=rsa; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsBgKRxlt5FsetvBRRsHN9GUtyiibmbfNwhlw
qrtAY/O3Nv8AlZE8FFqb9doztZ/ktU155ZGoRX
/TpMrWInhd47qXVf7z6Wz8tZsIF5w0uvJcWxOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69G1op
/HkeWyStjkk7nVHRXDprUY1/OXSuHFGID1BK+Ci3yMN98qRcFzWS+kyWj "
"g44Gt79X2Oh/qv1ESLo4SGdNQtb0VxwGFJ6kp0LLP2EJBqiBaWtYOAxrz9Kf2hvVCF6uhRV4iyzd5o9Irw
edkIx7QyYdGu7cI+blh9bVd6VxuzX7gxxV722iYewAlh5iJBAAd7jwIDAQAB" ) ; ----- DKIM key
20171003 for doc.mf.net
```

Create Keys button: This button will create a set of private and public keys for DKIM signing.

Upload Keys button: If you already have keys you wish to use, they can be uploaded here. A dialog box will appear.

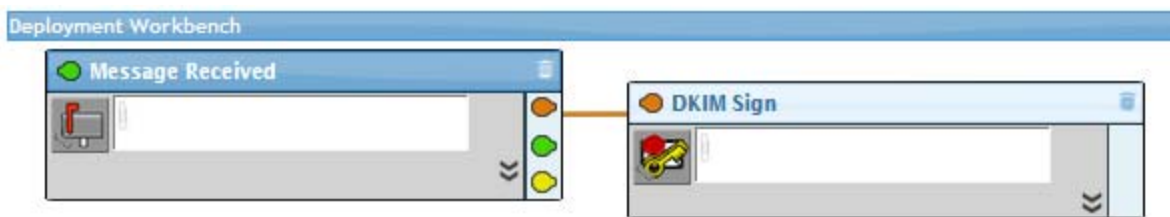


Setting up DKIM Signing: DKIM signing is a DNS function.

1. After setting up the public key, you will have to create a new TXT record in your DNS that Secure Messaging Gateway will use to sign each message. The DNS TXT record is required to be of the form <selector>._domainkey.<domain>. For example, the TXT record for the above screenshot would be *20171003._domainkey.doc.mf.net*.

2. The content of the TXT record is the key within the parentheses {}. For example, using the example above, you would copy into the TXT record: "v=DKIM1; k=rsa; s=email; " "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsBgKRxlt5FsetvBRRsHN9GUTyIibmbfNwh1wqrtAY/O3Nv8AlZE8FFqb9doztZ/ktU155ZGoRX/TpMrWInhd47qXVf7z6Wz8tZsIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69G1op/HkeWyStjkk7nVHRXDprUY1/0XSuHFGTD1BK+Ci3yMN98qRcFzWS+kyWj" "g44Gt79XZOh/qv1ESLo4SGdNQtb0VxwGFJ6kp0lLP2EJBqiBaWtYOArz9Kf2hvVCF6uhRV4iyzd5o9IrwedkIx7QyYdGu7cI+blh9bVd6VxuzX7gxxV722iYewAlh5iJBAA7jwIDAQAB"

3. Finally, you need to create a DKIM signing service in Secure Messaging Gateway, either in an existing policy or in its own policy.



4. To verify that this worked send a message from the domain that is DKIM signing to an external domain. The DKIM signature should be added to the message.

Notes

Enter any notes about the domain.

Policy Management

Policies define the entry point for messages to be filtered within your organization. To scan messages, at least one policy must be defined.



Policies can be created either automatically with *Add with wizard* or manually with *Add new*.

After policies have been created, configuration of scanning functionality is accessed from the 'Policy scan configuration' folder in the navigation panel.

Multiple policies may be created to direct messages into different scan configurations. This separation is performed by policy qualifications, which will check a set of message attributes to determine if the message should be scanned by the policy. For example, to create separate policies for inbound and outbound mail, two policies would be created, each having the 'Scan by message direction' qualification and the appropriate direction enabled. As messages pass through the system, the policy manager will determine the correct policy to use.

On the right side of the policy title bars are sorting arrows. To change the order of the policies, press the appropriate arrow to move a policy up or down. Messages are tested against policies in order from top to bottom. In complex multi-policy layouts, order can be important and will determine which policy a message will be scanned by. For example, a policy for messages over a certain size could be placed at the top of the policy list, followed by a generic policy. With this order, the generic policy would only be chosen when the size limit is not exceeded.



After policies are created here they can be configured by choosing the policy to be configured under Policy Scan Configuration.

Manual Policy Creation

Policies can be created manually and by selecting items more options are revealed.

Manage Policies 🔄 📄

Basic Policy
⬆ ⬇ ⬆

Enabled
 Scan by message direction
 Handle inbound mail
 Handle outbound mail
 Handle internal mail
 Limit by source address
 Invert address list
 Match address list

Limit by recipient address
 Invert address list
 Match address list

Limit by sender IP address
 Invert address list
 Match address list

Limit by message size
 Minimum message size
 Maximum message size
 Message size test will not be applied when no selections are enabled

Limit by interface type
 Invert interface type list
 Matched interface types [type list]

Limit interface
 Invert interface list
 SMTP Interface

Limit by processing server
 Invert server list
 SF145.gwava.com

Scan archives by default
 Maximum archive scan depth
 Maximum archive files
 Notes

Enabled: Default, checked

Scan by message direction

Handle inbound mail

Handle outbound mail

Handle internal mail

Limit by source address

Invert address list: Reverses the effect of the listed items.

Match address list

Limit by recipient address

Invert address list: Reverses the effect of the listed items.

Match address list

Limit by sender IP address

Invert address list: Reverses the effect of the listed items.

Match address list

Limit by message size

Minimum message size

Maximum message size

Limit by interface type

Invert interface type list: Reverses the effect of the listed items.

Matched interface types [type list]

Limit interface

Invert interface list: Reverses the effect of the listed items.

[Available interfaces]

Limit by processing server

Invert server list: Reverses the effect of the listed items.

[Processing server name]

Scan archives by default: Default, enabled. This will decompress and scan compressed attachments including ZIP, GZ, and TAR.

Maximum archive scan depth: Default, 6.

Maximum archive files: Default, 1000.

Notes: Store notes about the policy.

Policy Scan Configuration

The Policy Scan Configuration folder provides access to the mail filter policies created in Policy Management.

From here each policy can be accessed and customized with filters, services and exceptions.

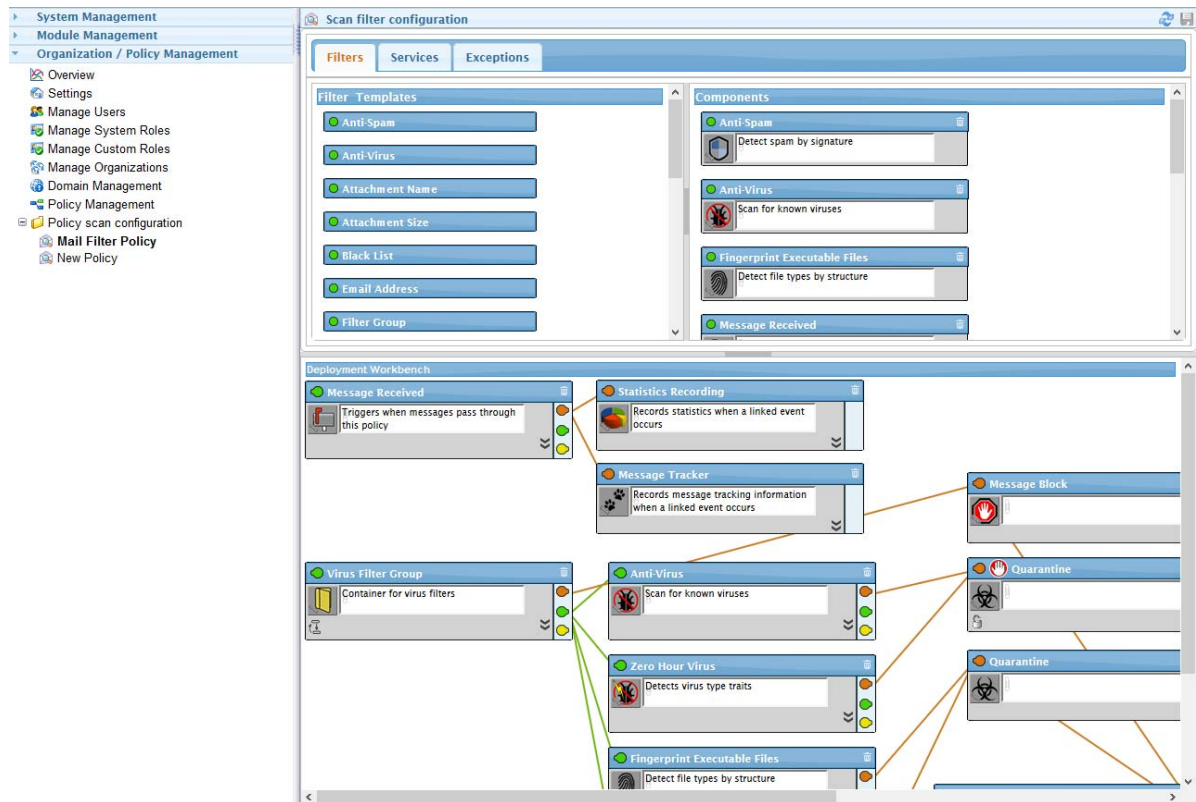
Filters scan messages passing through the system. Any message entering a policy will trigger all filters that are part of the policy.

Services are actions to be taken when a filter catches a message.

Exceptions provide a bypass to the service action taken.

For example. An Attachment Name filter can be set to trigger on attachments named "GreatDeal.zip" because it usually isn't but does not contain a virus and isn't spam, but it is part of marketing emails that the overly enthusiastic marketing company your company contracts sends all the time. The Block service can be used to keep message this from going to all the users, but an exception is made for the VP of Sales so they know what is happening.

Select a policy to view the configuration workbench. A wizard created policy will have Filters and Services in place by default. Manually created policies will need them added.



Drag items from the Template panel to the Workbench panel.

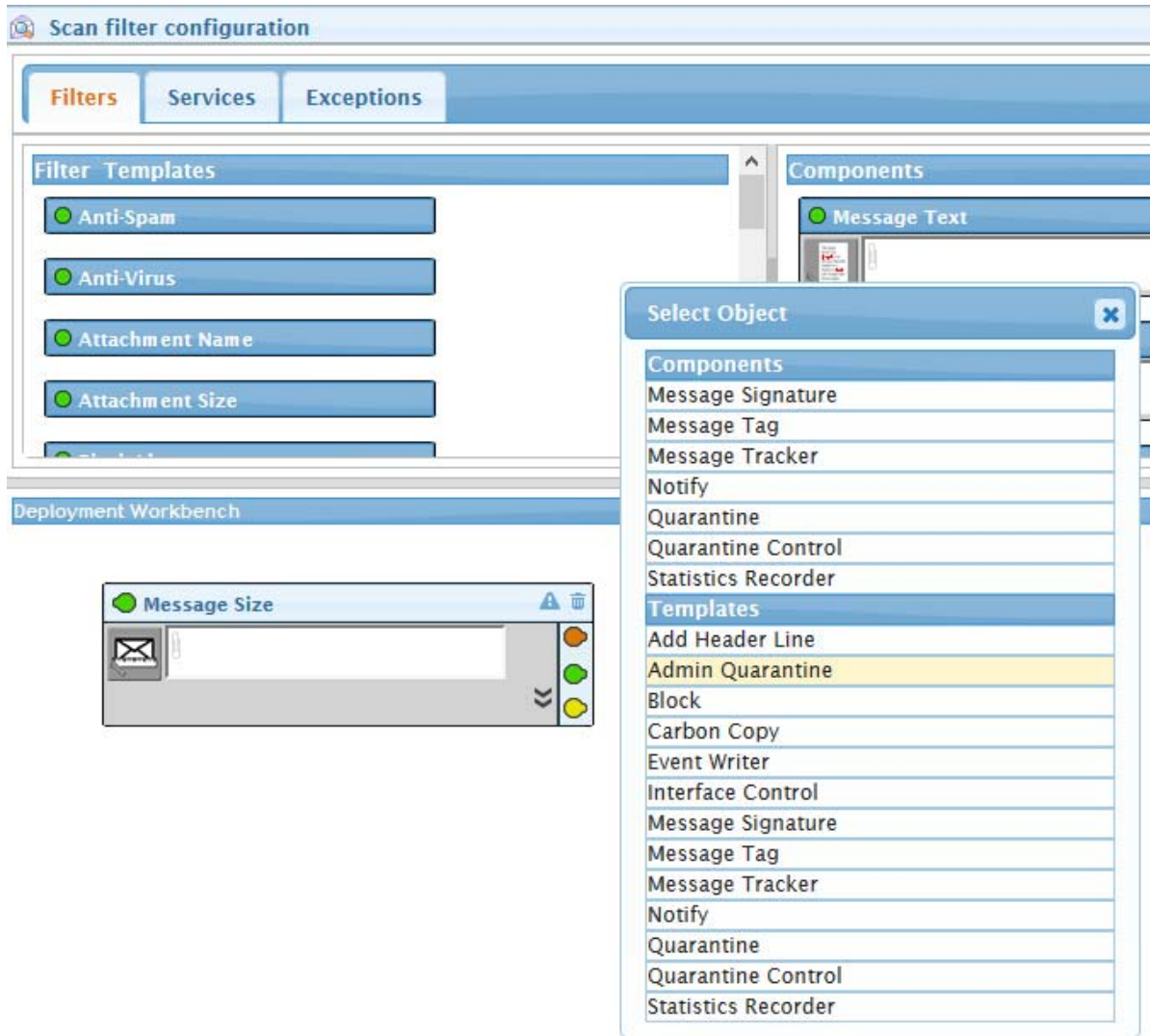
Connect items together by clicking and dragging the colored pin to the appropriate destination.

Red pins on Filters go to *Red titles* on Services.

Green pins on Filters go to *Green titles* on Filter Groups.

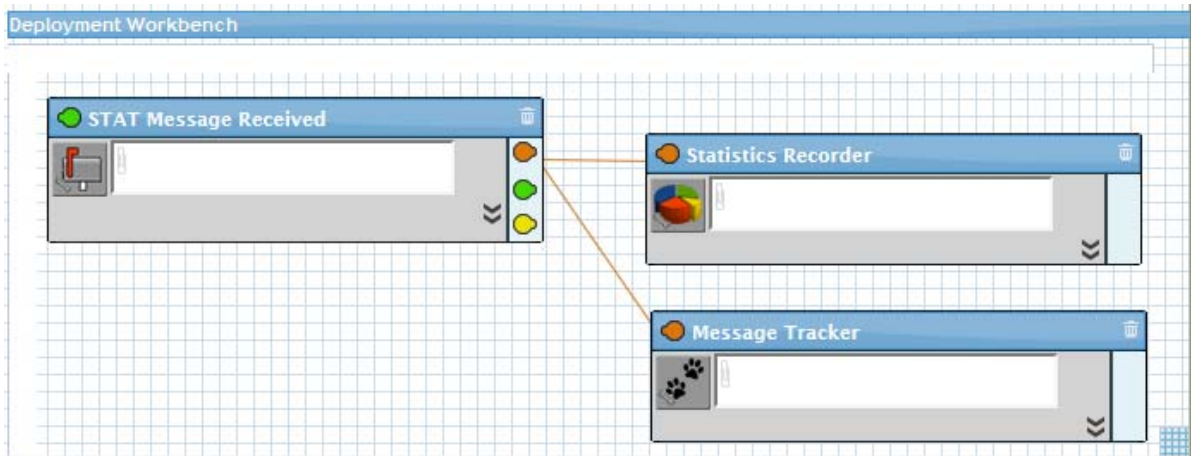
Yellow pins on Filters go to *Yellow titles* on Exceptions.

Alternatively, drag the pin and release over the white space to have a menu of allowed items appear



The workbench can be navigated with click and drag. Links between nodes will highlight as the mouse hovers over each node. Ctrl-click to select multiple nodes and highlight their links

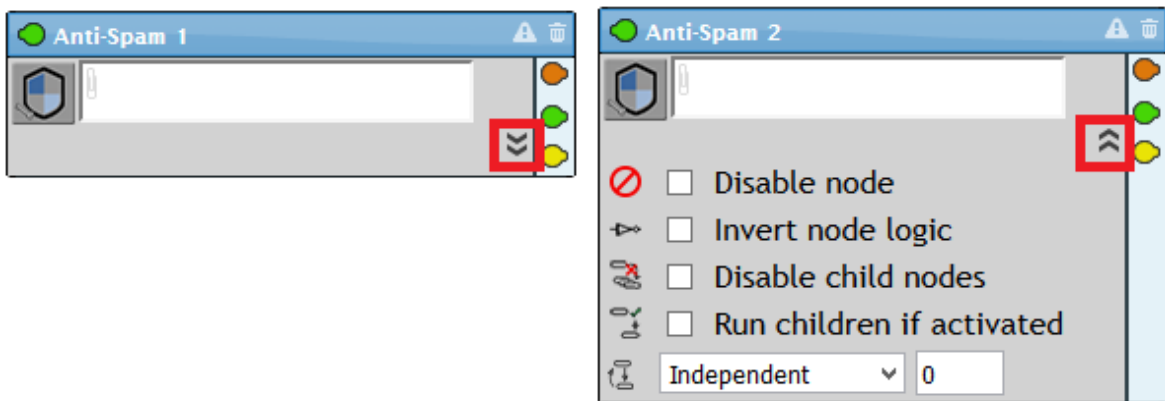
A snap-to-grid option can be toggled by clicking on the grid button at the bottom-right



Component Settings

Components can be renamed by clicking on their name.

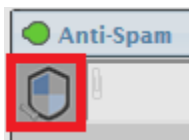
Individual component settings are accessed through the reveal chevron.



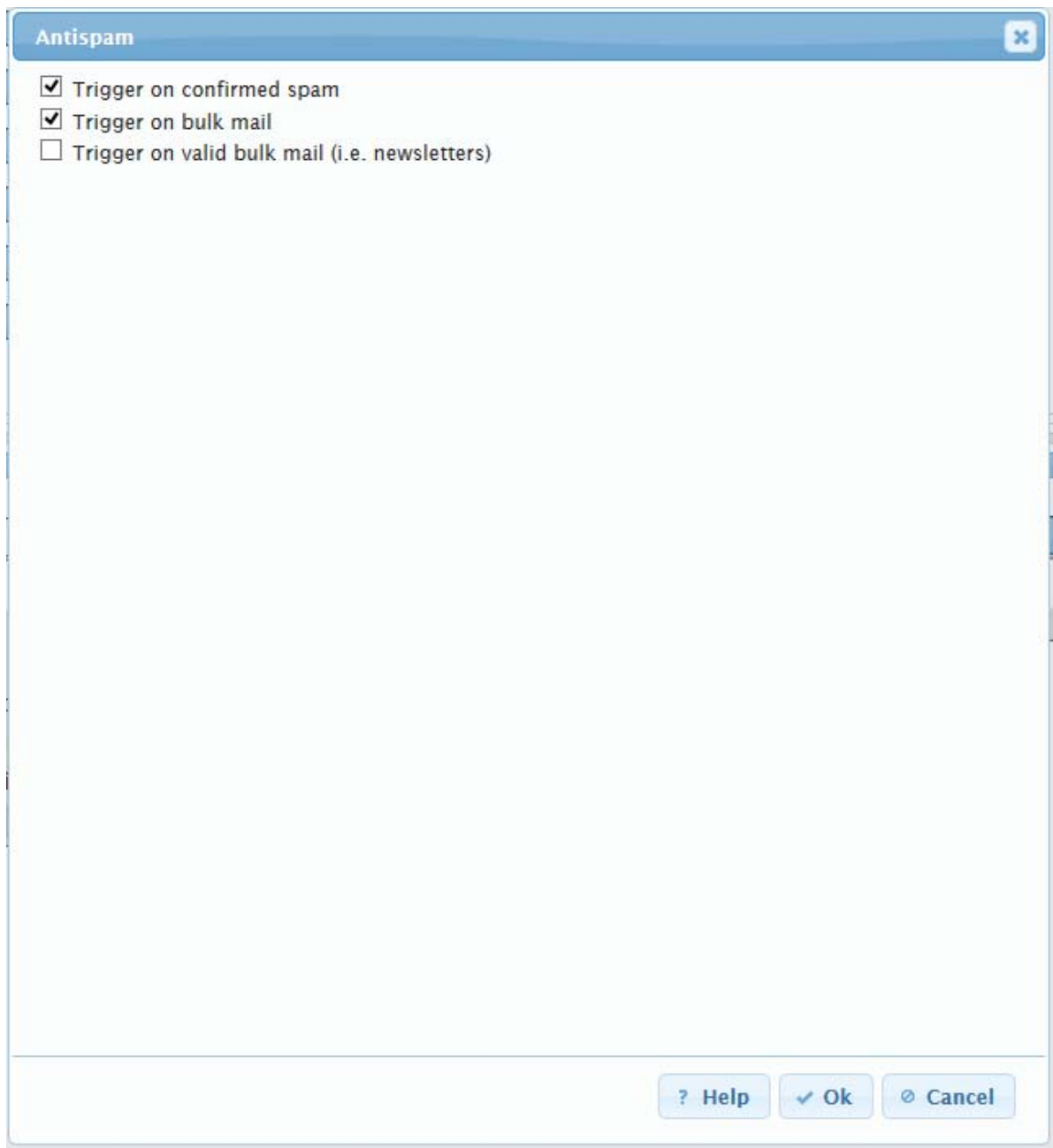
Component Configuration

Click on the component's icon to open the configuration dialog box.

For example, click on the Anti-Spam icon.



The Anti-Spam settings dialog box appears.

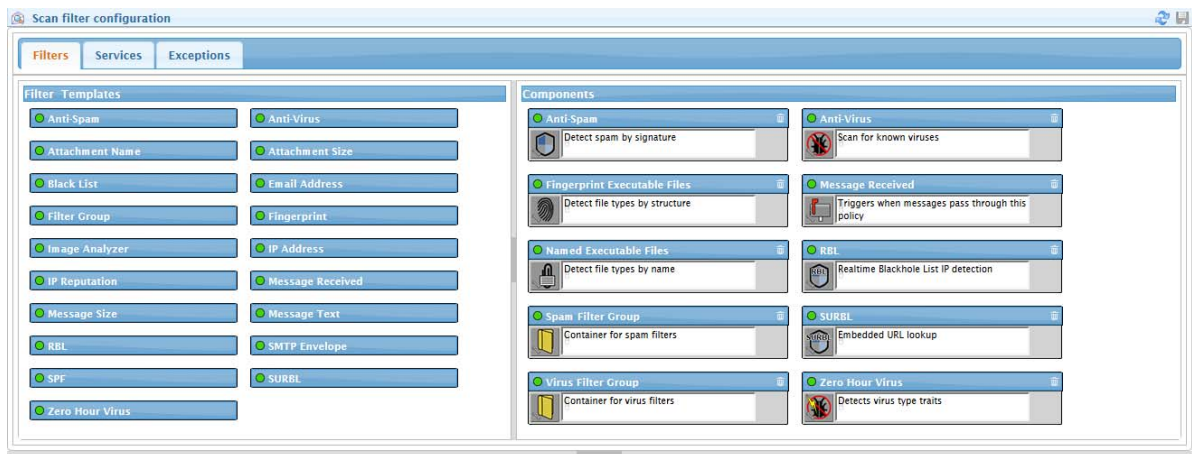


Select setting to trigger on.

Click on the "? Help" button for more information on the function.

Filters

There are a number of filters that will trigger when a message enters the system. These are indicated by the green pin on the component.



Anti-Spam

The anti-spam system searches messages for spam. There are options to select which actions to take depending on the results. A filter that has exceptions connected to it will override the block service. To add a message or message source to the list, simply input it into the provided list.

Options

Trigger on confirmed spam

Trigger on bulk mail

Trigger on valid bulk mail (i.e. newsletters)

Anti-Virus

The Anti Virus event scans messages for known viruses. The anti virus engine is set and requires no further configuration. Messages which have been detected to have a virus will have the connected action applied.

Options

This item does not require configuration

Attachment Name

The Attachment Name filter sorts attachment types according to their name, such as .doc or .iso. Attachment names may be specified in the provided field. To add a name and manage that specific type by name, simply type the desired name into the list. Multiple names may be specified by placing each name on it's own line. The attachment name differs from the fingerprint filter in that the fingerprint detects file types regardless of name, while the attachment name filter only looks at the file name.

Options

Add each criteria on its own line

Attachment size

The Attachment size event filter allows the admin to limit the size of attachments passing through the system. Message attachments which are outside of the specified size ranges will trigger this filter and cause the service selected to be enacted on that message or attachment

Options

Enable maximum size test

Maximum allowable size (bytes)

Enable minimum size test

Minimum allowable size (bytes)

Black List

Black List particular address pairs or addresses users have blacklisted in QMS

Options

Black List Data Source

Create a data source by clicking the plus sign. Add sender and recipient address pairs.

Link to a QMS data source by clicking on the link chain. Add additional sender and recipient address pairs.

DKIM

DomainKeys Identified Mail (DKIM) provides a method for validating a domain name identity that is associated with a message through cryptographic authentication. See [DKIM.org \(http://www.dkim.org/\)](http://www.dkim.org/). Very simply, DKIM adds a checksum to the email, to verify that the message is from the sender and has not been altered along the way.

This is unlike the typical filter, instead of looking for things to filter a message out, this will filter to allow a message in. Depending on the use case the "Invert mode logic" switch may be needed. A DKIM filter cannot be used with tags as that would alter the message and break the verification.

Option

Treat message as verified when signature not present.

Email Address

The Email Address Filter scans recipient or sender addresses against the provided list. Specify the desired addresses by inputting them into the field provided. Separate multiple addresses by placing each address on its own line. The sender, recipient, or both will be scanned according to the configuration. If the Email Address Filter is triggered, it will enact the connected service for that message.

Options

Scan sender address

Scan recipient address

Search criteria (add each criteria on its own line)

Filter Group

The Filter Group is an organizational placeholder, a building block to allow grouping of different filters to one node to simplify the deployment workbench. The Filter Group requires no configuration. Connecting filters to this group block ties all filters to the same action or item. Organization of the workbench is simplified with this block for complex deployments. Use this block to clean up the lines connecting associated filters, services, and exceptions.

Options

This item does not require configuration. Container nodes group tests together either for organizational clarity or to blend tests together to create meta-rules.

Fingerprint

Select file type fingerprint(s): The Fingerprint Filter searches message attachments for file types, regardless of whether they are named correctly. To configure the fingerprint filter, select the desired file types from the available file type list by clicking on them. Remove file types from the selected list by clicking on them. Only file types listed are available for selection. Deep/excessive compressed files The ZIPDEEP and ZIPWIDE fingerprints are special purpose tests that provide the ability to test for compressed files that exceed reasonable limits of these files. These limits are defined within the policy management page and are used to prevent malicious attacks from causing system resource starvation. Applying these specific fingerprints will refer to the policy settings for the limits tested. These tests will also extract archives from within archives as part of the test process, and will include all supported archive types.

Options

Click "Add new types" button and click on files types to activate available file types to scan.

Image Analyzer

NOTE: Requires separate license.

The Image analyzer scans images looking for pornographic content. Each scanned message is scored between 0-100. Scores will vary depending on settings. The Minimum image width, specified in pixels, determines if an image will be scanned. Images smaller than the defined size are skipped. The sensitivity will determine how aggressive Secure Messaging Gateway will be when scanning an image. When the sensitivity is higher, Secure Messaging Gateway will scan the image more thoroughly. The threshold is the level at which the Image Analyzer filter is triggered and the associated action is taken.

Options

Minimum image size: Default, 100 x 100

Sensitivity: Default, 65

Threshold: Default, 75 - 100

IP Address

The IP Address filter event scans messages for a match to any specified IP Address. Messages coming from a specific IP Address can be blocked by specifying that address in this filter. Messages coming into the filter will be scanned for a match to any IP address specified in the list. To add an address to the filter list, simply select the field and input the address or addresses into the list. For multiple addresses, place each IP address on its own line.

Options

Search criteria (add each criteria on its own line)

IP Reputation

IP Reputation works much like a RBL or SURBL filter but also uses a whitelist for common message sources. IP Reputation will temporarily block messages from sources which are not found on either list. The temporary fail is performed via a connection drop. If the sending gateway repeats sending attempts, the messages will be allowed through. For an IP Reputation filter to be effective, it needs to be utilized on the SMTP interface with both trigger options enabled. If the trigger options are disabled, the events will not cause the filter to drop the connection and block the message.

Options

Trigger on confirmed IP

Trigger on suspect IP

Message Received

The message received event is activated for all messages received by the Secure Messaging Gateway system, in or outbound. This filter allows administrators to dictate general services on messages. The Message Received event may also be restricted to a specific message direction: Inbound, Outbound, Internal, and External mail. When combined with the desired services, the Message Received event may be used, for example, to append a signature on all messages leaving the system, or may be used to add header lines to all internal mail.

Options

Used to feed data to the Statistics and Message Tracker filters.

Message direction

Message Size

The Message Size filter allows the administrator to limit the size of messages passing through the system. Messages which are outside of the specified size range will trigger the event and have the associated action applied.

Options

Enable maximum size test

Maximum allowable size (bytes)

Enable minimum size test

Minimum allowable size (bytes)

Message Text

The Message text filter scans messages for matching text strings, in the locations selected. Custom text strings may be specified in this filter. For multiple text strings, place each on a separate line. The Text filter can scan for text in specific locations of messages. You must enable a location to be scanned before the text filter will be active. One or all locations may be selected at the same time.

Options

Look in message body

Look in message subject

Look in message header

Look in message source file

RBL

The RBL (Real-time Blackhole List or Real-time Block List) Filter checks incoming messages to see if any sending server(s) are included on any of the configured RBL servers. To configure the RBL Filter, input the desired RBL server into the RBL server field. The RBL Filter may be limited to certain lines in the message. The default is to scan the entire header of a message. The 'Received header scan range' limits the lines of a header to be scanned. The beginning and end line scanned may be specified. ie. 1-5, would scan the first through the 5th line of the header, while 4-7 would only scan the 4th through 7th lines of the header.

Options

Include connecting IP address

Include ip addresses located in headers

Received headers scan range

RBL Server

sbl-xbl.spamhaus.org (Default)

bl.spamcop.net (Default)

Skip Local IP

SMTP Envelope

The SMTP envelope filter checks to see if specific attributes of the SMTP connection are present. The Client authenticated test looks for the inbound SMTP connection to successfully provide valid login credentials for the system. (Username and Password) The SSL secure test looks to see if the client establishes and sends its data over a secure channel Client Switched to SSL using STARTTLS looks to see if the incoming client was secure from the beginning of the session or whether SSL was initiated after initial client connection. All features have the options 'yes', 'no', and 'don't test'. If selected either 'yes' or 'no', incoming messages will be scanned and, if detected, the selected filter will enact connected services associated.

Options

Client is authenticated

Client is SSL secure

Client switched to SSL using STARTTLS

SPF

The SPF (Sender Policy Framework) Filter 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, sending messages to you.

Options

Treat ~all as -all

SURBL

The SURBL (previously stood for Spam URI RBL) Filter checks each message against the SURBL databases listed to see if the sending server is included on the SURBL list. To add a SURBL server to the list, simply type it into the list. Multiple servers may be listed, one on each line, however it is recommended to only have one as multiple server lists may slow performance.

Options

SURBL server list (add each server on its own line)

Zero Hour Virus

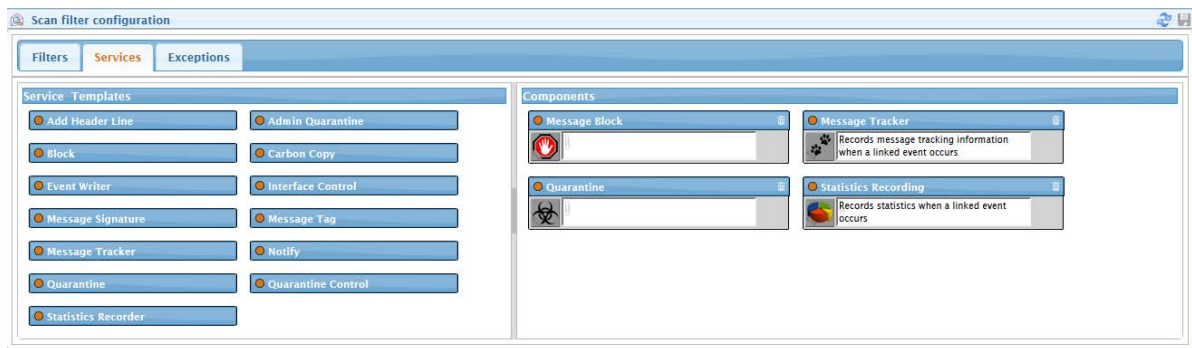
The Zero Hour Virus filter checks each message for virus-like characteristics to protect against new and unidentified viruses.

Options

This item does not require configuration

Services

Services are the actions Secure Messaging Gateway takes on a message. These are indicated by the red pin on the component.



Add Header Line

The Add Header service injects the specified header line or lines into messages. To add a line or lines to a new header for the message, simply specify the desired line(s) in the provided field. Messages referred to this service will have these lines added to the beginning of the message.

Options

Message header

Admin Quarantine

The Admin Quarantine service sends messages into the Quarantine system under administrator rights. Mail which has been quarantined will remain in the Quarantine system for 30 days by default. Normally, users are able to release messages from their own quarantine, however, the admin quarantine only allows users with administrator rights to release these messages.

Options

This item does not require configuration. Use of this service will quarantine messages that are only accessible by a quarantine administrator.

Block

The block service prevents delivery of a message to the intended recipient(s). A filter that has exceptions connected to it will override the block service.

Options

This item does not require configuration

Carbon Copy

The Carbon Copy service creates a BCC message and sends it to the specified address. This Service will be active on any filter that it is associated with. To add addresses to the list, simply enter them into the provided area. Multiple addresses may be used, each on an individual line.

Options

Addresses to copy to (add each address on its own line)

Event Writer

The Event Writer creates a file associated with each time a connected filter or service is activated. The Event Writer is a simple way to create a custom log of whenever an event occurs. When attached to any event, the writer will create the specified file with the specified text. This is in addition to any notifications. If a desired event is to be recorded, or a file is to be created whenever an event occurs, the Event Writer should be used in association with that event. Tie the event writer to the desired event in the workbench and specify the destination file name and contents. While the file name may be anything desired, the contents will be created as shown in the Event Text window.

Options

Destination file

Event text (include line feeds to prevent data being written to a single line)

Interface Control

Use this node to override actions of the interface that requested a message scan. Setting the delivery response overrides the default response sent to the connected mail system. This service is typically coupled with the block/quarantine service combination, where messages are blocked by Secure Messaging Gateway and placed in quarantine. In this situation, the sender is informed that the message was blocked, and may attempt to resend the message, even though it was in fact received - but not delivered on to the intended recipient. Overriding the response in this condition with an 'Accepted' response overrides the rejection response caused by the block service.

Options

Delivery response

Accept (2xx)

Delay (3xx)

Reject (4xx)

Message Signature

The Message Signature Service appends a signature onto the end of messages. To dictate a signature to be added to messages, simply add the desired signature into the configuration field utilizing the tools provided.

Options

Signatures: Text, HTML or both

Automatic text signature

Placement priority

Message Tag

Use the Message Tag service to replace or alter the subject line of a message.

Rule Priority

If multiple Message Tag services are applied during the scan process, the rule priority sets the order in which the rules are run. Each altered subject is fed into the next Message Tag service, starting with the highest numbered priority item and working down.

Rewrite Rule

The message subject will be replaced with the text provided here. Using the macro variables referenced, information from the original subject line can be included

Example

In this example, rather than rejecting or quarantining spam, the system will change the subject to indicate that the message is probably spam to the end user. Rewrite Rule: [possible spam] %original%

Options

Rule Priority

Rewrite Rule

Variable reference

%original% - Insert the original header content

%% - Insert a percent symbol

Message Tracker

The Message Tracker service saves information about the message and results of the scanning process. The Message Tracker System contains detailed information about the message and the scanning process as well as information about the receipt and delivery of the message. Information will be recorded for all triggered filters unless you select the checkbox to only track filters that are connected to the message tracker service.

Options

Record only filters connected to this service

Notify

When a filter is triggered there is the option of sending a notification.

For example, if an Attachment Size filter triggered because a an attachment was too large, a notification can be sent to the sender reminding them of the attachment size limitation. A notification can also be sent to the recipient to tell them that a message was received but could not be delivered due to the attachment size limitation. Another notification can be sent to the system administrator to alert them of the issue.

Options

Notification template: To customize templates, see [Templates \(Templates.htm\)](#)

Notify Generic (en)

Notify Recipients (en)

Notify Sender (en)

Sender address: Enter a valid email address to be used by Secure Messaging Gateway as the notification sending address. This does not have to exist in the email system, but a validly formatted email address is required by most email servers. For example, SecureGatewayNotificationSender@gwava.com

Customization

SenderName: Sender display name.

Subject: Notification subject.

MessageText: Text message body.

MessageHTML: HTML message body.

Notify sender: If enabled the sender of the triggering message will be sent a notification. Default, disabled.

Notify recipients: if enabled the recipients of the triggering message will be sent a notification. Default, disabled.

Additional addresses to notify (add additional addresses on their own line)

Quarantine

The Quarantine service places messages into the Quarantine Management System, (QMS). The Quarantine Management System is the holding location, where messages await possible review and, or, release to mailboxes. Users may manage their own quarantine if given rights to do so. Administrators may restrict specific types or filter-flagged messages from being released from QMS. All configuration of Quarantine activity is completed with User rights and the within QMS itself. This service building block is only for placing messages in the QMS system.

Options

This item does not require configuration. Use of this service will quarantine messages for user review. Quarantining a message does not cause messages to be blocked. To block and quarantine messages, ensure that a block service is also linked to the applicable filters.

Quarantine Control

Quarantine control provides the ability to selectively control what actions are available to the quarantine system for individual messages based on the configured filters. To implement this service, link the quarantine control node to the event that contains the filter that determines the control point. For example, to prevent dangerous attachments from being accessed, create a fingerprint filter to detect program file types and attach it to a quarantine control node with the disable release and disable attachment download options selected. With this setup, any messages that are placed in quarantine that have dangerous attachments can be reviewed by users, but not accessed. Disable digest - Prevents the quarantine service from including messages in the digest process Disable message release - Prevents users from releasing messages from the quarantine system. Disable attachment download - Prevents users from downloading attachments from the quarantine message viewer. Disable message view - Prevents users from opening and viewing messages. Messages are still listed in the users quarantine. Disable HTML view - Prevents users from viewing the HTML portion of messages which may contain objectionable images. Where 'User' is specified, this refers to

controlling the end user functionality of the quarantine system. Where 'All' is specified, this refers to controlling all users of the quarantine system, including system administrators. This option provides safety against human error only, as admins can override the setting from the quarantine.

Options

Disable digest

Disable message release: Default, no

Disable attachment download: Default, no

Disable message view: Default, no

Disable HTML view: Default, no

Statistics Recorder

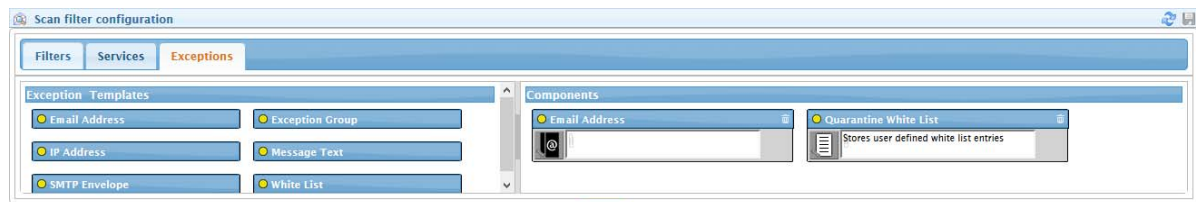
The statistics recorder records data on messages passing through the system where it is connected to events, exceptions, and filters. This is used with the Message Received filter. This Service requires no configuration. Simply set it in the correct listening spot in the system.

Options

This item does not require configuration

Exceptions

Exceptions can be made to each Filter for particular circumstances. These are indicated by the yellow pin on the component.



Email Address

The Address Exception tells the system to skip a connected event test for messages containing the listed sender or recipient address. The sender or recipient, or both address locations can be specified. If a recipient address is on the exception list, messages will not be tested against the different connected event(s). To add an email address to the list, simply input it into the configuration window. Multiple addresses may be specified, simply place each address on its own line.

Options

Scan sender address

Scan recipient address

Search criteria (add each criteria on its own line). There can be no spaces or blank lines.

Exception Group

A Group node groups exceptions together, either for organizational clarity or to blend exceptions together to build meta-exceptions. These provide the ability to create complex exception rules with multiple types of exceptions within the same rule.

Options

This item does not require configuration. Group nodes group exceptions together either for organizational clarity or to blend exceptions together to build meta-exceptions. These provide the ability to create complex exception rules with multiple types of exceptions within the same rule.

IP Address

The IP Address Exception instructs the system to ignore results for tests to which the exception is applied. When active, the system will compare the originating IP address against the exempted list. To add an Address to the list, simply enter the address into the list. Add multiple addresses to the list by placing them on their own individual lines.

Options

Search criteria (add each criteria on its own line). There can be no spaces or blank lines.

Message Text

The message Text exception tells the system to exempt messages from associated event tests if the specified text is present in the body of the message. To add a text exception, simply add the desired text into the list.

Options

Look in message body

Look in message subject

Look in message header

Look in message source file

Search criteria (add each criteria on its own line)

SMTP Envelope

The SMTP envelope filter checks to see if specific attributes of the SMTP connection are present. The Client authenticated test looks for the inbound SMTP connection to successfully provide valid login credentials for the system. (Username and Password) The SSL secure test looks to see if the client establishes and sends its data over a secure channel Client Switched to SSL using STARTTLS looks to see if the incoming client was secure from the beginning of the session or whether SSL was initiated after initial client connection. All features have the options 'yes', 'no', and 'don't test'. If selected either 'yes' or 'no', incoming messages will be scanned and, if detected, the selected filter will enact connected services associated.

Options

Client is authenticated

Client is SSL secure

Client switched to SSL using STARTTLS

White List

White List particular address pairs or addresses users have listed in QMS

Options

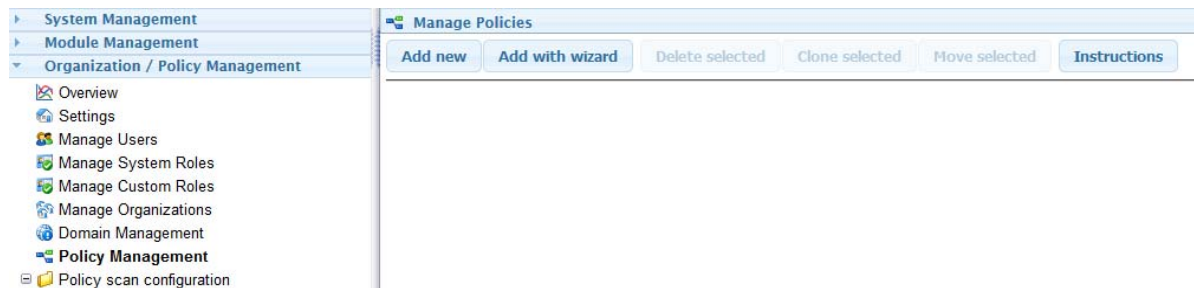
White List Data Source

Create a data source by clicking the plus sign. Add sender and recipient address pairs.

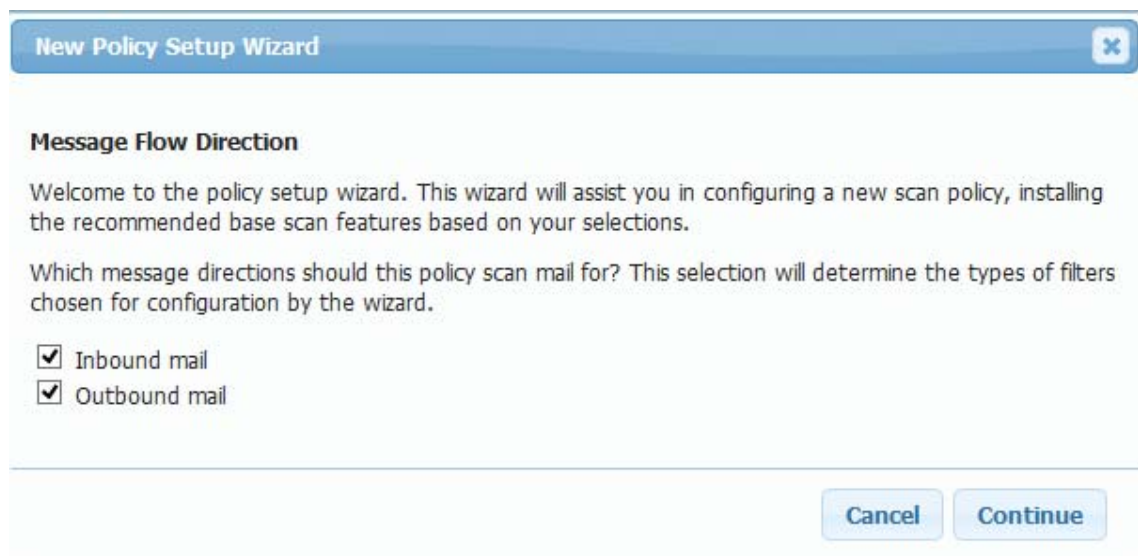
Link to a QMS data source by clicking on the link chain. Add additional sender and recipient address pairs.

New Policy Wizard

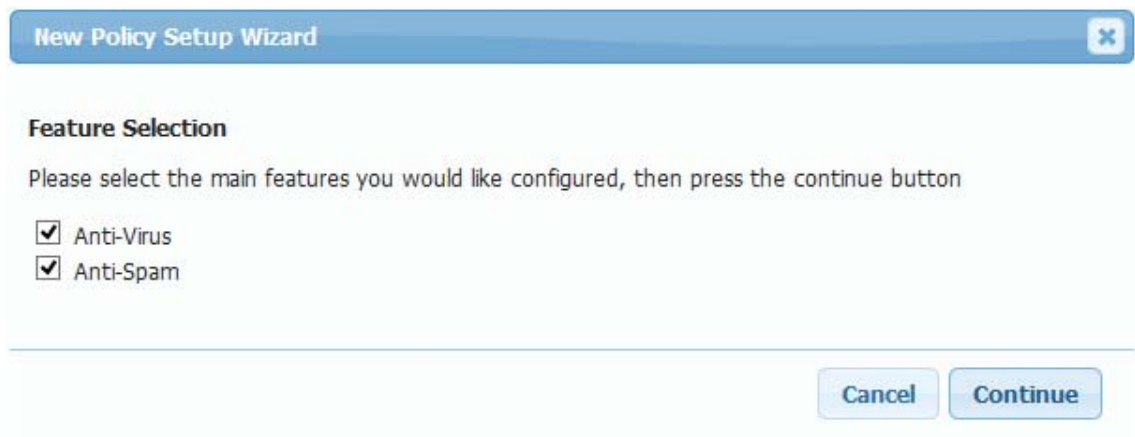
Create a new policy with the wizard. Click on *Add with wizard*.



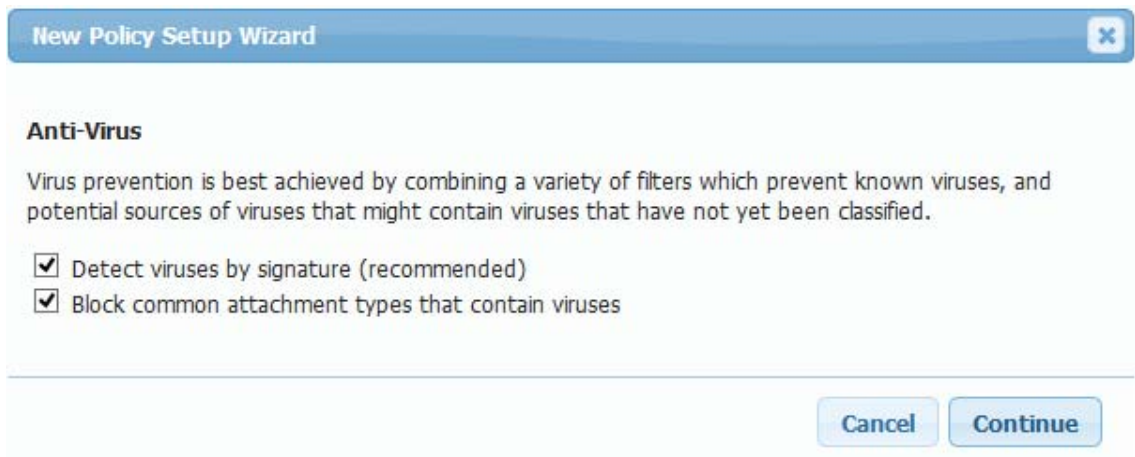
1. Select the Message Flow Direction. You can choose Inbound and/or Outbound.



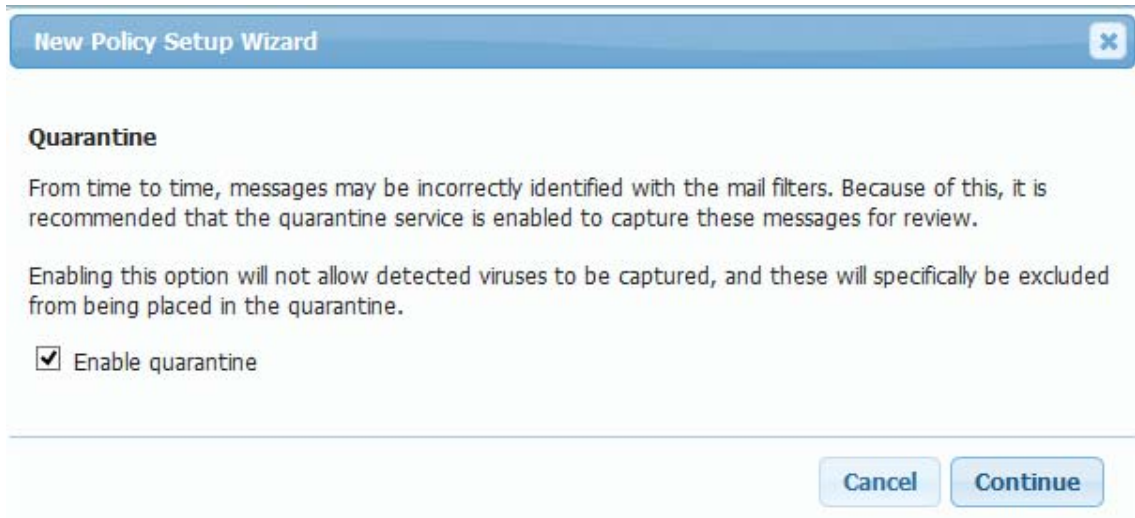
2. Select the features to be configured. Anti-Virus and/or Anti-Spam.



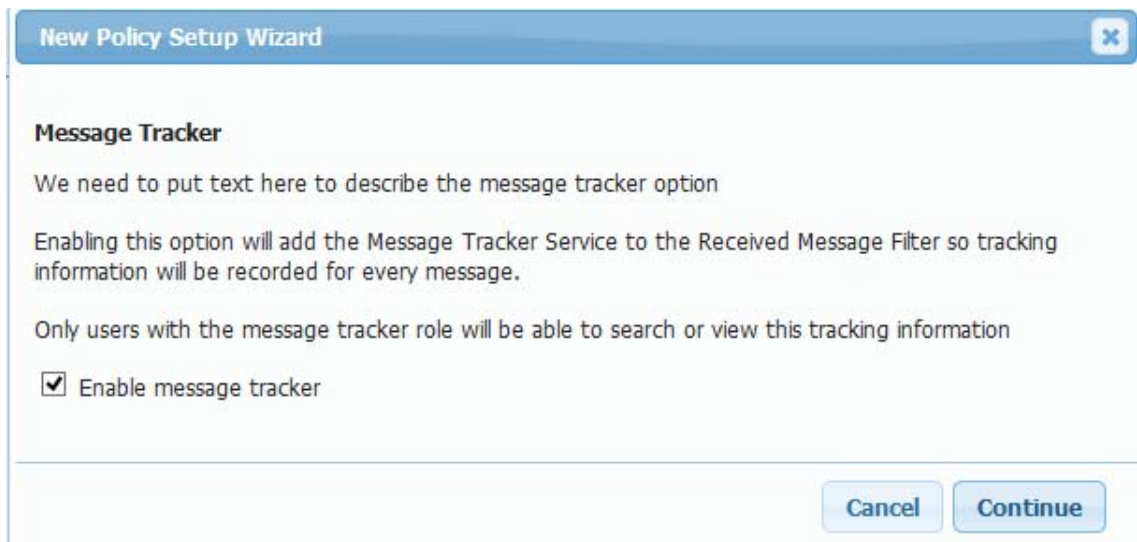
3. Select Anti-Virus filters, Detect viruses by signature (recommended) and/or Block common attachment types that contain viruses



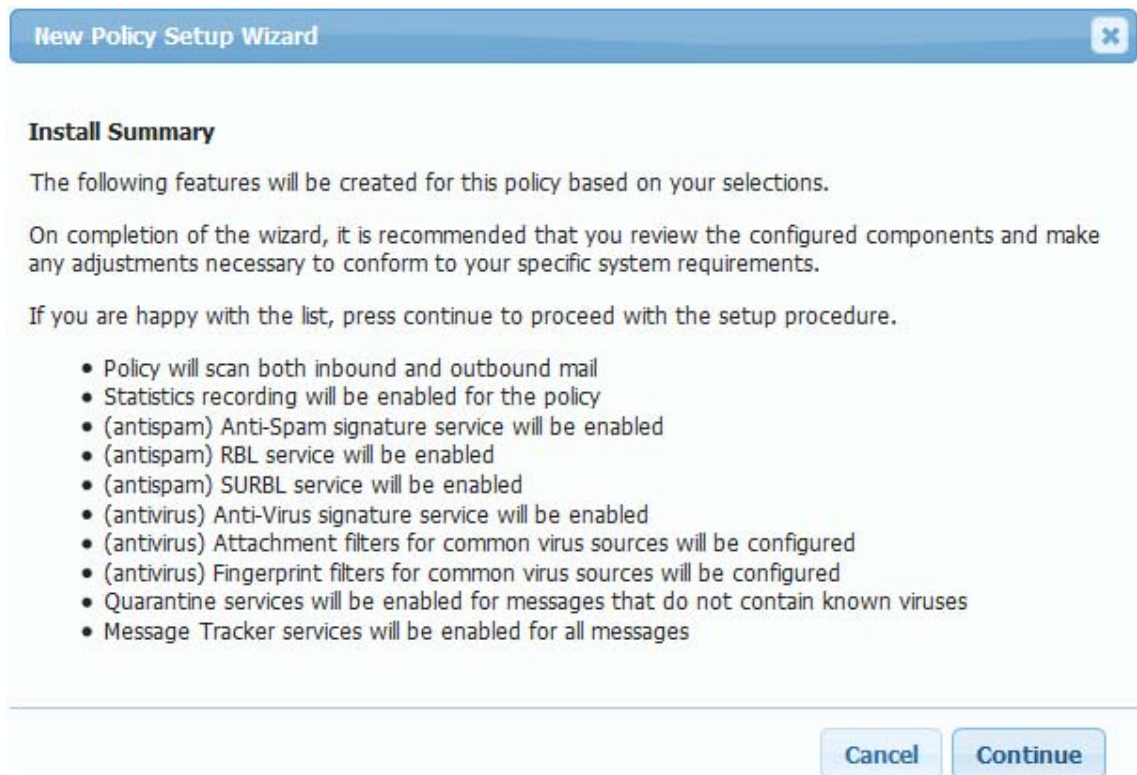
4. Select if you want messages quarantined.



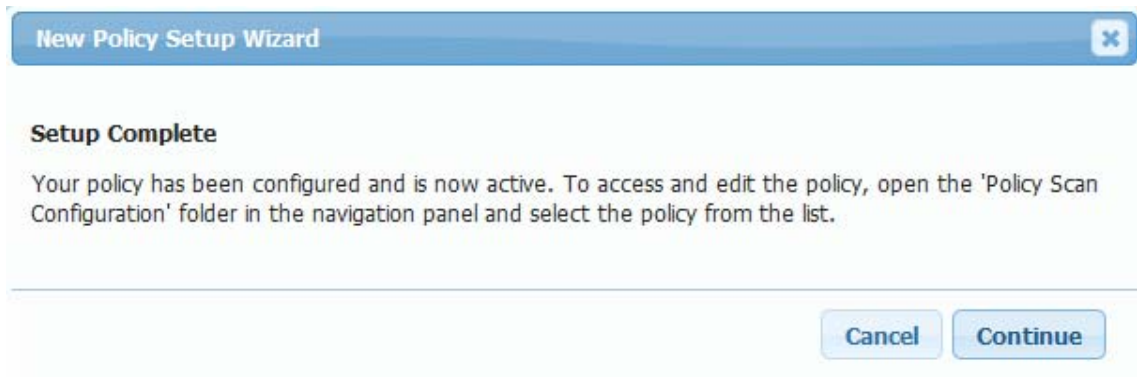
5. Select if you want messages tracked in the system.



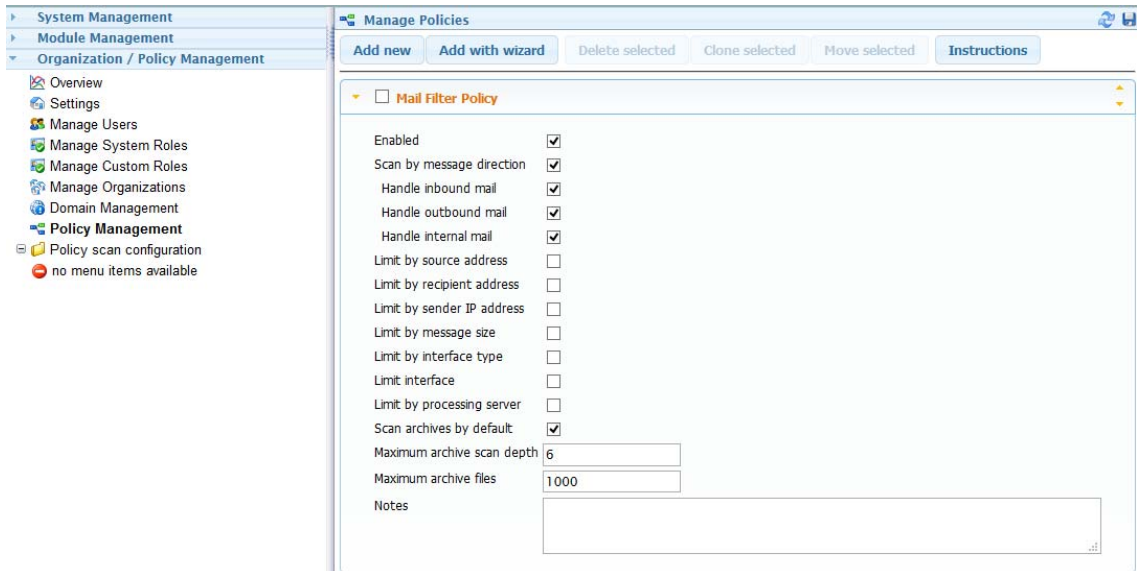
6. A summary of what the wizard will do will appear.



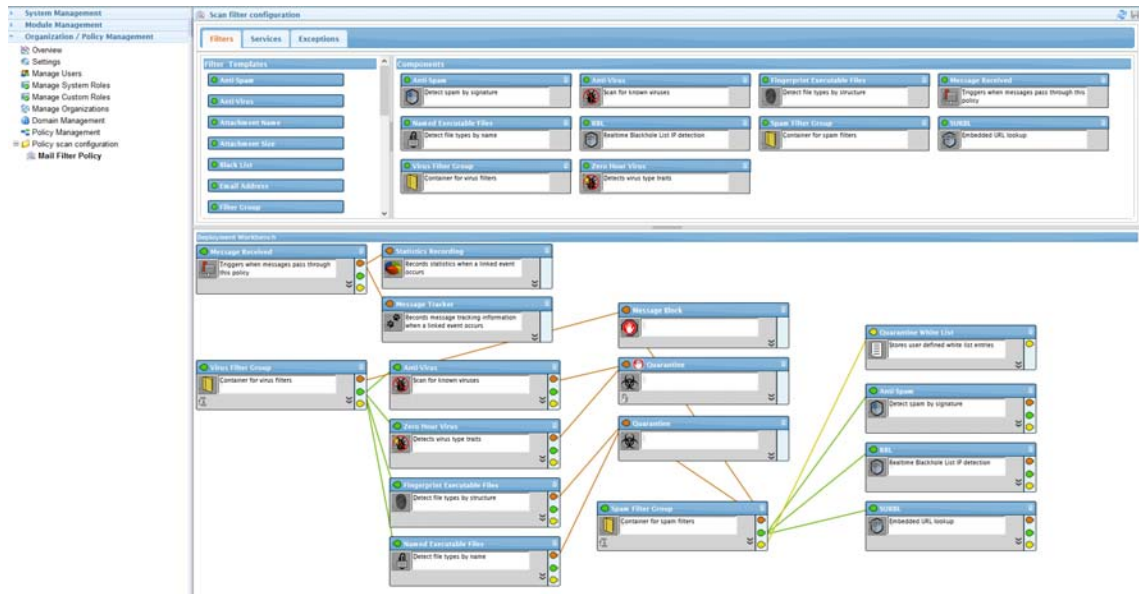
7. In a moment, it will be done.



8. The new policy will appear. Clicking on the title allows for changing the name.



- Open the Policy scan configuration folder, or refresh to see the new policy, and click on the policy to see the workbench.



Creating a Statistics and Tracking Policy

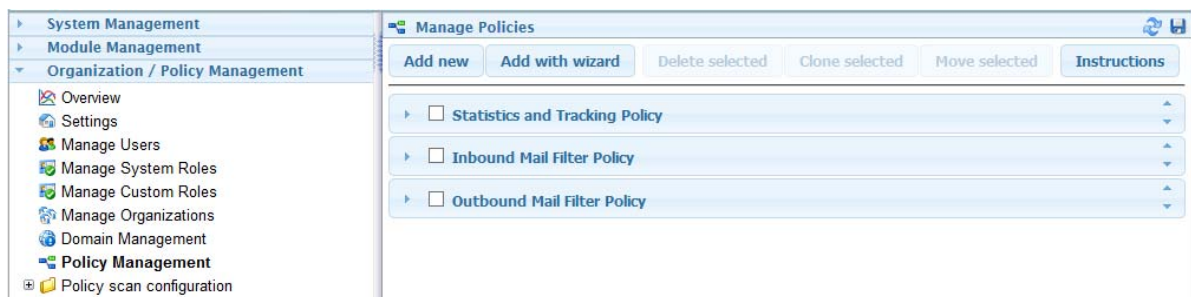
Creating a policy manually involves:

- Creating the policy
- Setting the policy priority, messages move through the policies from top to bottom
- Set the policy message scan direction
- Configuring the policy with filters, services and exceptions

When creating a policy manually, one of the simplest to create is a Statistics and Tracking policy.

Create the Policy

Under *Organization / Policy Management | Policy Management*, click *Add New* to create a new policy and name it something easy to remember like Statistics and Tracking Policy.



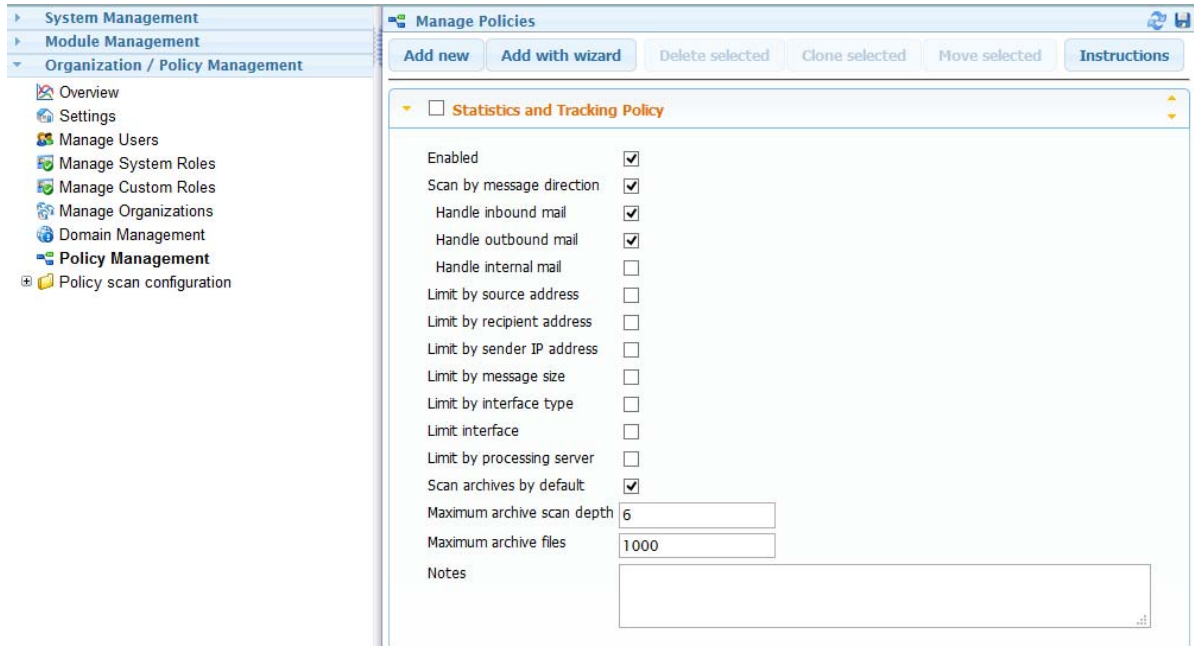
Set the Policy Priority

If you have more than one policy use the arrows on the right on the panel to move the policy to the top.

Messages move through policies from top to bottom. If a policy filters a message, for example an exception allows a message through, none of the lower policies will see the message.

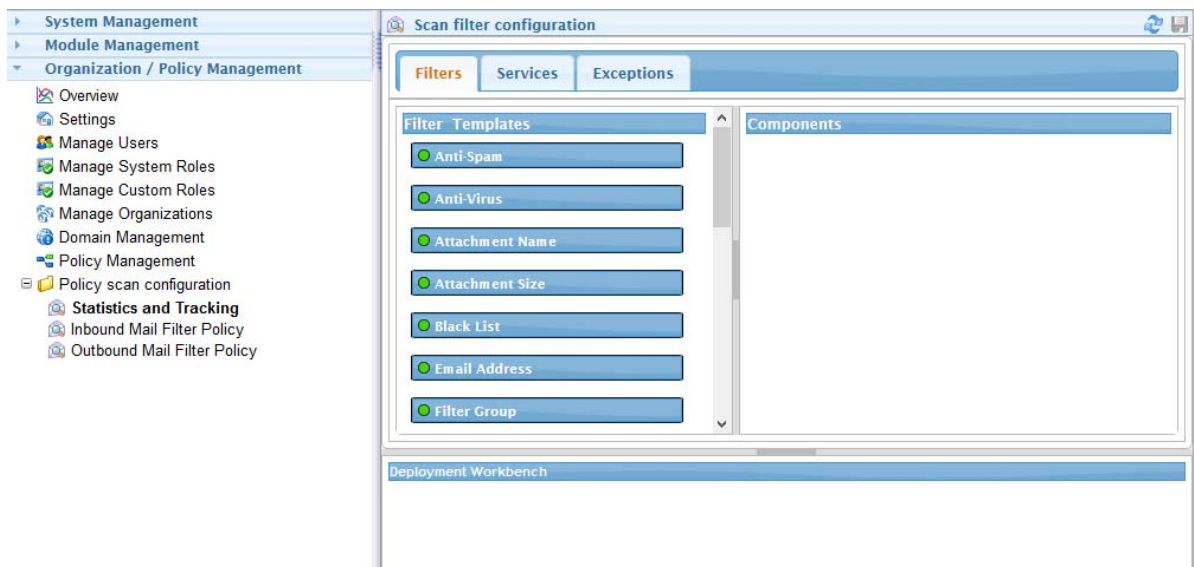
Set the Policy Message Direction

Open the panel and enable *Scan by message direction* then enable *Handle inbound mail* and *Handle outbound mail*.



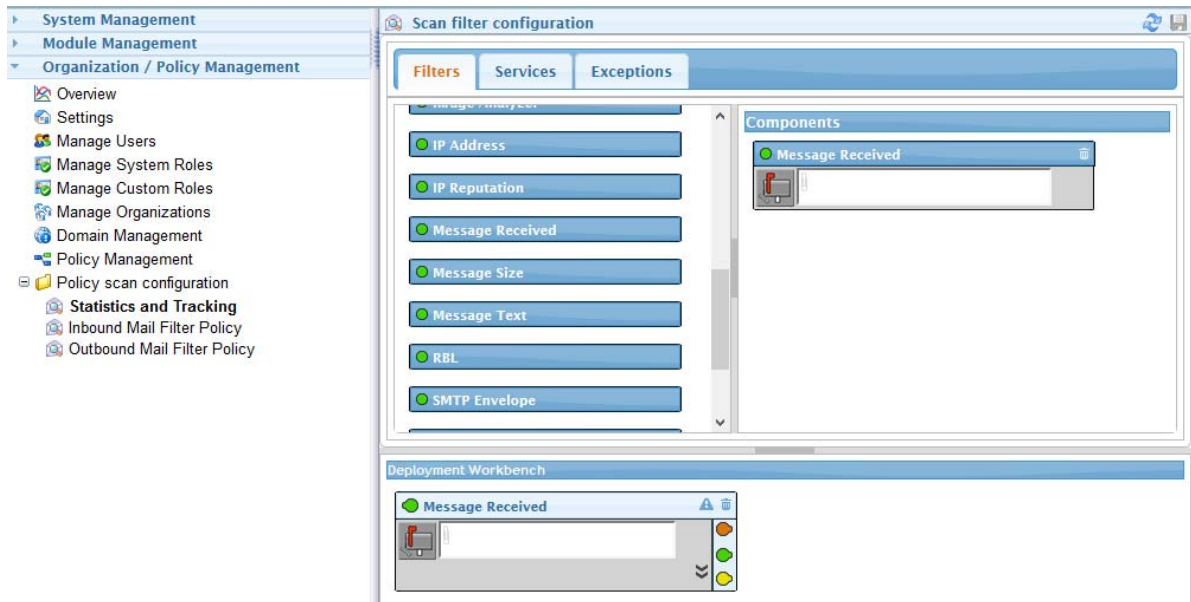
Configure the Scanner

Open the *Policy scan configuration* folder and select the policy. The workbench will be empty.



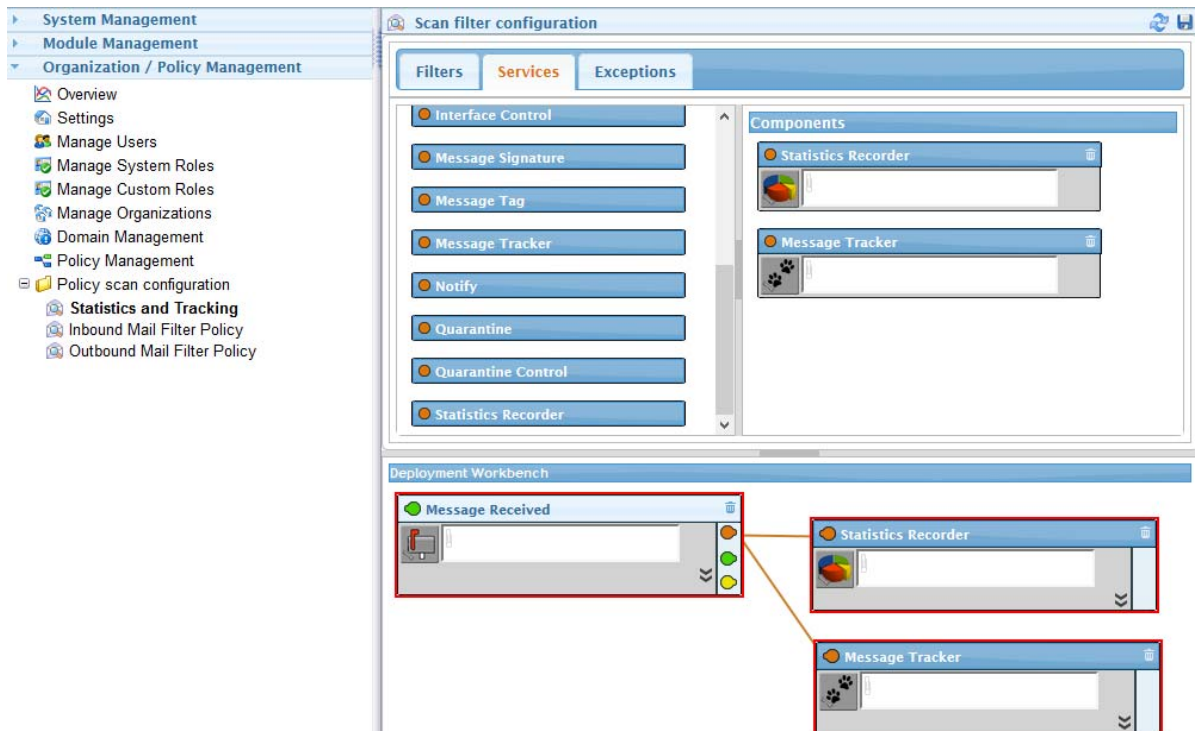
Add the Filter

Drag the *Message Received* filter from the Filter Templates pane to the Deployment workbench. Generally, whenever a message passes through Secure Messaging Gateway it will be scanned, but for the Statistics and Message Tracking services the Message Received filter is needed.

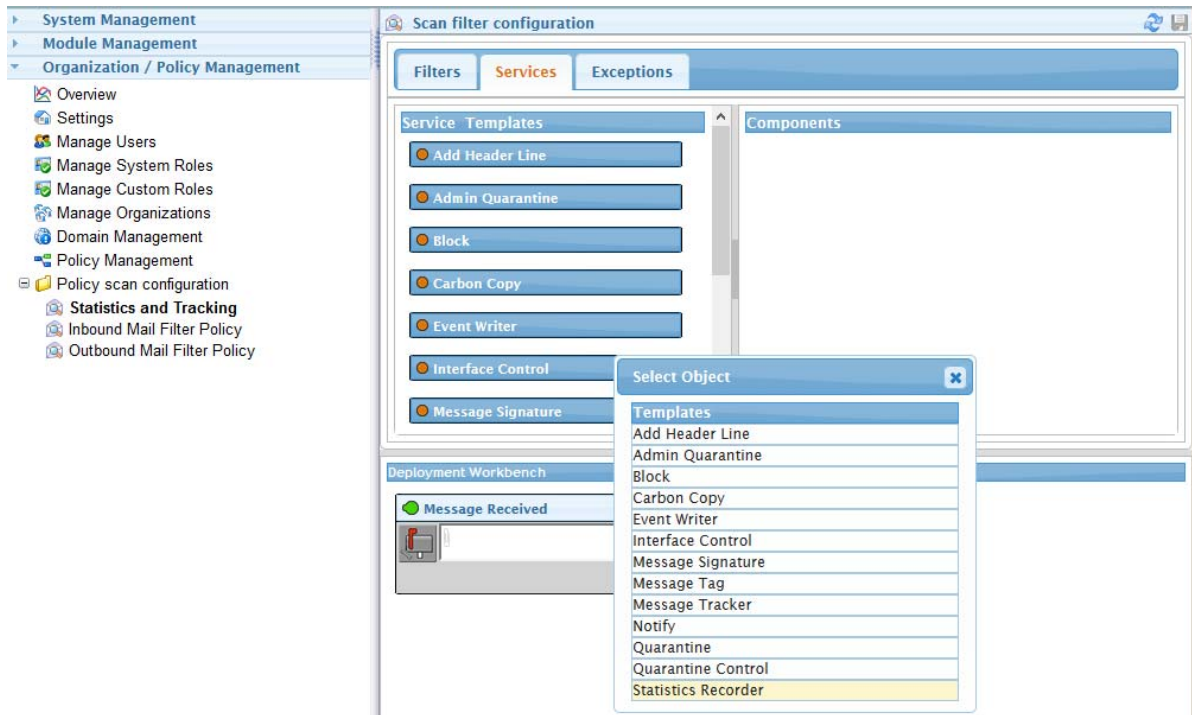


Add the Service

A service can be added by selecting the Services tab and dragging the desired service to the workbench and then clicking and dragging the red services pin on the right side of the filter to the service. Multiple services may be attached to a filter.

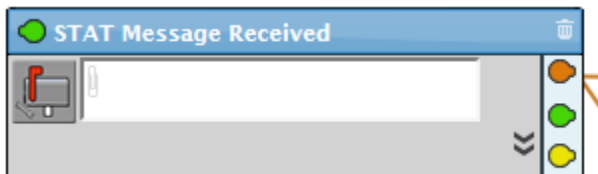


Alternatively, drag the red services pin on the right side of the filter and drop on any white space within the workbench and a service selection menu will appear. Select the service desired, for example, Statistics Recorder.

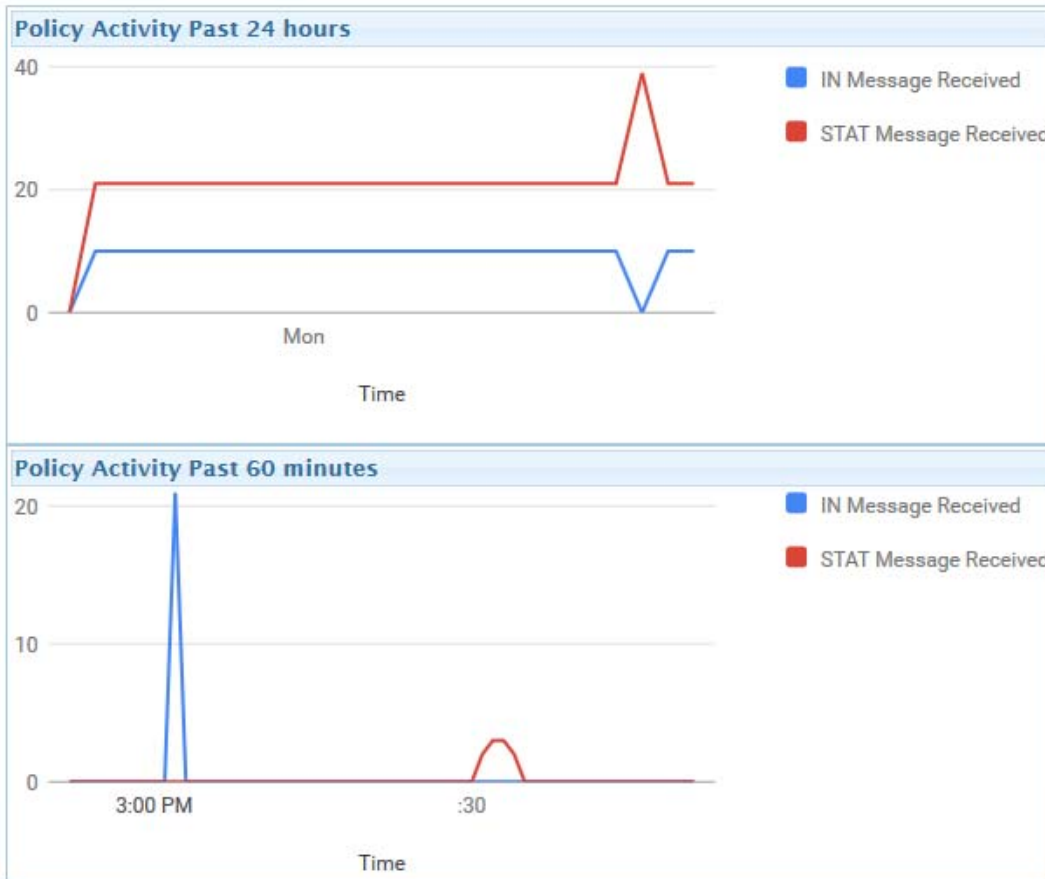


Click on *Save* and the policy will become active immediately. All messages passing through Secure Messaging Gateway will have statistical data and message tracking.

If multiple Message Received filters are used it is recommended to name them uniquely.



Statistical data will appear under *Organization / Policy Management | Overview*



Message tracking data will appear in the Message Tracker. Log out of the Admin console and log back into the Message Tracker.

Jun 8, 2017

Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address
08-Jun-2017 11:34:47 am	Fruit flavors are used in fizz drinks. 1263368060	script@sf.gwava.net	test7@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:34:25 am	The hail pattered on the burnt brown grass. 498208501	script@sf.gwava.net	test8@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:34:03 am	Whittings are small fish caught in nets. 2120411854	script@sf.gwava.net	test9@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:33:52 am	A thick coat of black paint covered all. 1128763930	script@sf.gwava.net	test5@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:33:30 am	The leaf drifts along with a slow spin. 946886760	script@sf.gwava.net	test4@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:33:08 am	A castle built from sand fails to endure. 1357637890	script@sf.gwava.net	test6@doc.mf.net	internal	none	151.155.183.142
08-Jun-2017 11:32:46 am	The fly made its way along the wall. 826354919	script@sf.gwava.net	test3@doc.mf.net	internal	full	151.155.183.142
08-Jun-2017 11:32:24 am	They felt gay when the ship arrived in port. 25998381	script@sf.gwava.net	test2@doc.mf.net	internal	full	151.155.183.142

Creating a Block and Quarantine with Exceptions Policy

Creating a policy manually involves:

1. Creating the policy
2. Setting the policy priority, messages move through the policies from top to bottom

3. Set the policy message scan direction
4. Configuring the policy with filters, services and exceptions

For this example we will assume that a supplier has an overly enthusiastic marketing department and orders to reduce the amount of unwanted mail but allowing the desired mail through have come down.

In this case, the Inbound Mail Filter Policy is a wizard created policy that deals with general spam, and malware. However, unwanted message are getting through and need to be dealt with.

Create the Policy

Under *Organization / Policy Management | Policy Management*, click *Add New* to create a new policy and name it something easy to remember like *Overly Enthusiastic Marketing Policy*.

Set the Policy Priority

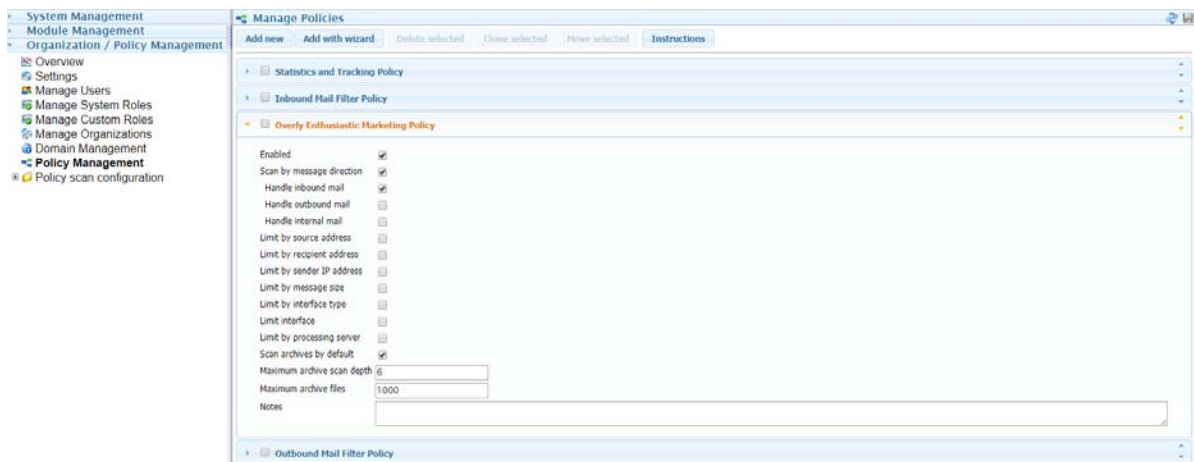
If you have more then one policy use the arrows on the right on the panel to move the policy to the top.

Messages move through policies from top to bottom. If a policy filters a message, for example an exception allows a message through, none of the lower policies will see the message.

As the unwanted messages are passing through the existing filters we will set the next filter below it.

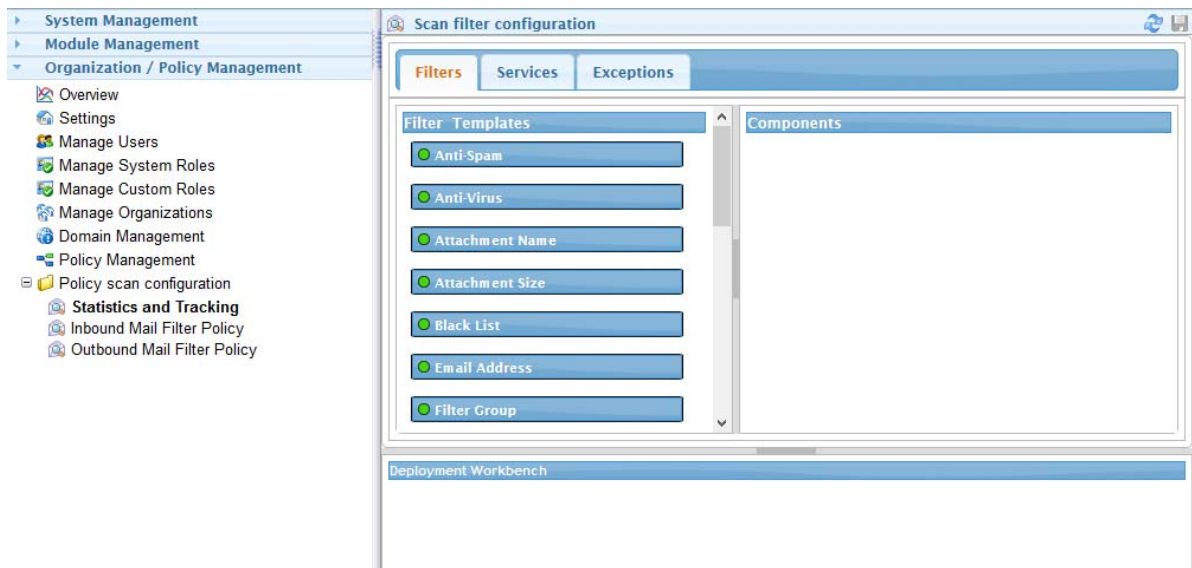
Set the Policy Message Direction

Open the panel and enable *Scan by message direction* then enable *Handle inbound mail*.



Configure the Scanner

Open the *Policy scan configuration* folder and select the policy. The workbench will be empty.



Add the Filter

There are a number of filters that could be used to manage the unwanted mail.

Black List: This requires a known Sender address and Recipient address. This is useful if the CEO is getting too much email from a particular marketer.

Email Address: This can filter by sender or recipient address and is useful when one sending is sending to many users in the system.

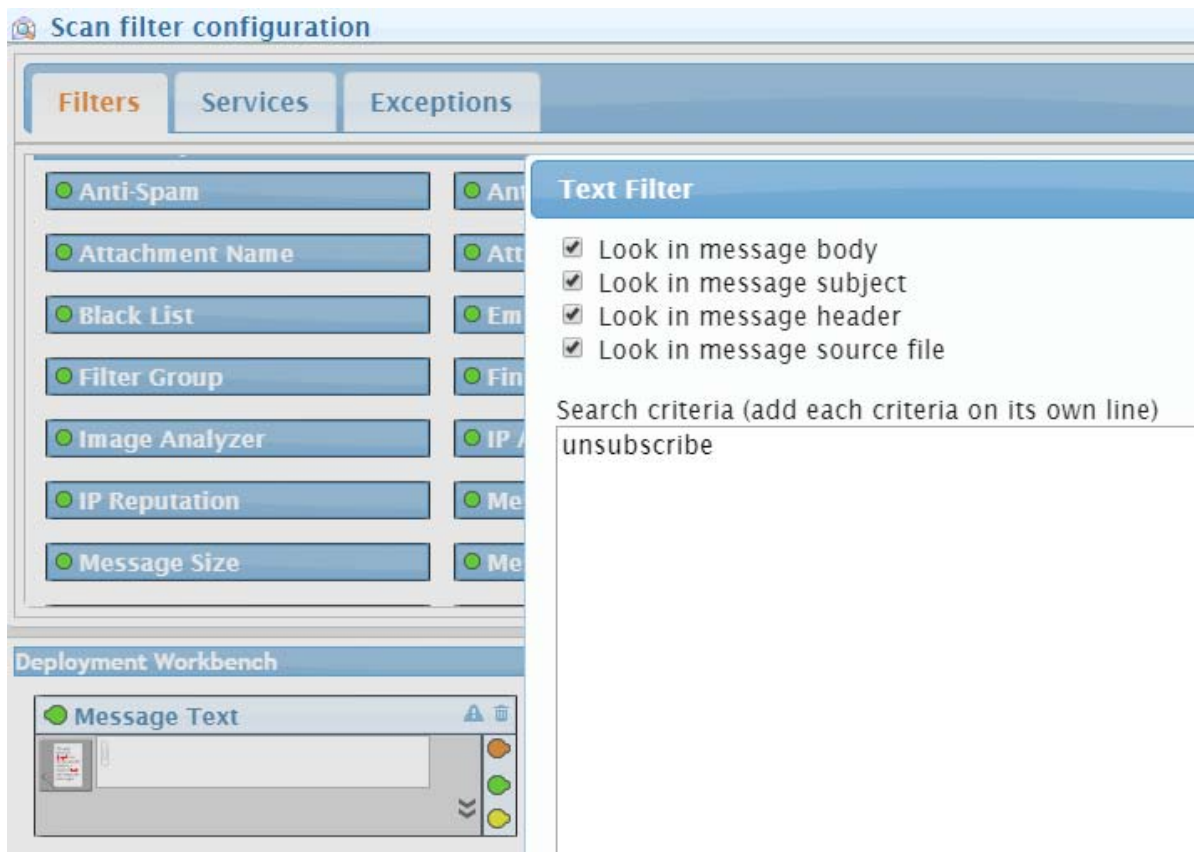
IP Address: This filter's criteria is an IP address or IP range. Useful if you are getting spammed from a particular company or country.

Message Text: This filter will scan the message body, subject, header and/or source file for particular text.

For this example we will use the Message Test filter.

Drag the *Message Text* filter from the Filter Templates pane to the Deployment workbench.

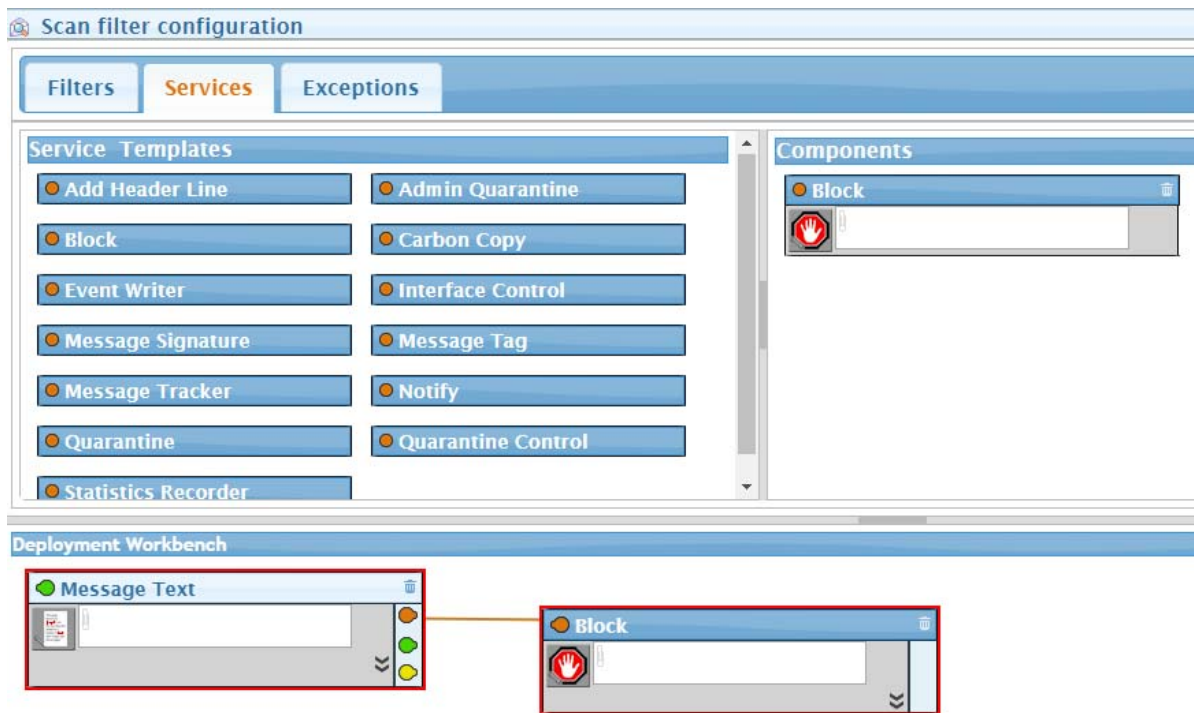
Click on the filter icon to open the filter criteria, enable all sources and enter, for this example, the word "unsubscribe". More words may be added, each on their own line.



The filter will now scan messages for the word unsubscribe, but without one or more services nothing will be done with the message.

Add Service

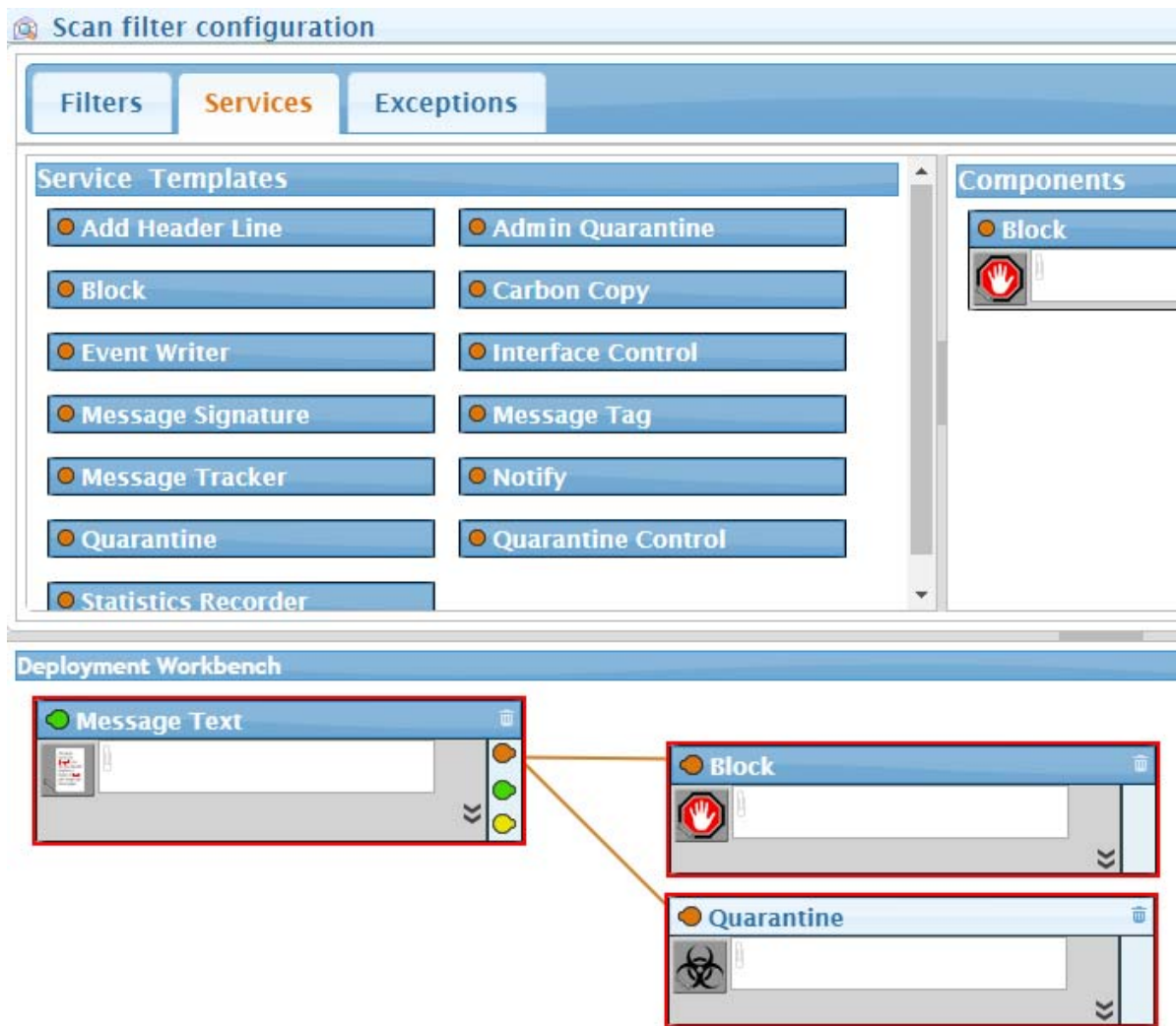
Select the *Services* tab and drag and drop the Block service to the workbench, or drag and drop the red Services pin and select Block.



Messages containing the word unsubscribe will now be blocked by Secure Messaging Gateway. However, some of your users may want to subscribe to certain newsletters so there needs to be a way to allow them to allow them through. That means Quarantining the messages.

Add the Quarantine Service

Select the *Services* tab and drag and drop the Quarantine service to the workbench, or drag and drop the red Services pin and select Quarantine.

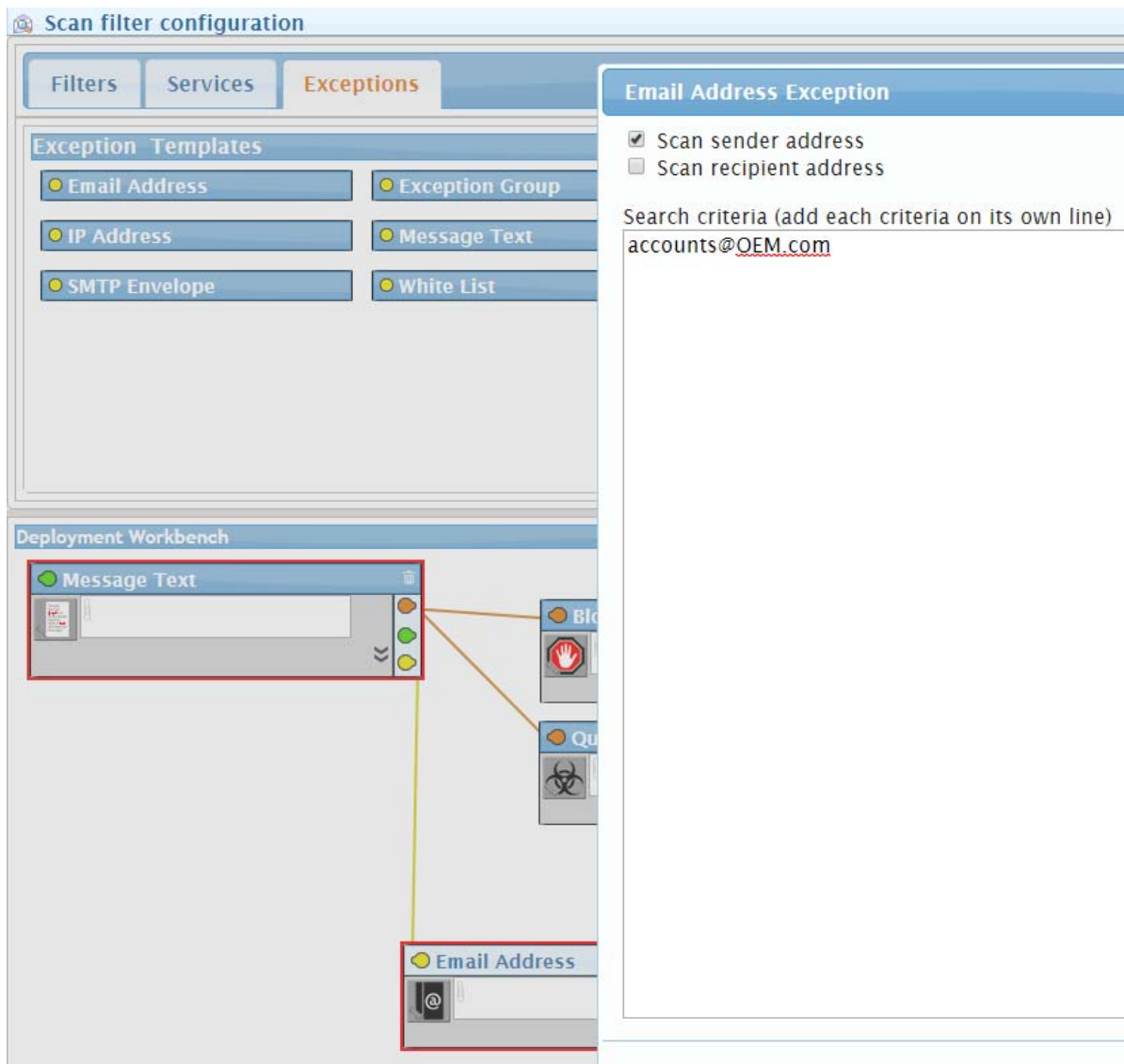


As part of the post-install tasks Quarantine digests and user auto-provisioning should have been configured. Now when messages containing the word unsubscribe enter the system, they are blocked and saved in the quarantine and a digest sent to the user to alert them to the quarantined message(s).

But there may be certain messages that have to get through from accounts at Overly Enthusiatic Marketing. An exception can be created.

Add an Exception

Select the *Exceptions* tab and drag and drop the Email Address exception to the workbench, or drag and drop the yellow Exceptions pin and select Email Address. Click on the icon of the exception to configure with an email address. In this example, accounts@OEM.com.



Click on *Save* and the policy will become active immediately.

Creating an Anti-Virus Policy

Creating a policy manually involves:

1. Creating the policy
2. Setting the policy priority, messages move through the policies from top to bottom
3. Set the policy message scan direction
4. Configuring the policy with filters, services and exceptions

For this example we will assume that a supplier has an overly enthusiastic marketing department and orders to reduce the amount of unwanted mail but allowing the desired mail through have come down.

In this case, the Inbound Mail Filter Policy is a wizard created policy that deals with general spam, and malware. However, unwanted message are getting through and need to be dealt with.

Create the Policy

Under *Organization / Policy Management | Policy Management*, click *Add New* to create a new policy and name it something easy to remember like *Anti-Virus Inbound Policy*.

Set the Policy Priority

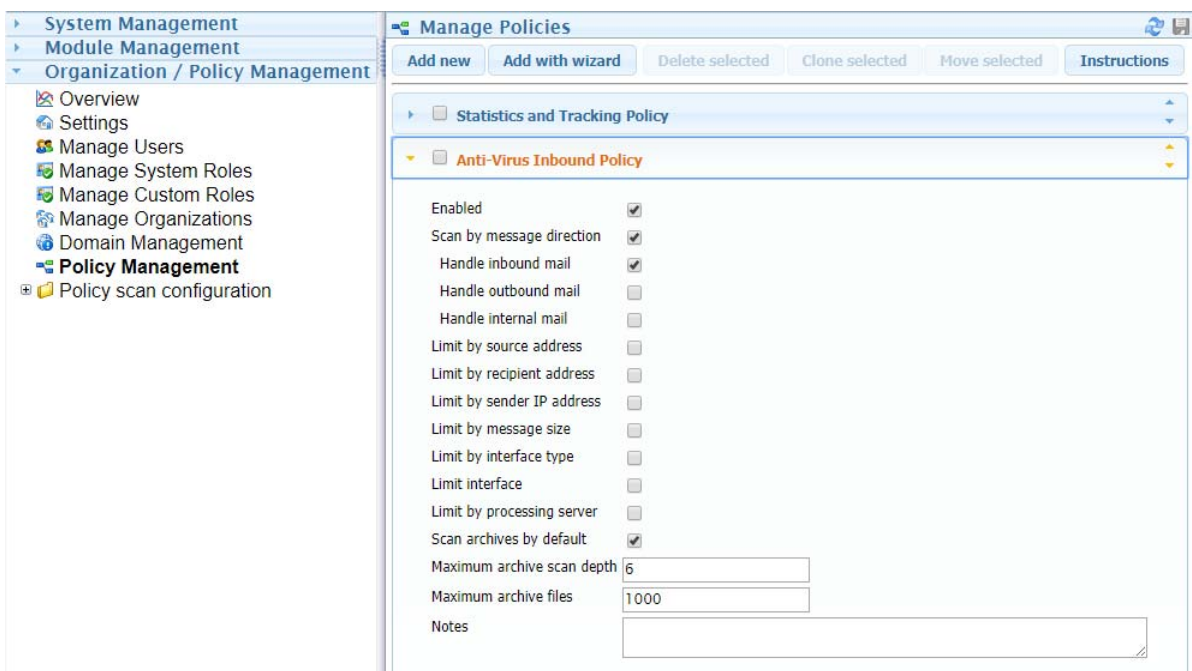
If you have more than one policy use the arrows on the right on the panel to move the policy to the top.

Messages move through policies from top to bottom. If a policy filters a message, for example an exception allows a message through, none of the lower policies will see the message.

As the unwanted messages are passing through the existing filters we will set the next filter below it.

Set the Policy Message Direction

Open the panel and enable *Scan by message direction* then enable *Handle inbound mail*.



Configure the Scanner

Open the *Policy scan configuration* folder and select the policy. The workbench will be empty.

Add the Filter

There are two filters that will block viruses: *Anti-Virus* and *Zero Hour Virus*.

Anti-Virus scans for known virus signatures and is updated no longer than hourly.

Zero Hour Virus uses a heuristic method of determining if the traits of a virus exist in a message. This functionality used to be combined into the *Anti-Virus* scanner. This may trigger false positives, so it has been broken out into its own filter so exceptions may be created while continuing to keep the attack surface as small as possible.

Drag the filters to the Workbench.

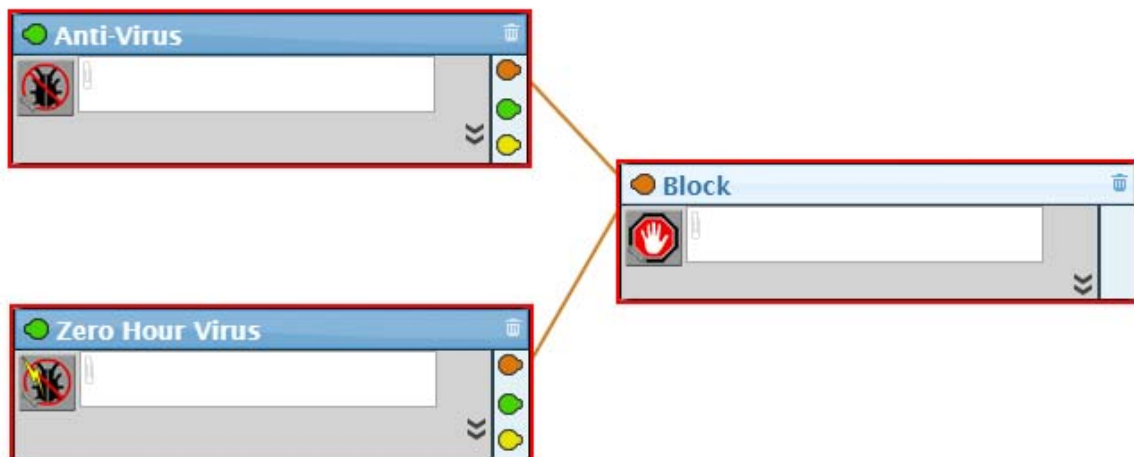
The filter will now scan messages for the word unsubscribe, but without one or more services nothing will be done with the message.

Add Service

Select the *Services* tab.

Because we do not want viruses to enter the system, drag and drop the *Block* service to the workbench, or drag and drop the red Services pin and select Block.

Connect the Red Services pin to the service with drop and drop.

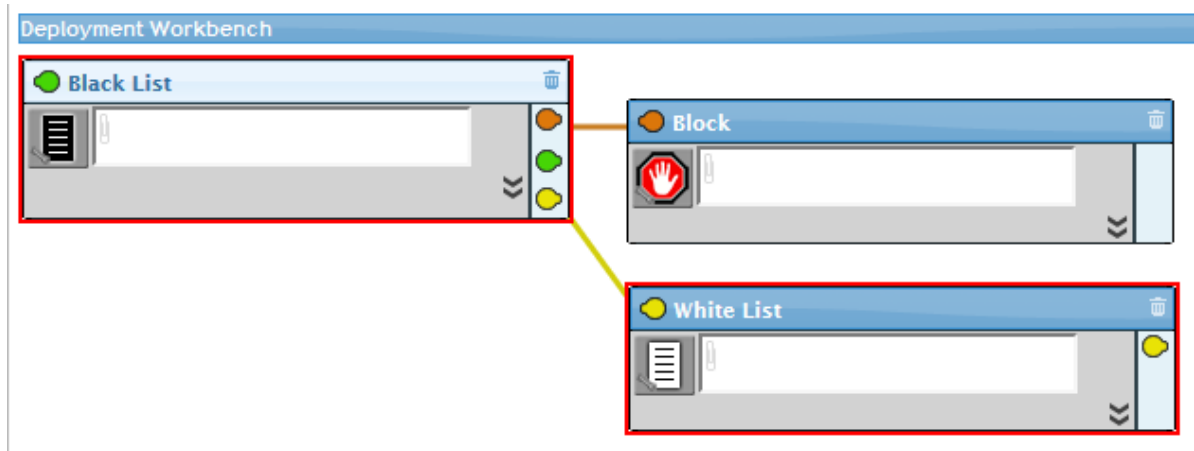


Press Save.

Items with viruses will now be blocked.

Enabling Black List and White List

To configure Black list and White list for users and groups in Secure Gateway you will first have to add the elements to a new or existing policy.



Configure Black list:

1. Add the Black list filter to a policy and connect it to a Block service.
2. Configure the Black list by clicking on the black list icon to open the configuration dialog box.

Black List

Black List Data Source [No data source] + 🔗

✓ Ok ⌂ Cancel

- From the Black List Data Source dropdown menu select a source or use the plus (+) button to create a data source. For example, "Black list addresses".

Black List

Black List Data Source Black list addresses + 🔗 🗑️

Sender Address	Recipient Address
<input type="text"/>	<input type="text"/>

- Link the data source to the QMS system by clicking on the link (chain) button. The data source will now have (QMS link) added to the name.

5. Sender and Recipient email addresses need to be added in pairs and can be added or removed in the configuration dialog box.
6. Press Ok.
7. Click the Save icon.

Configure White list:

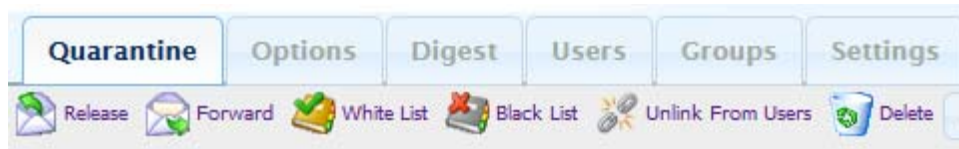
1. Add the White list exception to a policy and connect it to a Black list service.
2. Configure the White list by clicking on the white list icon to open the configuration dialog box.
3. From the White List Data Source dropdown menu select a source or use the plus(+) button to create a data source. For example, "White list addresses".

4. Link the data source to the QMS system by clicking on the link (chain) button. The data source will now have (QMS link) added to the name.

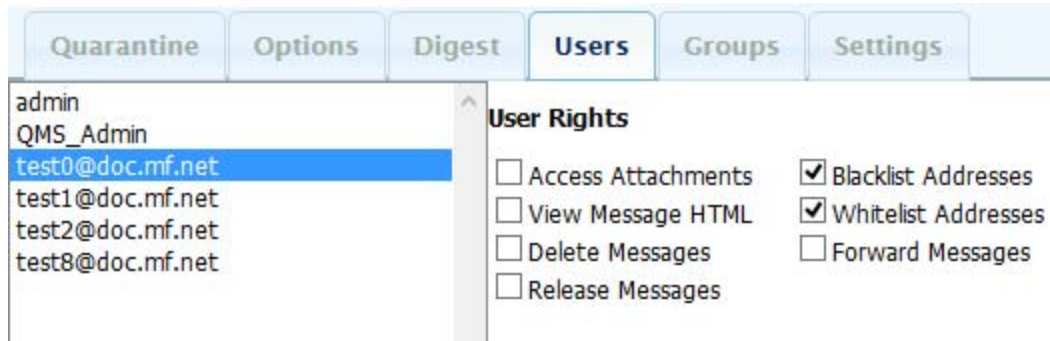
5. Sender and Recipient email addresses need to be added in pairs and can be added or removed in the configuration dialog box.
6. Press Ok.
7. Click the Save icon.

QMS Configuration

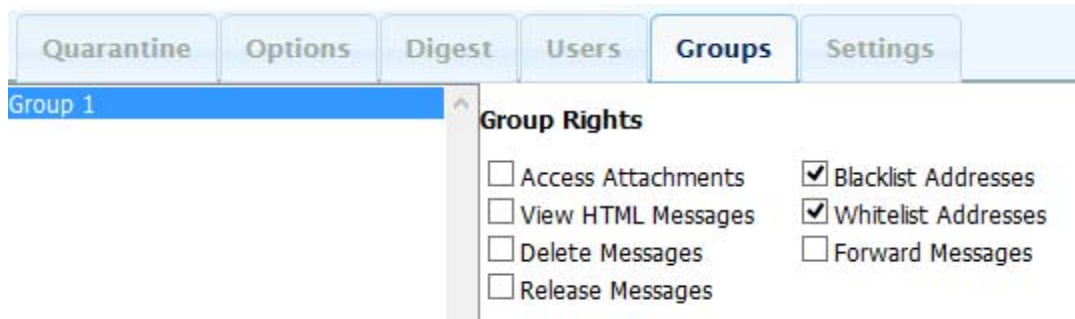
1. Log into the QMS as admin.
2. White list and Black list action buttons will appear in the Quarantine.



3. To grant users rights to use Black list and White list select a user from the User tab and enable the right.



4. To grant groups rights to use Black list and White list select a group the Group tab and enable the right.



Setting up DKIM Verification

Unlike the typical filter in Secure Messaging Gateway, instead of looking for things to filter a message out by, this will filter searches for something to allow a message in. Depending on the use case the "Invert mode logic" switch may be needed.

Blocking Messages Without a Valid DKIM Signature

This is useful for blocking spammers attempting to spoof a legitimate email domain.

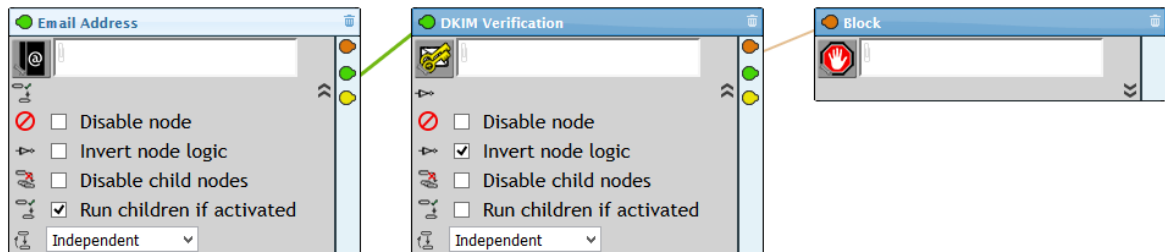
If you know that a sending domain applies DKIM signatures to all of their outbound

email, you can define a rule chain to protect against spoofed email attempts of that domain. This setup will start with an email address filter connected to a child DKIM filter, followed by a block service connected to the DKIM filter.

The address filter will be set to include sender addresses, and have a pattern for the source domain (i.e. *@microfocus.com). This primary address filter determines whether the DKIM filter will be checked. Enable Run children if activated so the rest of the chain will complete.

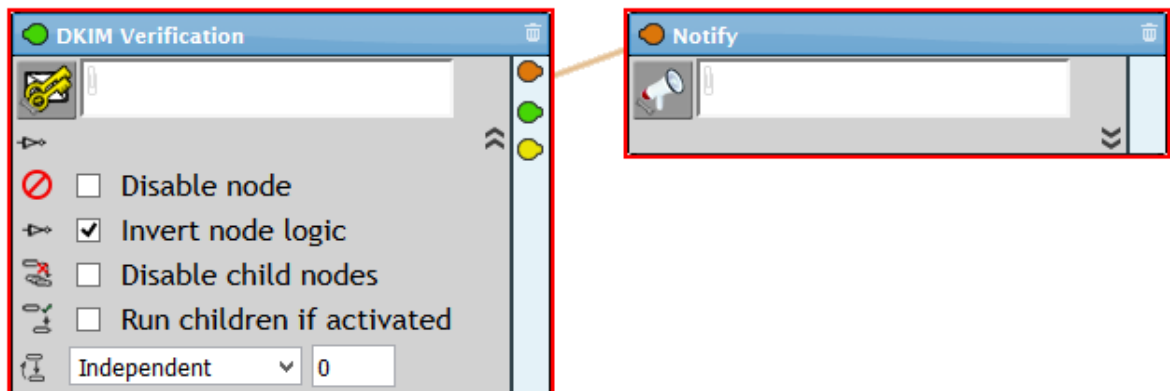
As the DKIM filter activates when a valid signature is detected, this node must be configured with 'Invert node logic' to detect messages that do not have a valid signature.

The results of this logic chain is, "If the email address IS from *@microfocus.com AND the DKIM signature IS NOT valid THEN block the message".



Sending a Notification That a Message Has a Valid DKIM Signature

This policy is useful to notify users that a message has a valid DKIM signature. While using a Tag service would appear to make sense, that would alter the message and break DKIM.



Configure the Notify Service to send a message alerting the user that the message has a valid DKIM signature. It is recommended to include the subject.

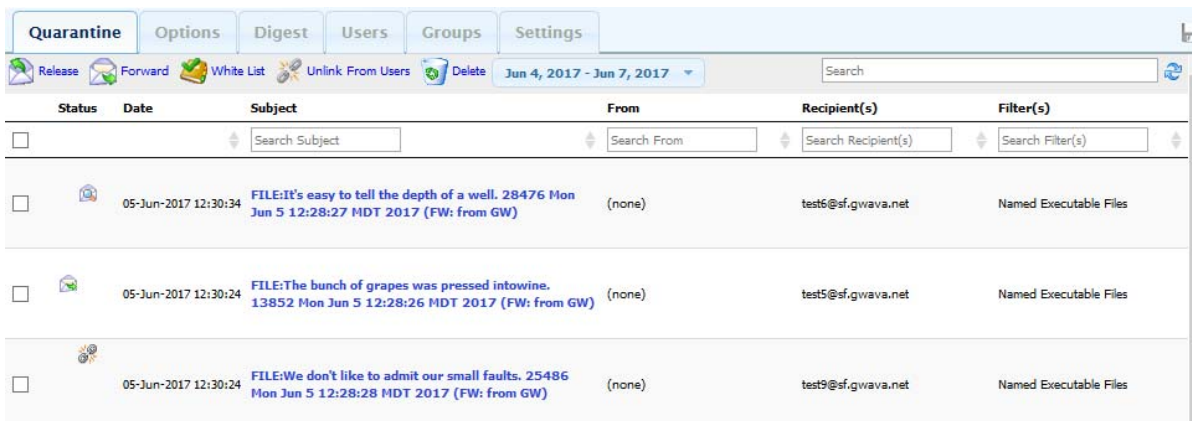
4 Quarantine System

From the login screen admin may choose to connect to the Quarantine System, if the user only has quarantine system rights they will be login directly into the Quarantine System.



Quarantine

As the *System Administrator* all quarantined messages will be shown.



Status	Date	Subject	From	Recipient(s)	Filter(s)
<input type="checkbox"/>		<input type="text" value="Search Subject"/>	<input type="text" value="Search From"/>	<input type="text" value="Search Recipient(s)"/>	<input type="text" value="Search Filter(s)"/>
<input type="checkbox"/>	05-Jun-2017 12:30:34	FILE:It's easy to tell the depth of a well. 28476 Mon Jun 5 12:28:27 MDT 2017 (FW: from GW)	(none)	test6@sf.gwava.net	Named Executable Files
<input type="checkbox"/>	05-Jun-2017 12:30:24	FILE:The bunch of grapes was pressed intowine. 13852 Mon Jun 5 12:28:26 MDT 2017 (FW: from GW)	(none)	test5@sf.gwava.net	Named Executable Files
<input type="checkbox"/>	05-Jun-2017 12:30:24	FILE:We don't like to admit our small faults. 25486 Mon Jun 5 12:28:28 MDT 2017 (FW: from GW)	(none)	test9@sf.gwava.net	Named Executable Files

A *QMS Administrator* will have access to all quarantined messages as well as their own quarantine area through the toggle button



Quarantine Options Digest Users Groups Settings						
Release Forward White List Unlink From Users Delete Jun 9, 2017 - Jun 12, 2017						
Status	Date	Subject	From	Recipient(s)	Filter(s)	
<input type="checkbox"/>		<input type="text" value="Search Subject"/>	<input type="text" value="Search From"/>	<input type="text" value="Search Recipient(s)"/>	<input type="text" value="Search Filter(s)"/>	
<input type="checkbox"/>	12-Jun-2017 12:33:36	He smoke a big pipe with strong contents. 1907555452	script@sf.gwava.net	test4@doc.mf.net	Message Text	

A QMS User will only have access to their own quarantine area.

Quarantine Options						
Release Forward White List Delete Jun 9, 2017 - Jun 12, 2017 Search						
Status	Date	Subject	From	Filter(s)		
<input type="checkbox"/>		<input type="text" value="Search Subject"/>	<input type="text" value="Search From"/>	<input type="text" value="Search Filter(s)"/>		
<input type="checkbox"/>	12-Jun-2017 12:05:15	The case was puzzling to the old and wise. 7452003	script@sf.gwava.net	Message Text		

Show 20 messages

Showing 1 to 1 of 1 messages

First Previous 1 Next Last

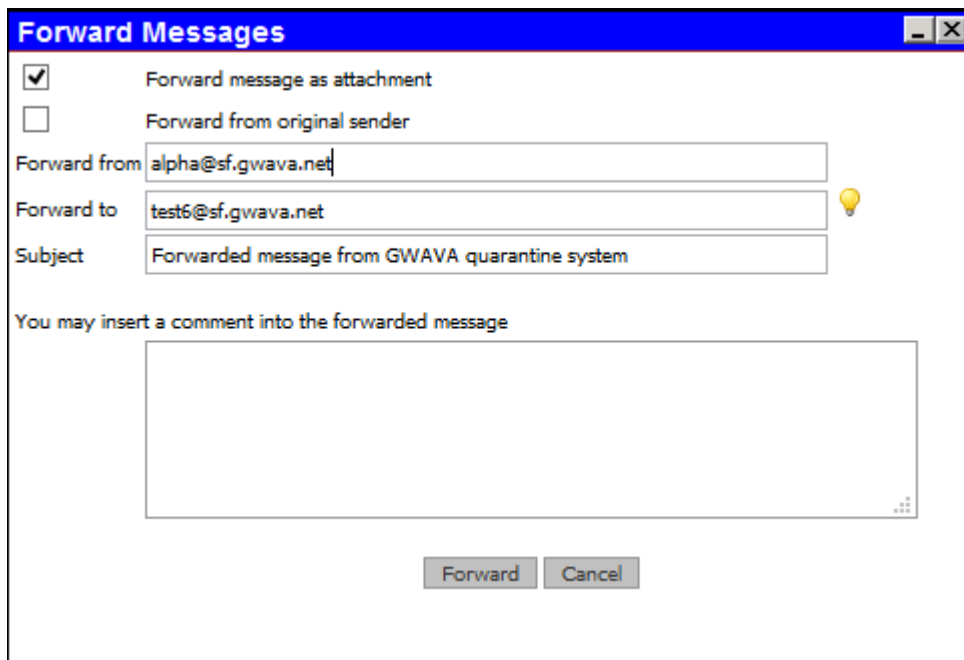
Columns with up and down arrows, including Date, Subject, From and Filters, can be used to sort the messages.

From here the following actions can be taken to the message after selecting one or more messages using the checkbox on the left:

View a message by clicking on the Subject. Viewed messages will have an open envelope with magnifying glass icon in the Status column.

Release: Allow the messages to continue to the user's mailbox. Released messages will disappear from quarantine. A confirmation dialog box will appear.

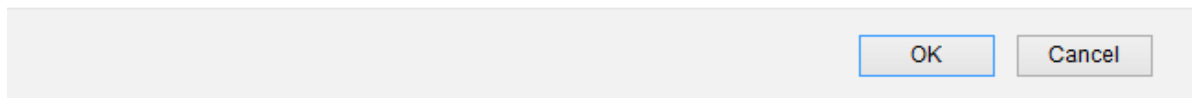
Forward: Send the message to another user's mailbox. Fill in the dialog box. Forwarding does not remove the message from quarantine. Forwarded messages will have an open envelope with forwarding arrow on it in the Status column.



White List: Add the sender to the white list to bypass quarantine. A warning dialog box will appear. White listed messages will disappear from quarantine.

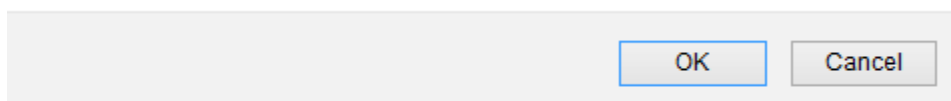
Adding the selected item to the whitelist will allow future messages from this e-mail address to be delivered you. The whitelist can be managed from the options page if you want to remove entries at a later time.

Are you sure you want to whitelist the selected sender address?



Unlink from Users: Removes the message from the personal quarantine of the recipients, but leaves it in the administrator quarantine. A warning dialog box will appear. A broken chain icon will appear in the Status column.

Are you sure you want to unlink the selected message from the owner's quarantine?



Delete: Removes the message from the system. A confirmation dialog box will appear.

Date Range: Clicking on the date range specifies the time frame to be displayed.

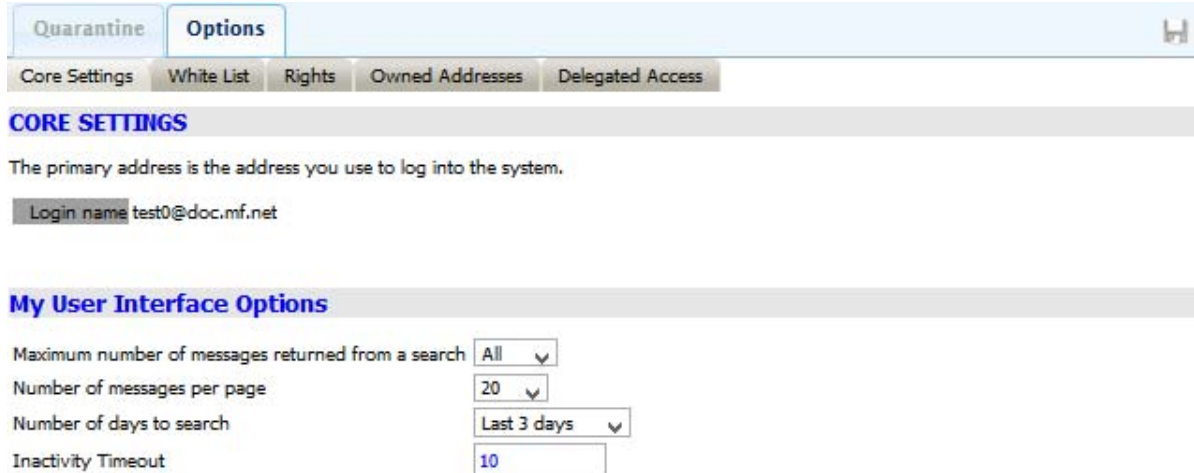


Options

The Options tab provides access to setting information.

Core Settings

Core Setting are the user definable options available.



The primary address is the address you use to log into the system.

Maximum number of messages returned from a search. Default, All.

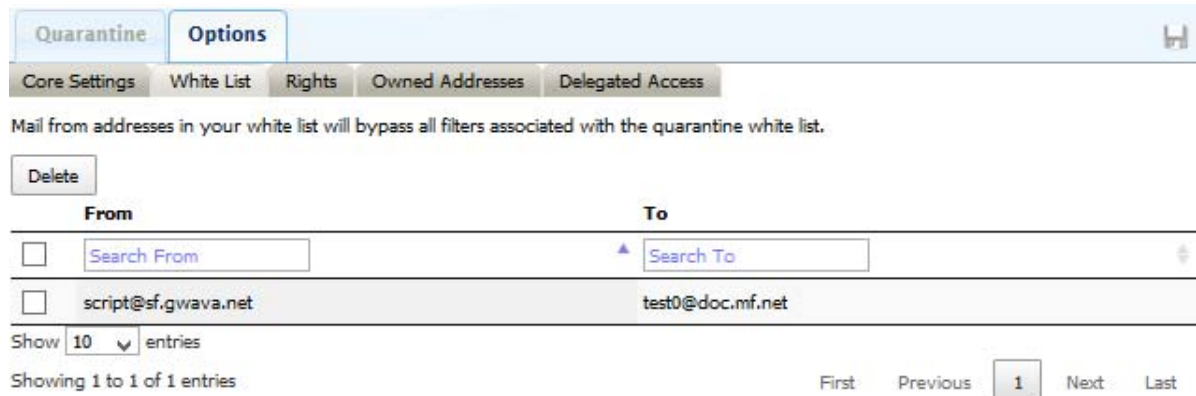
Number of messages per page. Default, 20.

Number of days to search. Default, Last 3 days.

Inactivity Timeout. Default, 10 minutes.

White List

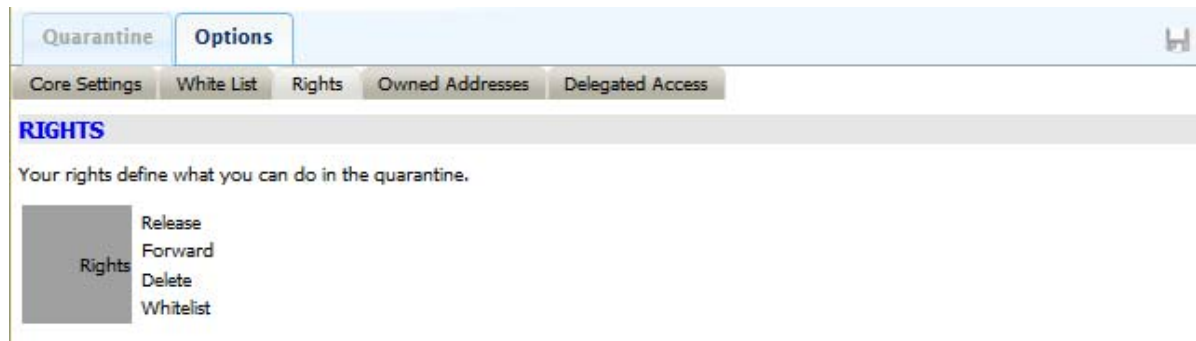
Items added to the white list from the Quarantine page are listed here.



Items may be removed from the white list by selecting and pressing the Delete button.

Rights

The Rights tab shows the rights granted to the currently logged in user.



An Administrator user can change the rights granted in the *System Administration | Organization / Policy Management | Manage Users* page.

Owned Addresses

A user can view the quarantines of the listed mailboxes. These are considered part of the identity of the logged in user.

Add an owned address by clicking *Add* and providing a valid address and password.

Remove an owned address by selecting one or more addresses and clicking on *Delete*.

Quarantine Options

Core Settings White List Rights Owned Addresses Delegated Access

Owned Addresses

These are all of the e-mail addresses that the quarantine system considers to be a part of your identity when viewing messages. 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 any of these email addresses
- Add additional addresses, if you can authenticate with the email address. (If you cannot authenticate, your quarantine administrator may add them for you)

Delete Add

Address	
<input type="checkbox"/>	Search Address
<input type="checkbox"/>	test1@doc.mf.net

Show 10 entries

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Delegated Access

A user can grant another user the rights to access and manage their quarantine.

Add a delegate user by clicking *Add* and providing the email address. This grants the right to view the quarantine.

Remove a delegate by selecting one or more names and clicking on *Delete*.

Grant/revoke additional rights to the delegate user:


Delete: Allows/denies delegate to delete messages from quarantine.

Release: Allows/denies delegate to release messages from quarantine.

Forward: Allows/denies delegate to forward message from quarantine.

Blacklist: Allows/denies delegate to add addresses to the blacklist.

Whitelist: Allows/denies delegate to add addresses to the whilelist.

Quarantine Options 

Core Settings White List Rights Owned Addresses **Delegated Access**

Delegated Access

These are all the users you have granted access to your quarantine and the permissions you have given them. You may:

- Revoke access to your quarantine by deleting the user
- Grant access to your quarantine by adding users to this list
- Alter the permissions for any of the users

Login Name	Delete	Release	Forward	Blacklist	Whitelist
<input type="checkbox"/> <input type="text" value="Search Login Name"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> test2@doc.mf.net	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

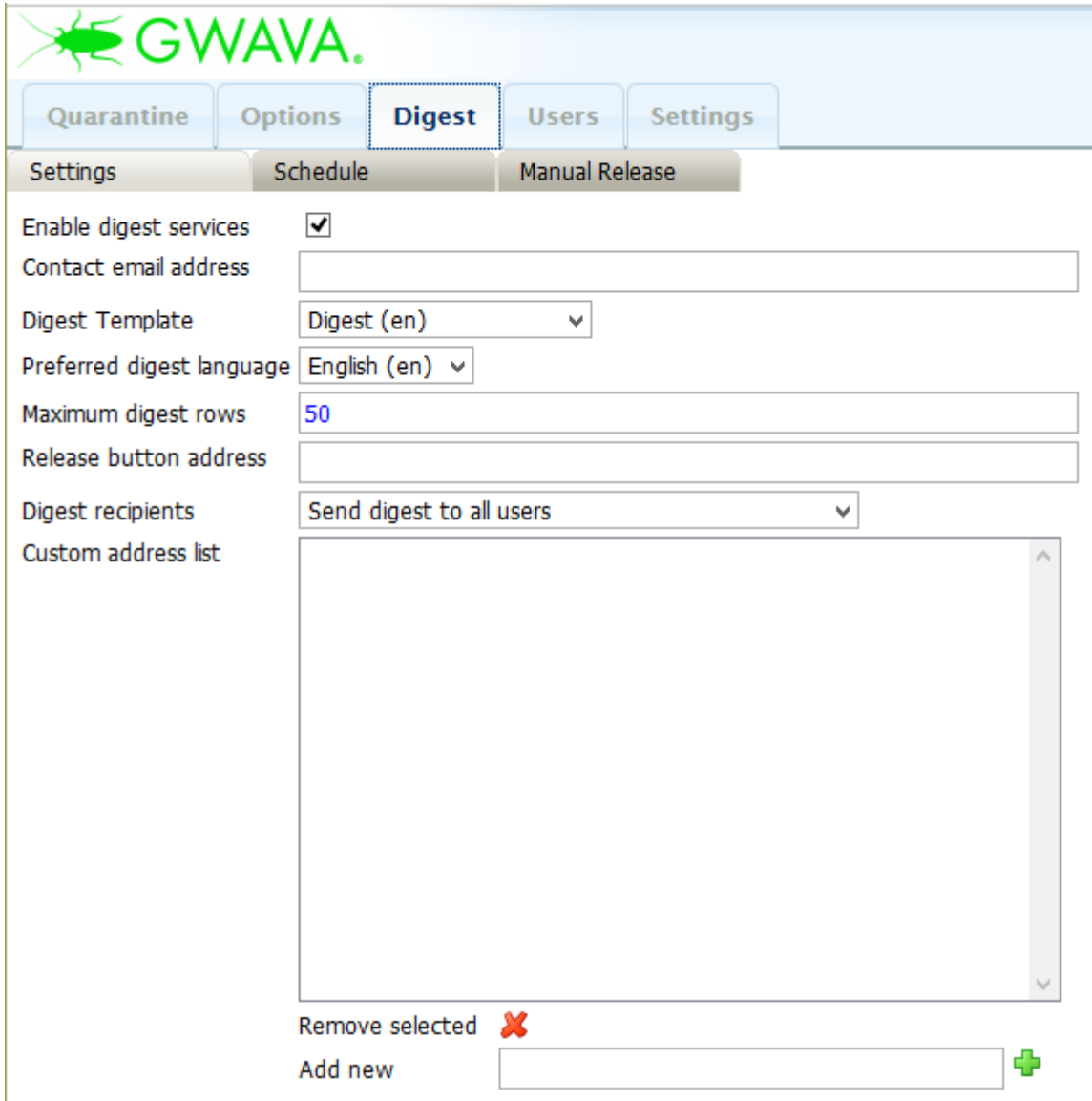
Show entries

Showing 1 to 1 of 1 entries First Previous **1** Next Last

Digest

Digests are sent to users to alert them that messages are in their quarantine.

Settings Tab



The screenshot shows the GWAVA interface with the 'Digest' tab selected. The 'Settings' sub-tab is active. The 'Enable digest services' checkbox is checked. The 'Contact email address' field is empty. The 'Digest Template' dropdown is set to 'Digest (en)'. The 'Preferred digest language' dropdown is set to 'English (en)'. The 'Maximum digest rows' field contains the value '50'. The 'Release button address' field is empty. The 'Digest recipients' dropdown is set to 'Send digest to all users'. The 'Custom address list' is an empty text area with a scroll bar. Below the text area are buttons for 'Remove selected' (with a red X icon) and 'Add new' (with a green plus icon and an empty input field).

Enable digest services: Default, disabled.

Contact email address: The email address the user can use to contact help to enter their quarantine. Default, blank.

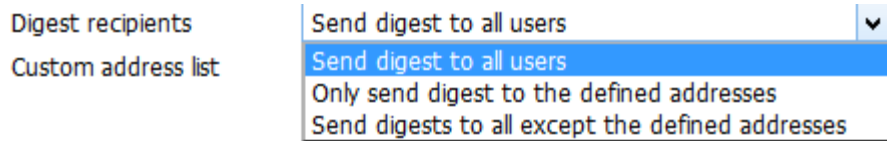
Digest Template: The default template selected in *System Administration | System Management | Templates*. Default, Digest (en).

Preferred digest language: The language the digest should use. Languages can be enabled under *System Administration | System Management | Languages*. Default, English (en).

Maximum digest rows: The maximum number of items shown in the digest. Default, 50.

Release button address:

Digest recipients: The recipients that should receive digest emails.



Send digest to all users (Default)

- ◆ Only send digest to the defined addresses

Send digest to all except the defined addresses

Custom address list. The list of addresses to be used by the system.

Schedule Tab

Under the *Schedule* sub tab select a day or time for the digests to be sent to users with quarantined messages. Generally, this will be set to once or twice a weekday.

Click on the Time row to select the entire row, click on the Day column to select an entire day, or the top corner for all.

Quarantine		Options		Digest		Users		Groups		Settings	
Settings			Schedule				Manual Release				
	Sun	Mon	Tue	Wed	Thu	Fri	Sat				
Midnight	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
1:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
2:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
3:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
4:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
5:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
6:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
7:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
8:00am	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
9:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
10:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
11:00am	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
Midday	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
1:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
2:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
3:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
4:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
5:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
6:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
7:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
8:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
9:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
10:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
11:00pm	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				

Manual Release Tab


Beyond the standard digest setup, certain custom options can be set.

[Quarantine](#)[Options](#)[Digest](#)[Users](#)[Settings](#)[Settings](#)[Schedule](#)[Manual Release](#)

Digest release period

No global digest time has been sent. The default digest time period is 24 hours.

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  03 ▾ May ▾ 2017 ▾ 13 ▾ 09 ▾ [Set](#)

Custom digest release

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

Start date  03 ▾ May ▾ 2017 ▾ 13 ▾ 09 ▾

End date  04 ▾ May ▾ 2017 ▾ 13 ▾ 09 ▾

Select users:

admin

release this address

release to all users ([with global digest rules](#))

update global digest start period on release to all

[send digest](#)

Digest release period

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.

Custom digest release

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

Start date

End date

Select users

Release this address

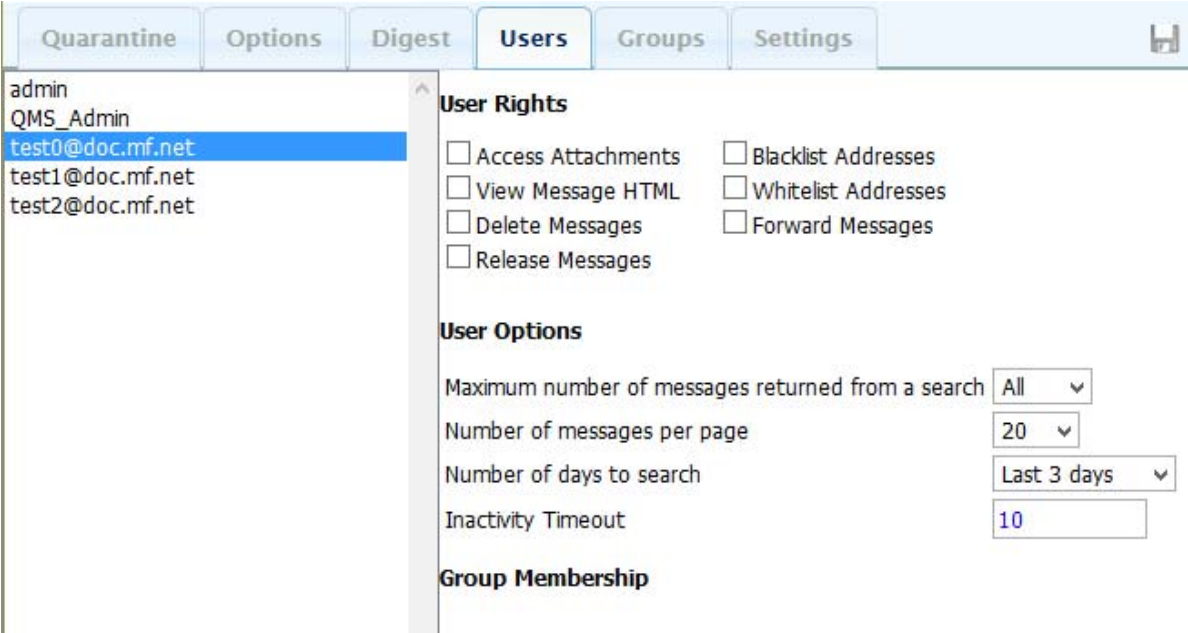
Release to all users (with global digest rules)

Update global digest start period on release to all

Send digest: This button sends a digest immediately.

Users

User rights can be managed at the user level in this interface.



The screenshot shows a web interface for managing users. At the top, there are tabs for Quarantine, Options, Digest, Users, Groups, and Settings. The 'Users' tab is active. On the left, a list of users is shown: admin, QMS_Admin, test0@doc.mf.net (highlighted), test1@doc.mf.net, and test2@doc.mf.net. The right side of the interface displays the configuration for the selected user, test0@doc.mf.net. It is divided into three sections: 'User Rights' with checkboxes for Access Attachments, View Message HTML, Delete Messages, Release Messages, Blacklist Addresses, and Whitelist Addresses; 'User Options' with dropdown menus for 'Maximum number of messages returned from a search' (set to All), 'Number of messages per page' (set to 20), and 'Number of days to search' (set to Last 3 days), and a text input for 'Inactivity Timeout' (set to 10); and 'Group Membership'.

User Rights

System Administrator or QMS Administrator users can modify these rights.

Access Attachments

View Message HTML

Delete Messages

Release Messages

Blacklist Addresses

Whitelist Addresses

Forward Messages

User Options

Maximum number of messages returned from a search

100

200

500

1000

All (Default)

Number of messages per page

10

20 (Default)

50

100

All

Number of days to search

Last 24 hours

Last 2 days

Last 3 days (Default)

Last 7 days

Last 30 days

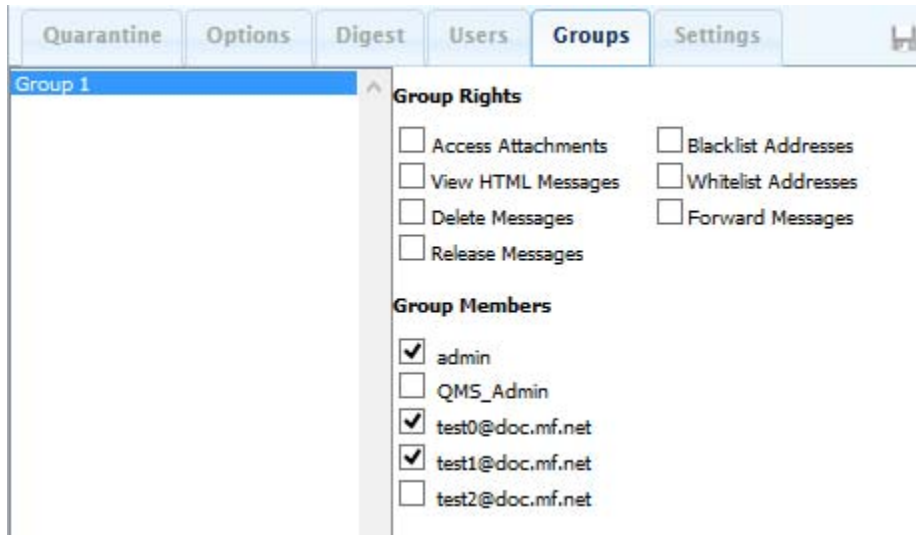
Inactivity Timeout: Default 10 minutes.

Group Membership

The list of groups the user is a member of.

Groups

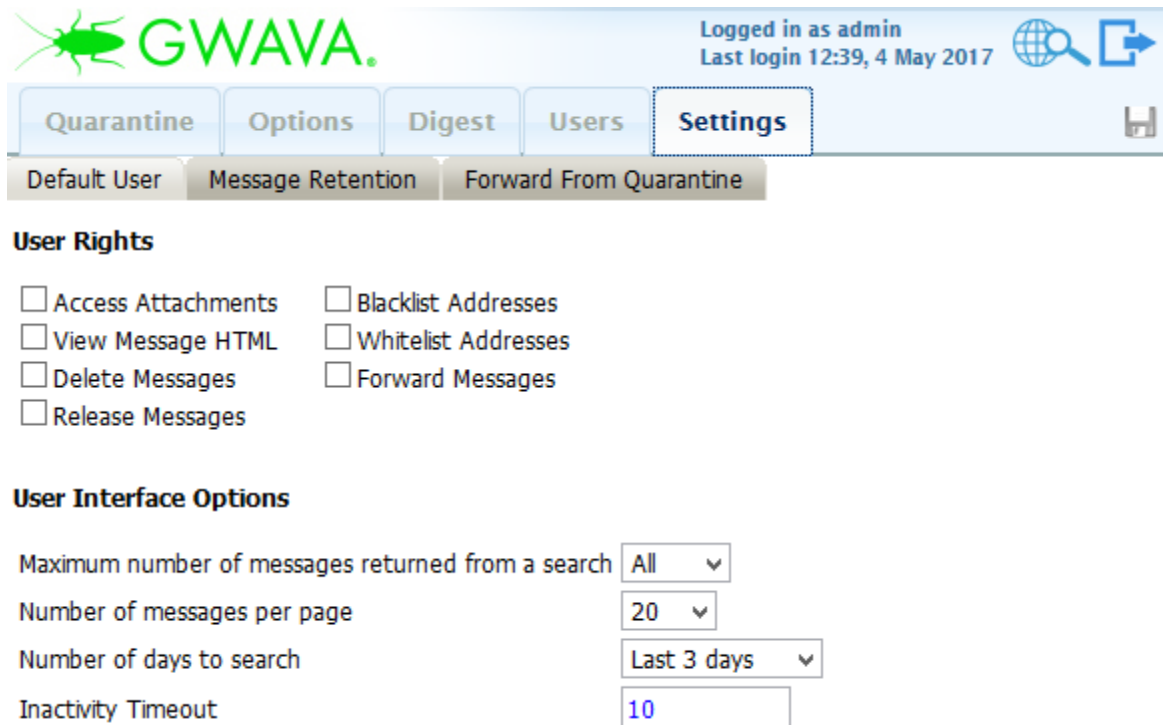
Users can be organized into Groups to make management easier.



Groups are created by the System Administrator as a [Custom Role \(Manage_Custom_Roles.htm#Creating_a_Group\)](#).

Settings

Settings for the default user, how long messages are retained and forwarded, can be set under this tab.



Default User

User Rights

Access Attachments

View Message HTML

Delete Messages

Release Messages

Blacklist Addresses

Whitelist Addresses

Forward Messages

User Interface Options

Maximum number of messages returned from a search

100

200

500

1000

All (Default)

Number of messages per page

10

20 (Default)

50

100

All

Number of days to search

Last 24 hours

Last 2 days

Last 3 days (Default)

Last 7 days

Last 30 days

Inactivity Timeout. Default, 10 minutes.

Message Retention



Message Retention Policy

Enable quarantine message pruning	<input checked="" type="checkbox"/>
Days to retain messages in quarantine	<input type="text" value="60"/>
Prune message information	<input checked="" type="checkbox"/>
Delete stored messages	<input checked="" type="checkbox"/>

Enable quarantine message pruning: Default, enabled.

Days to retain messages in quarantine: Default, 60.

Prune message information: Default, enabled.

Delete stored messages: Default, enabled.

Forward from Quarantine



Forward From Quarantine

Forward as an attachment template	<input type="text" value="Forward From Quarantine (en)"/>
Preferred forward as an attachment language	<input type="text" value="English (en)"/>

Forward as an attachment template: Default, Forward From Quarantine (en).

Preferred forward as an attachment language: Default, English (en).

5 Message Tracker

Select the Message Tracker when logging in to view.



Message Tracker interface

The message tracker interface allows messages to be tracked through the system.

Each column can be sorted by clicking on the arrows.

Jun 19, 2017 Search

Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address
19-Jun-2017 12:34:44 pm	A blue crane is a tall wading bird. 478685461	script@sf.gwava.net	test7@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:34:22 pm	His hip struck the knee of the next player. 1988893851	script@sf.gwava.net	test9@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:34:00 pm	The goose was brought straight from the old market. 1462980723	script@sf.gwava.net	test8@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:33:38 pm	Screen the porch with woven straw mats. 1170864218	script@sf.gwava.net	test5@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:33:27 pm	The sand drifts over the sills of the old house. 376325950	script@sf.gwava.net	test6@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:33:05 pm	Go now and come here later. 423062554	script@sf.gwava.net	test4@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:32:43 pm	The marsh will freeze when cold enough. 1002658249	script@sf.gwava.net	test3@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:32:21 pm	Port is a strong wine with a smoky taste. 840402094	script@sf.gwava.net	test1@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:31:59 pm	Take shelter in this tent, but keep still. 238750082	script@sf.gwava.net	test2@doc.mf.net	internal	none	151.155.183.142
19-Jun-2017 12:31:37 pm	A six comes up more often than a ten. 1636634308	script@sf.gwava.net	test0@doc.mf.net	internal	none	151.155.183.142

Show 10 messages

Showing 1 to 10 of 424 Print Copy CSV Excel PDF Column visibility First Previous 1 2 3 4 5 ... 43 Next Last

Messages can be shown in groups of 10, 20, 50, 100 or All.

The amount of message visible is shown at the lower left.

The list of messages can be printed, copied, saved to CSV, Excel or PDF formats.

Column visibility can be selected under the button.



Search

Each column can be searched individually.

Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address
Date	<input type="text" value="river"/>	<input type="text" value="Search Sender"/>	<input type="text" value="Search Recipient(s)"/>	<input type="text" value="Search Direction"/>	<input type="text" value="Search Block State"/>	<input type="text" value="Search Sending IP Address"/>
19-Jun-2017 01:02:17 am	The source of the huge river is the clear spring. 16922 Mon Jun 19 01:00:02 MDT 2017 (Forward from GW)	(none)	Alan@sf.gwava.net	inbound	none	151.155.183.147
19-Jun-2017 01:02:25 pm	Watch the log float in the wide river. 13915 Mon Jun 19 13:00:08 MDT 2017 (FW: from GW)	(none)	test6@doc.mf.net	inbound	none	151.155.183.142

Then entire date range can be searched using the search box to find specific messages. Press the search refresh button to clear the search and refresh the list.

Jun 19, 2017							<input type="text" value="Tire"/>
Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address	
Date	<input type="text" value="Search Subject"/>	<input type="text" value="Search Sender"/>	<input type="text" value="Search Recipient(s)"/>	<input type="text" value="Search Direction"/>	<input type="text" value="Search Block State"/>	<input type="text" value="Search Sending IP Address"/>	
19-Jun-2017 08:32:22 am	The tube was blown and the tire flat and useless. 400867366	script@sf.gwava.net	test4@doc.mf.net	internal	full	151.155.183.142	
19-Jun-2017 06:02:24 am	A sip of tea revives his tired friend. 3287 Mon Jun 19 06:00:10 MDT 2017 (FW: from GW)	(none)	test8@sf.gwava.net	inbound	none	151.155.183.147	
19-Jun-2017 06:02:24 am	A sip of tea revives his tired friend. 3287 Mon Jun 19 06:00:10 MDT 2017 (FW: from GW)	(none)	test8@doc.mf.net	inbound	none	151.155.183.142	
19-Jun-2017 04:02:30 am	A sip of tea revives his tired friend. 12979 Mon Jun 19 04:00:07 MDT 2017 (FW: from GW)	(none)	test2@doc.mf.net	inbound	none	151.155.183.142	
19-Jun-2017 04:02:19 am	A sip of tea revives his tired friend. 12979 Mon Jun 19 04:00:07 MDT 2017 (FW: from GW)	(none)	test2@sf.gwava.net	inbound	none	151.155.183.147	

Show 10 messages

Showing 1 to 5 of 5 (filtered from 424 total messages) First Previous Next Last

Date Range

Change the visible date range by selecting the Date drop down menu.

Jun 19, 2017

Today
 Yesterday
 This week
 Last week
 This month
 Last month
 This year

April 2017							May 2017							June 2017								
Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa		
						1		1	2	3	4	5	6							1	2	3
2	3	4	5	6	7	8	7	8	9	10	11	12	13	4	5	6	7	8	9	10		
9	10	11	12	13	14	15	14	15	16	17	18	19	20	11	12	13	14	15	16	17		
16	17	18	19	20	21	22	21	22	23	24	25	26	27	18	19	20	21	22	23	24		
23	24	25	26	27	28	29	28	29	30	31				25	26	27	28	29	30			
30																						

Apply Clear Cancel

Message Details

Click on a message to bring up a details dialog box. The policy and filters that triggered on the message will be shown.

Message Details
✕

Date: 19-Jun-2017 11:34:47 am

Subject: Press the pants and sew a button on the vest. 308825513

Sender: script@sf.gwava.net

Policy: Inbound Mail Filter Policy

Recipients: test8@doc.mf.net

Filters: IN Message Received
Message Text

6 User Guide

Quarantine Management System

The Micro Focus Secure Messaging Gateway is a gatekeeper that stands between the internet and your company's email system. It filters out emails that have viruses in them or are spam. Most of the time it takes care of them silently but occasionally there will be emails that it is not sure about and your system administrator has configured Secure Messaging Gateway to stop the delivery of the suspicious mail but let you know that it is waiting outside by sending you an email. The suspicious email is held in the Quarantine.

Quarantine Email

You may receive a message from Secure Messaging Gateway to let you know that a message is being held in the quarantine.

It will look something like this.



E-Mail Restriction Report

One message was quarantined on 18-Aug-2017

The e-mail listed below were quarantined by Secure Gateway and may be unsolicited (SPAM). To retrieve a message, click the Release button and a copy of the message will be sent to you.

[Manage my quarantine](#)

Reason	Subject	Sender	Date	Action
Email Address	These days a chicken leg is a rare dish. 25934 Fri Aug 18 12:00:07 MDT 2017 (FW: from GW)		18 Aug 2017 12:00:24 PM	Release

www.gwava.com • [About Secure Gateway](#)

Copyright © 2016. GWAVA, Inc., a Micro Focus Company. All rights reserved. Content may not be reproduced without permission.

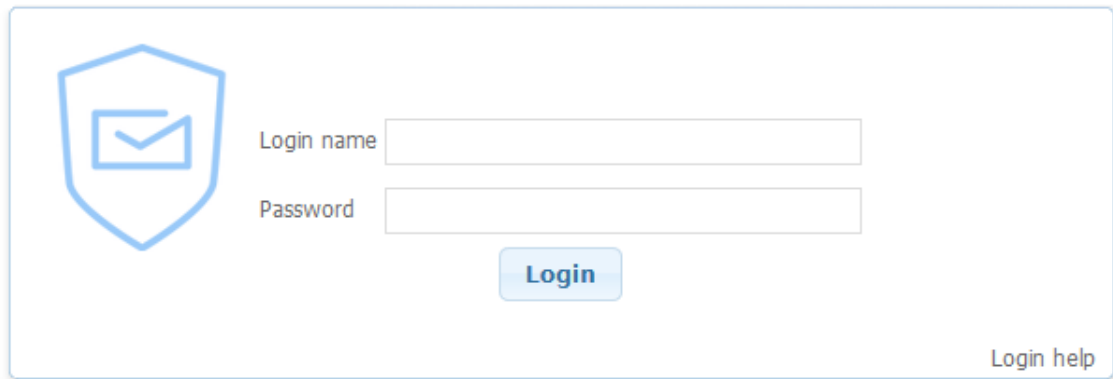
If you believe the message was quarantined in error, you can allow delivery to be completed by taking the Release action at the far right.

You can also manage your quarantine by clicking on the "Manage my Quarantine" button.

Quarantine Management System

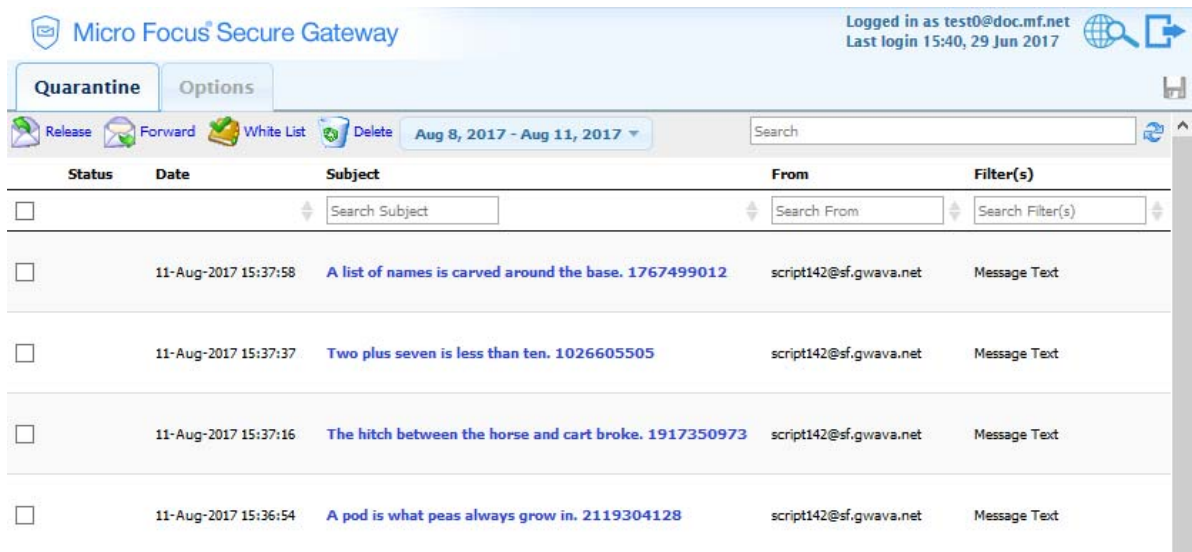
You can manage your quarantine by logging into the Quarantine Management System (QMS) using your email credentials.

Micro Focus® Secure Gateway



The login form features a shield icon with an envelope inside on the left. To its right are two input fields: 'Login name' and 'Password'. Below these fields is a blue 'Login' button. In the bottom right corner, there is a link for 'Login help'.

This brings you to the main quarantine screen in the QMS.

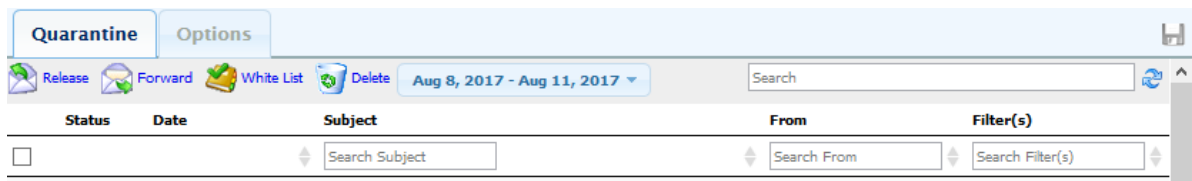


The screenshot shows the 'Quarantine' tab selected in the Micro Focus Secure Gateway interface. The user is logged in as 'test0@doc.mf.net' with a last login of '15:40, 29 Jun 2017'. The interface includes a toolbar with 'Release', 'Forward', 'White List', and 'Delete' actions, and a date range filter set to 'Aug 8, 2017 - Aug 11, 2017'. A search bar is present. Below the toolbar is a table of quarantined messages.

Status	Date	Subject	From	Filter(s)
<input type="checkbox"/>		<input type="text" value="Search Subject"/>	<input type="text" value="Search From"/>	<input type="text" value="Search Filter(s)"/>
<input type="checkbox"/>	11-Aug-2017 15:37:58	A list of names is carved around the base. 1767499012	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:37:37	Two plus seven is less than ten. 1026605505	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:37:16	The hitch between the horse and cart broke. 1917350973	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:36:54	A pod is what peas always grow in. 2119304128	script142@sf.gwava.net	Message Text

Quarantine Actions

From here you may take action on one or more of the quarantined emails. Select one or more messages using the checkbox on the right.



This screenshot is identical to the one above, showing the 'Quarantine' tab and the toolbar with 'Release', 'Forward', 'White List', and 'Delete' actions.

- ◆ *Release*: Releases the select message from the quarantine to be delivered to your mailbox.
- ◆ *Forward*: Allows you to forward the message to an email address other than your own.
- ◆ *White List*: Adds the sender's email address to your white list so they will not be quarantined. This can be managed under the Options tab.

- ◆ Delete: Immediately deletes the message from quarantine and does not deliver it.
- ◆ *Date Range*: Clicking on the date range specifies the time frame to be displayed.



- ◆ Search: Allows you to search the entire message in the quarantine for the keyword(s).

The Subject, From and Filter(s) search fields will only search those specific fields.

Clicking on the Recycle button will clear the search field.

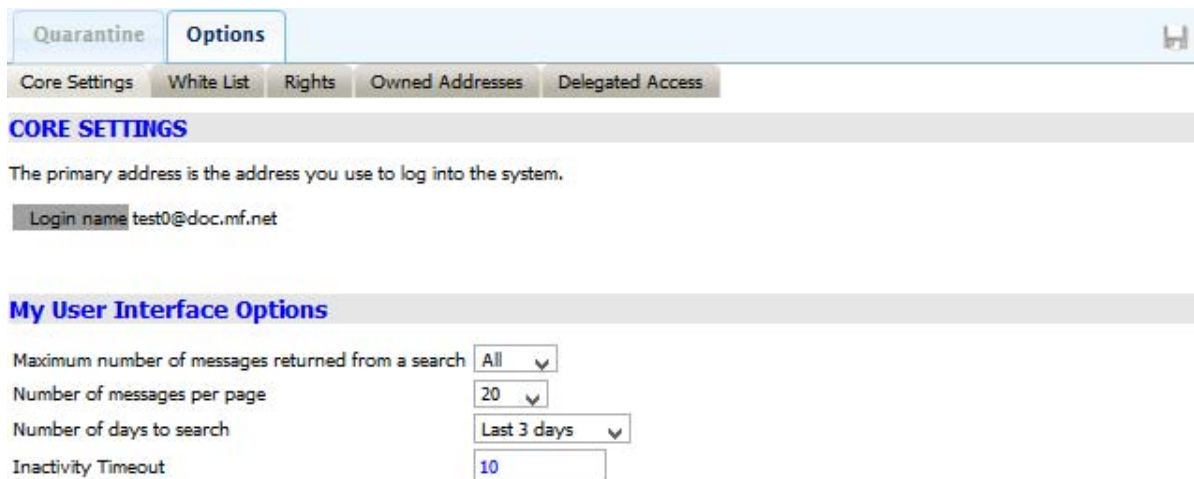
You can sort by the Date, Subject, From or Filter(s) column by clicking on the arrows

Options

The Options tab provides access to settings information. You may use this to customize your quarantine.

Core Settings

Core Setting are the available user definable options.



The *primary address* is the address you use to log into the system.

Maximum number of messages returned from a search. Default, All.

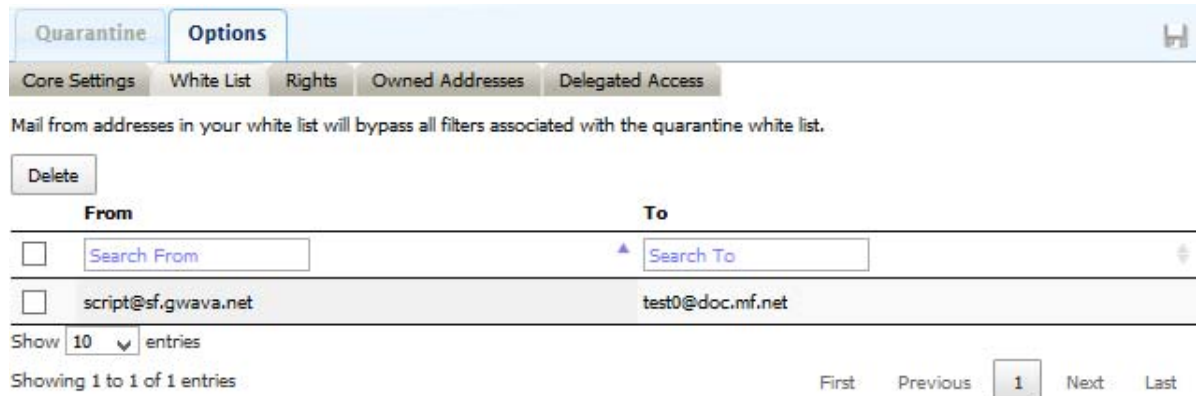
Number of messages per page. Default, 20.

Number of days to search. Default, Last 3 days.

Inactivity Timeout. Default, 10 minutes.

White List

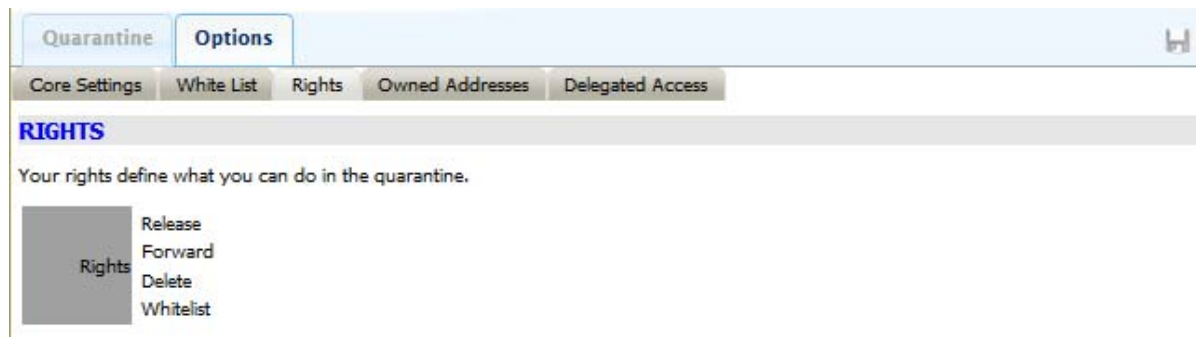
Items added to the white list from the Quarantine page are listed here.



Items may be removed from the white list by selecting and pressing the Delete button.

Rights

The Rights tab shows the rights granted to the currently logged in user.



An Administrator user can change the rights granted in the *System Administration | Organization / Policy Management | Manage Users* page.

Owned Addresses

A user can view the quarantines of the listed mailboxes. These are considered part of the identity of the logged in user.

Add an owned address by clicking *Add* and providing a valid address and password.

Remove an owned address by selecting one or more addresses and clicking on *Delete*.

Quarantine Options

Core Settings White List Rights Owned Addresses Delegated Access

Owned Addresses

These are all of the e-mail addresses that the quarantine system considers to be a part of your identity when viewing messages. 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 any of these email addresses
- Add additional addresses, if you can authenticate with the email address. (If you cannot authenticate, your quarantine administrator may add them for you)

Delete Add

Address

Search Address

test1@doc.mf.net

Show 10 entries

Showing 1 to 1 of 1 entries First Previous 1 Next Last

Delegated Access

A user can grant another user the rights to access and manage their quarantine.

Add a delegate user by clicking *Add* and providing the email address. This grants the right to view the quarantine.

Remove a delegate by selecting one or more names and clicking on *Delete*.

Grant/revoke additional rights to the delegate user:

Delete: Allows/denies delegate to delete messages from quarantine.

Release: Allows/denies delegate to release messages from quarantine.

Forward: Allows/denies delegate to forward message from quarantine.

Blacklist: Allows/denies delegate to add addresses to the blacklist.

Whitelist: Allows/denies delegate to add addresses to the whilelist.

Quarantine Options

Core Settings White List Rights Owned Addresses Delegated Access

Delegated Access

These are all the users you have granted access to your quarantine and the permissions you have given them. You may:

- Revoke access to your quarantine by deleting the user
- Grant access to your quarantine by adding users to this list
- Alter the permissions for any of the users

Delete Add

Login Name	Delete	Release	Forward	Blacklist	Whitelist
<input type="checkbox"/> Search Login Name					
<input type="checkbox"/> test2@doc.mf.net	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Show 10 entries

Showing 1 to 1 of 1 entries First Previous 1 Next Last

