Legal Notices

© Copyright 2019 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.
## Contents

**Preface**  

**1 Release Notes**  
- New Features ......................................................... 11  
- Release Notes ......................................................... 11  
- Revision History ..................................................... 11  

**2 Overview**  
- Micro Focus Secure Messaging Gateway Overview .................. 33  
- Key Concepts ......................................................... 33  
- Micro Focus GWAVA Family of Message Handling Products ......... 34  

**3 Installation**  
- System Requirements .................................................. 35  
- Overview .............................................................. 35  
- System Requirements .................................................. 35  
- Ports Used by Secure Messaging Gateway ............................. 36  
- Inbound and general traffic ......................................... 36  
- Outbound traffic ....................................................... 36  
- VMware OVA Deployment ............................................. 36  
- OVA Deployment ....................................................... 36  
- Hyper-V Deployment ................................................... 41  
- Virtual Machine Post-deployment Tasks ............................. 49  
- ISO Installation ......................................................... 53  
- Post-Installation Configuration ..................................... 55  
- Post-Configuration Tasks ............................................ 63  
  - On the Secure Messaging Gateway server ......................... 63  
  - On the Email Server ............................................... 66  
- Installing Additional Servers into an Existing Network .......... 67  
  - Overview ............................................................ 67  
  - Setup ............................................................... 67  
- GWAVA 6 to Secure Messaging Gateway Migration .................. 71  
  - Pre-migration Tasks ............................................... 71  
  - Migration Tasks .................................................... 77  
- Manual Migration to SMG ............................................. 83  
- Setting up a Multi-Tenant System ................................... 84  
- Securing the SMG Web UI ............................................ 85  

**4 System Administration**  
- System Overview ...................................................... 87  
- Console Navigation Bar .............................................. 87  
- System Administration Console .................................... 88
## 5 Module Administration

- Module Management .................................................. 117
  - Module Status .................................................. 117
  - Starting and Stopping Modules ................................ 117
- Interfaces Overview .................................................. 117
- SMTP Interface ....................................................... 118
  - SMTP Module Troubleshooting ..................................... 123
- IMAP Interface ...................................................... 123
  - IMAP Interface Manager ........................................... 124
  - Reference .......................................................... 124
- 3rd Party Integration ................................................ 126
  - GroupWise 18 ....................................................... 127
- IMAP Scanning .......................................................... 131
- Address Transformation Manager .................................. 133
- Scan Engine Manager .................................................. 135
  - Load Balancing .................................................... 135
  - Fault Tolerance .................................................... 136
  - Organizational Units .............................................. 136
  - Message Filter engine .............................................. 136
- Mail Relay Module Manager .......................................... 136
- QMS Module Manager .................................................. 139
- Stats Module Manager .................................................. 140
- Message Tracker Module Manager ................................... 141

## 6 Policy Administration

- Organization / Policy Management Overview ...................... 143
- Settings ............................................................... 144
- Manage Users .......................................................... 145
Manage System roles .................................................................147
Roles ......................................................................................148
Manage Custom Roles ............................................................153
Create Custom Role ...............................................................154
Creating a Group .................................................................155
Group Management ...............................................................156
Manage Organizations ...........................................................156
Add New Organization ............................................................157
Domain Management .............................................................160
Add New ..................................................................................160
Policy Management ...............................................................166
Set the Policy Priority ............................................................167
Manual Policy Creation ..........................................................167
SMTP Policy Creation With the Wizard ..................................169
IMAP Policy Creation With the Wizard .....................................173
Policy Scan Configuration ......................................................181
Component Settings ..............................................................183
Filters .....................................................................................184
Anti-Spam ..............................................................................185
Anti-Virus ..............................................................................185
Attachment Name .................................................................186
Attachment size ....................................................................186
Black List ...............................................................................186
Clam Anti-Virus ....................................................................186
DKIM Verification ..................................................................187
Email Address .......................................................................187
Filter Group ..........................................................................187
Fingerprint ............................................................................188
IP Address .............................................................................188
IP Reputation .........................................................................188
Message Received ...............................................................189
Message Size .........................................................................189
Message Text ..........................................................................189
RBL .........................................................................................190
SMTP Envelope ....................................................................190
SPF .........................................................................................191
SURBL ....................................................................................191
Zero Hour Virus .....................................................................191
Services ..................................................................................191
Add Header Line .....................................................................192
Admin Quarantine .................................................................192
Block ......................................................................................192
Carbon Copy ..........................................................................193
DKIM Sign ............................................................................193
Event Writer ...........................................................................193
Ham Reporting .......................................................................193
Interface Control ....................................................................194
Message Signature ..................................................................194
Message Tag ...........................................................................194
Message Tracker ....................................................................195
Notify ......................................................................................195
Quarantine ..............................................................................196
Quarantine Control ...............................................................197
Spam Reporting ......................................................................197
## Contents

### Quarantine System

- **Statistics Recorder** .................................................. 198
- **Exceptions** .................................................................... 198
- **Email Address** ............................................................... 198
- **Exception Group** ............................................................ 198
- **IP Address** .................................................................... 199
- **Message Text** ............................................................... 199
- **SMTP Envelope** ............................................................. 199
- **White List** ..................................................................... 200

### 7 Policy Configuration Tips and Tricks

- Creating a Statistics and Tracking Policy .................................. 201
- Creating a Block and Quarantine with Exceptions Policy ............. 206
  - Creating a policy manually involves: ................................ 206
  - Create the Policy ............................................................... 206
- Creating an Anti-Virus Policy .................................................. 211
  - Create the Policy ............................................................... 212
  - Set the Policy Message Direction ..................................... 212
  - Configure the Scanner ....................................................... 212
- Enabling Black List and White List ........................................ 213
  - Configure Black list: ......................................................... 214
  - Configure White list: ........................................................ 216
- **Black List and White List QMS Configuration** ....................... 216
- Creating a DKIM Verification Policy ...................................... 217
  - Blocking Messages Without a Valid DKIM Signature ............... 217
  - Sending a Notification That a Message Has a Valid DKIM Signature ................................................................. 218
- Enabling DKIM Signing ......................................................... 218
  - Prerequisites .................................................................... 219
  - Setting up DKIM Signing ................................................... 219
- Creating HAM and SPAM Reporting Policy ............................... 220
  - Spam Reporting ............................................................... 221
  - Ham Reporting ................................................................. 221
- Adding Clam Anti-Virus ........................................................ 221
- Solving “No policies were located to scan this message” ................ 222
- Block Outbound Messages Not From Your Domain .................... 222

### 8 Quarantine System

- **Quarantine** ..................................................................... 225
- **Quarantine Options** ........................................................ 228
  - Core Settings .................................................................... 228
  - White List ..................................................................... 229
  - Rights ........................................................................... 229
  - Owned Addresses ............................................................. 230
  - Delegated Access ............................................................. 230
- **Quarantine Digest** ............................................................ 231
  - Settings Tab .................................................................... 232
  - Schedule Tab .................................................................... 233
  - Manual Release Tab ........................................................ 234
- **Quarantine Users** ............................................................ 236
  - User Rights ..................................................................... 237
  - User Options .................................................................... 237
  - Group Membership .......................................................... 238
Preface

About This Guide

This Micro Focus Secure Messaging Gateway (SMG) 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. The administrator is expected to be familiar with DNS, SSL, SMTP, RBL, SRBL, and GroupWise or Exchange authentication formats.

A user guide section is included. The user is expected to be able to click on links to access the quarantine and add email addresses to black and white lists.

Technical Support

If you have a technical support question, please consult the Micro Focus Technical Support at https://www.microfocus.com/support-and-services/ (https://www.microfocus.com/support-and-services/)

Sales

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

To contact a Micro Focus sales team member, please 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.

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

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

This document communicates the major new features and changes in this revision of Secure Messaging Gateway.

New Features and Release Notes for this update are listed below.

New Features

Enhancements are listed here. These enhancements are not limited to the previous revision of Secure Messaging Gateway and could affect other revisions.

- Nodes now have top/bottom buttons and double-clicking the button moves the node to the top or bottom of the node stack.
- Added the COMNOTEXT fingerprint type which complements the COM fingerprint.
- Many Security enhancements

Release Notes

Bug fixes are listed here.

Revision: 658 - created 25-Apr-2019
Added important infrastructure changes and security enhancements

Revision History

The revision history of Secure Messaging Gateway.

Revision: 658 - created 25-Apr-2019
Added important infrastructure changes and security enhancements

Revision: 648 - created 28-Mar-2019
GWAV-2620 - Fix recent virus patterns not being detected
GWAV-2748 - Fix SMTP proxy process not attempting direct host connection when MX records do not exist
GWAV-2548 - Fix issue with IMAP job status report record consuming all record numbers
Write contents of failed insertion query to qms log

Revision: 623 - created 28-Feb-2019
GWAV-2742 - Fix crash when DNS records larger than 10kb are queried
GWAV-2531 - Fix gwvrelay not encoding end of data character in some situations, causing messages to be truncated
GWAV-2651 - Change SMTP response to 4xx when data connection error occurs during or after DATA command
GWAV-2652  - Fix logged error not reporting correct message when 3rd party interface passes incorrect application key
GWAV-2575  - Remove 'authenticated relay' option from SMTP interface UI, which is not currently implemented
GWAV-2733  Fixed display of Internal ID in qms message properties page.
GWAV-2735  - Fix duplicate item drop on workbench leaving broken title on page

**Revision:** 598 - created 30-Jan-2019
GWAV-2543  - Fix invalid paths to md5 function for web UI causing automated signups to fail to set user passwords
GWAV-2527  - Fix log retention days setting not taking effect
GWAV-2549  - Add max line length byte count to exceeded line length response
GWAV-2500  - Fix manual digest release not working when email address has uppercase characters
GWAV-2550  - Fix placeholder text in forwarded messages
GWAV-2551  - Fix Message Received filter displaying incorrect state for external direction in node editor
GWAV-2504  - Persistent z-index property of workbench nodes
Fix memory leak in QMS when storing messages
Fix temp file manager thread synchronization crash
Fix ham reporting service node editor not loading correctly
More logging added to smtp server session process
GWAV-2301  - Fix signature service conflicting with DKIM service
Update the 3rd party license document
GWAV-2556  - Replace DNS resolver code
GWAV-2532  - Additional fixes to module status page regressions
GWAV-2532  - Remove error messages from code
Update a gwava.com link to microfocus.com

**Revision:** 584 - created 12-Dec-2018
GWAV-2532  - Additional fixes to module status page regressions
GWAV-2532  - Remove error messages from code
Update a gwava.com link to microfocus.com

**Revision:** 574 - created 29-Nov-2018
GWAV-2293  - Fix text filters not locating text with filters that start or end with non-word characters
GWAV-2435  - Fix HTML meta-data not being scanned with text filters
GWAV-2434  - Fix login failing with SMTP lookup for provisioned users
GWAV-2503  - Fix some event node properties resetting when changes are made to the node
GWAV-2502  - Fix regression from CSRF update causing template upload to fail
GWAV-1324  - Fix issue removing new node links on workbench immediately after saving changes
GWAV-2507  - Regression fixed when using IE11 to install licenses
GWAV-2506  - Fix regression preventing migration tool from being run
GWAV-2508  - Fix gwvsmtp crash when connected outbound mail servers drop connection after the MAIL command
GWAV-2509  - Address translation not working for outbound mail
GWAV-2297  - SMTP host test window fixed to fit page when multiple interfaces are included in test
GWAV-2285 - Fix display of long policy and OU names in navigation panel of admin UI
GWAV-2499 - Add COM fingerprint that skips text/plain message parts
GWAV-2430 - Remove SIZE parameter from MAIL command when remote host does not declare it in response to EHLO
GWAV-2415 - Add error handling for QMS slave upload files
GWAV-2328 - Fix module status page to display times in timezone of users browser
GWAV-2515 - Fix buffer overflow crash when handling very long path names
GWAV-2516 - Add support for diagnostic scan of multiple files
GWAV-2532 - This change to module_status.php disables the start, stop and restart ALL buttons and removes the start and stop for gwavaman

Revision: 550 - created 25-Oct-2018
GWAV-2423 - Fix code lockup with specific type of broken zip files
GWAV-2420 - Fix regression in DKIM key upload dialog
GWAV-2277 - Fix 3rd party interfaces masquerading and loading as SMTP interfaces
GWAV-2435 - Fix text in HTML tags not being included in text filter scan
GWAV-2438 - Fix module status page error when redirected to from online update page
GWAV-2437 - Fix SMTP interface screen not expanding SMTP interfaces when address transformation rules exist
Sync LDAP lookup method in QMS from GWAVAMAN libraries

Revision: 537 - created 27-Sep-2018
GWAV-2352 - Fixed problem with adding new server to existing SMG network
GWAV-2353 - Fix regressions in UI with SMTP interface address transformation details
Add SMTP client IP address to log when client connects
GWAV-2357 - Fix TLS downgrade reconnections failing to close previous connection
GWAV-2356 - Add timeout override for failed TLS connections that don't drop the connection
Fix regression in QMS UI, not saving digest recipient target
Fix regression in QMS UI, not saving group settings
GWAV-2347 - Fixed and HTML issue that prevented row from successfully loading/being displayed.
GWAV-2405 - Fix policy save not working sometimes
Fix rights lookup when saving system roles as an OU admin causing unresponsive script and subsequent UI failure
3rd party licenses file
GWAV-2306 - CSRF prevention implemented
GWAV-2414 - The recipient address in this case was not being escaped properly.

Revision: 518 - created 30-Aug-2018
GWAV-2272 - Additional security updates
GWAV-2320 - Owner's are allowed to release messages to their inbox even if they have never logged into QMS.
GWAV-2332 - Attempt to create the "cache" directory in the qms root path each time qms starts.
GWAV-2315 - Fixed typo strlower replaced with strtolower
GWAV-2330 - Fix regression in scan editor
GWAV-2334 - Fix hover text on status icons
GWAV-2308 - More changes need to handle the ClamAv update
GWAV-2338 - Fix licenses not installing correctly
GWAV-2337 - Add SMTP greeting override for mail relay module
GWAV-2336 - Implement PFS
Removed problematic pg_escape_string, the template contents were getting double escaped.
GWAV-2340 - Disable SSL v2 v3 and TLS v1 protocols by default and expose options for these in the UI for gwvsmt
GWAV-2346 - Issue with link to quarantine fixed.
Revision: 498 - created 26-Jul-2018
GWAV-2242 - Digest Actions (blacklist, whitelist, release, delete) weren't working from the digest.
Revision: 488 - created 26-Jul-2018
GWAV-2242 - Digest Actions (blacklist, whitelist, release, delete) weren't working from the digest.
GWAV-2289 - QMS release by admin was failing.
GWAV-2272 - Additional security updates
GWAV-2261 - Fixed an issue with the previous change that was causing a crash
GWAV-2311 - Modify a text label for consistency
Revision: 471 - created 28-Jun-2018
GWAV-2241 - Module startup process now wait for 60 seconds to obtain an application lock before giving up
GWAV-2241 - Set heartbeat process to start after application restart detection is complete
GWAV-2239 - Fix DB schema 114 update failing if IA nodes have been configured
GWAV-2220 - Fix menu initialization taking a long time to complete
GWAV-2249 - Solve login case sensitivity issue preventing access to QMS data after successful authentication
GWAV-2246 - Resolve browser autofill causing addition of records in domain UI page
GWAV-2247 - Resolve browser autofill causing addition of records in relay module UI page
GWAV-2200 - Ideas Portal
GWAV-867 - Add Secondary AV Scanner - CLAMAV
GWAV-2226 - Report connection drop reason in SMTP responses
GWAV-2240 - Correct URL in digest footer
GWAV-2265 - Intercept browser auto-fill causing issues with scan engine page fields
Revision: 444 - created 31-May-2018
GWAV-2210 - Add test button to domain hosts
Add QMS helper script to QMS php lib
GWAV-2219 - Image analyzer filter removed from UI
GWAV-1817 - ZIPDEEP and ZIP WIDE fingerprint fixes
GWAV-1773 - Add exception information to report deep recursion detected by fingerprinting
GWAV-1405 - Apply default RBL servers to policies if none have been defined
GWAV-1722 - Respond with 5xx error when LDAP lookup is configured for recipient lookup, and recipient lookup is unsuccessful
GWAV-2066 - Fix possible script injection vulnerability in node editor
GWAV-2199 - Date sort in message tracker and qms as well as fix for GWAV-2217 blank white list and/or black list.
GWAV-2196 - Add SSL error detail to logs when STARTTLS failure occurs
GWAV-2216 - Fully implement ‘auto’ option for connection security when looking up users at login
GWAV-2217 - Fixed php error when there was no whitelist or blacklist while saving the options
GWAV-1877 - Pass destination SMTP response codes back to source SMTP server when only one destination server is involved in the transaction

**Revision:** 433 - created 26-Apr-2018
GWAV-2213 - Update to CTIPD 4.01.003.4
GWAV-2214 - Update to latest ctengine 8.02.0000.4
GWAV-2215 - Update to AV Engine Version 83886080; 5.0.0
GWAV-2215 - Update to AV SDK Version 100663296; 6.0.0
GWAV-2212 - Fix multiple IMAP interface types being created in database causing issues using IMAP interface

**Revision:** 417 - created 29-Mar-2018
GWAV-2196 - Fix failed STARTTLS negotiation resetting SMTP transaction to connected state
GWAV-2091 - Address Transformation
GWAV-2019 - mcrypt replacement
GWAV-1515 - IMAP scanner
GWAV-2000 - Licensing

**Revision:** 397 - created 22-Feb-2018
GWAV-2193 - Fixed issues related to custom digest URI

**Revision:** 387 - created 07-Feb-2018
GWAV-2185 - Fix failover scan engine always being connected to a second server
GWAV-2189 - Added spaces to action/links in message table.
GWAV-1986 - Fixed a problem where characters in the message subject were not properly encoded

**Revision:** 376 - created 25-Jan-2018
Restore the release from digest option
GWAV-2144 - Umlauts and other special characters that were incorrectly displayed in QMS and Message Tracker list should now display correctly
GWAV-2166 - Add GroupWise 18 interface types (imap,gms,wasp,mta) to manage policy page
GWAV-1434 - Add spam/ham reporting feature
Add per-OU language selection
GWAV-2066 - Rename to Secure Messaging Gateway
Fix GWAVA connection list gathering process recursively filling the connection queue
Update image for digest delete,release,blacklist,whitelist pages to reflect name change to Secure Messaging Gateway
GWAV-2167 - Fixed problem with digest template where message table was not populated in the html view
GWAV-2173 - Fix GWVRelay not retrying delayed recipients.
Fixed problem with links in text version of the digest.
Fixed problem with owner id in text view of digest
GWAV-2170 - Fix position of version information in titlebar

**Revision:** 358 - created 11-Jan-2018
GWAV-2157 - Reset address count for dictionary attack test when SMTP transaction resets
GWAV-2151 - Received header FROM needs to be the host name, not the senders domain
GWAV-2147 - Added code to handle the case where a forward as attachment template is not found
GWAV-2139 - QMS Admin rights overhaul
GWAV-2137 - Fix DKIM option to treat message verified when signature not present not working
GWAV-2130 - Remove redundant QMS rights
GWAV-2128 - GW 18 MTA cannot handle the formatted xml response
GWAV-2124 - Add missing script for system alerts
GWAV-2108 - Whitelists not reloading when items added from qms
GWAV-2077 - Tracker not showing connection info
GWAV-2076 - Message Tracker does not show any items when using IE
GWAV-2050 - Ability to Add to Global Whitelist/Blacklist from QMS as admin
GWAV-1974 - Whitelist, blacklist, delete directly from digest
GWAV-1954 - Fix white/black list entries not being stored in selected OU when logged in as admin
GWAV-1919 - Prevent database updates when versions are not contiguous
GWAV-1896 - Incorrect time zone shown in Message tracker
GWAV-1865 - REST API for access to Scan Engine
GWAV-1806 - Iterate through all configured scan engines when either connection or engine failure occurs
GWAV-1769 - Ability to manually add to QMS blacklist
GWAV-1768 - Ability to manually add to QMS whitelist
GWAV-1025 - Detecting Password protected ZIP as Nonextracting ZIP

Revision: 345 - created 30-Nov-2017
GWAV2092 - Child node activation problem
GWAV-2102 - Detect JAR files more precisely
GWAV-2104 - Add LDAP_OPT_REFERRALS option to LDAP options during LDAP user verification
GroupWise 18 Mobility Scanner
GroupWise 18 WebAccess Scanner
GroupWise 18 MTA Scanner
3rd Party Application Scanner
GWAV-2109 - Fix added port number causing scan engine bind address to revert to default
GWAV-2107 - Fix issue where workbench will not start when events have looped items with no parent
GWAV-2111 - Modify TCP connection code to attempt all IP addresses associated with A records
GWAV-1850 - Notification updates

Revision: 324 - created 26-Oct-2017
GWAV-1446 - Application lock fix
GWAV-1894 - Fixed problem with display of Owned and Delegated access tabs for admin and normal user access
GWAV-2073 - RCPT 550 response fix
GWAV-1268 - Extended office file support
GWAV-2034 - Fixed ZIPPW and ZIPDEEP tests not being run

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 today's 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 cengine version 8.00.0125.1
GWAV-1737 - Update to latest ctipd 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
Documention 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-1422 - 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 Ouid 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 ctipd.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 ctipd 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 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
Micro Focus Secure Messaging Gateway (SMG) 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. SMG also monitors network traffic to prevent pornographic images, and protects against cybercrime and DoS/DDoS attacks.

SMG protects business networks and communication data for thousands of organizations around the world in industries including government, education, financial services, healthcare, and business.

SMG 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.

SMG provides multi-layer spam defense to protect email and keep unwanted traffic away from your collaboration system.

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

Key Concepts

Once SMG is installed it will need to be configured:

1. SMG will need to be connected to your domain “Domain Management” on page 160.
2. The interfaces to be scanned will need to be configured “Interfaces Overview” on page 117.
3. Scanning policies will need to be created so messages will be scanned “Organization / Policy Management Overview” on page 143.

4. The quarantine digest will need to be configured so users are alerted when items are not allowed to reach them “Quarantine Digest” on page 231.

For normal use of SMG, the sysadmin should be familiar with:

- Using the Quarantine System “Quarantine” on page 225.

Micro Focus GWAVA Family of Message Handling Products

Micro Focus has a family of products that are related to message handling:

- 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.
- 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.
3 Installation

Secure Messaging Gateway (SMG) is installed as a virtual machine (VM) and can be installed in three ways:
- VMWare "VMware OVA Deployment" on page 36
- Hyper-V "Hyper-V Deployment" on page 41
- Your own VM from the ISO "ISO Installation" on page 53

Once installed the server will need to be configured "Post-Configuration Tasks" on page 63.

To add an additional SMG server to an existing system, go to "Installing Additional Servers into an Existing Network" on page 67

If you have an existing GWAVA system and wish to migrate the settings to a new SMG system, go to "GWAVA 6 to Secure Messaging Gateway Migration" on page 71

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, VMware, 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))

VMware OVA Deployment

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.

**Hyper-V Deployment**

Secure Messaging Gateway can be deployed in a Hyper-V environment.

1. Download the Hyper-V machine ZIP file.
2. Extract the contents of the ZIP file to a folder.
3. Import the Virtual Machine.
4. Begin the import process.
5. Select the folder of the extracted files. There should be 3 directories in this folder.

6. Select the Virtual Machine to Import.
7. Select the type. Recommended to Copy the virtual machine.
8. Select the Destination for the Virtual Machine.
9. Select the location to store the Disks.
10. Verify the Import.
11. Associate machine to correct Network Adapter.
12. Power on the machine.

From this point, it is the normal install procedure.

**Virtual Machine Post-deployment Tasks**

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:

   ```bash
   sudo /opt/gwavapreinstall.sh
   ```
Ubuntu 16.04 LTS guava tty1

guava login: guava
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/gwava/preinstall.sh
#############################################

guava@guava:~$ sudo /opt/gwava/preinstall.sh

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

BE ABOUT TO DOWNLOAD.

BEFORE CLICKING THE "ACCEPT" BUTTON OR USING THE SOFTWARE, PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY. BY CLICKING ACCEPT, YOU WILL BE DEEMED, FOR ALL LEGAL PURPOSES, TO HAVE READ, UNDERSTOOD 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 CONTRACT, BETWEEN YOURSELF AND MICRO FOCUS THAT SHALL, FOR ALL LEGAL PURPOSES, BE GOVERNED BY THE TERMS 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 RELATIONSHIP 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 out:

"Agreement" when used herein shall mean the EULA entered into between yourself and MICRO FOCUS governing 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 media 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 functionality 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? 1
SET_INTERFACE = ens160
```

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 interface 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 gwava7): 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.
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.

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. Continue with Post-Installation Configuration Tasks “Post-Installation Configuration” on page 55.

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” on page 35 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-Configuration Tasks” on page 63.

Post-Installation 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 Messaging Gateway Migration” on page 71.

If adding to an existing Secure Messaging Gateway network, see how to connect with an existing network “Installing Additional Servers into an Existing Network” on page 67.
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.
Postgres Database Configuration

If using an external database, they can be configured here:

- Config

```sql
DB server address: 127.0.0.1
DB name: SecureGateway
DB user name: postgres
DB password: **********
```
Postgres Database Configuration

- **Quarantine**

Postgres Database Configuration

- **Statistics**
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.

7. Continue with Post-configuration tasks.
Post-Configuration 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. Press “Add new” and name it after the fully qualified domain name of your email server.
   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
      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
2. Create a Policy:

Create at least one policy “Policy Management” on page 166 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.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable global digest services</td>
<td>☑</td>
</tr>
<tr>
<td>Contact email address</td>
<td></td>
</tr>
<tr>
<td>Digest Template</td>
<td>Digest (en)</td>
</tr>
<tr>
<td>Preferred digest language</td>
<td>English (en)</td>
</tr>
<tr>
<td>Maximum digest rows</td>
<td>50</td>
</tr>
<tr>
<td>Release button address</td>
<td></td>
</tr>
<tr>
<td>Digest recipients</td>
<td>Send digest to all users</td>
</tr>
<tr>
<td>Custom address list</td>
<td></td>
</tr>
</tbody>
</table>

Remove selected: ☒
Add new:
c. Under the Schedule sub tab select a day or time for the digests to be sent to users when the user has one or more quarantined messages. Quarantined messages will be removed after 30 days by default. 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.

<table>
<thead>
<tr>
<th>Quarantine</th>
<th>Options</th>
<th>Digest</th>
<th>Users</th>
<th>Groups</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td><strong>Schedule</strong></td>
<td><strong>Manual Release</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midnight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7:00am</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00am</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>9:00am</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>10:00am</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>11:00am</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Midday</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>2:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>3:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>4:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>5:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>6:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>7:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>8:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>9:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>10:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>11:00pm</td>
<td>✔️</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Additional setup may be required depending on the interface(s) installed. For example, an SMTP banner is recommended.

**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.
Installing Additional Servers into an Existing Network

If the Secure Messaging Gateway server is being deployed into an existing GWAVA or 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 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.
Installation

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 the server. See Post-install Tasks.

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

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

If the Secure Messaging Gateway server is being deployed into an existing GWAVA 6 network, Secure Messaging Gateway can be added to an existing GWAVA 6 network and the settings migrated from the primary GWAVA 6 server. There are a few settings which need to be configured, these will only apply to the primary GWAVA 6 server.

The GWAVA 6 Network shares the databases to keep the configuration, quarantine, and statistics up to date and common across the whole system. A GWAVA 6 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 6 appliances at multiple locations are required.

Determine type of database in use:

1. Open the GWAVA Management Web page.
2. Go to Server / Interface Management | <servername> | Server management | Server status.
3. Under Server Details | DB engine, it will tell you if you are using sqlite or postgres.
For SQLite, skip to the Migration.

For Postgres, setup the primary GWAVA 6 server to allow the migration. 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 6 servers.

In order for the databases to be accessible to the Secure Messaging Gateway server, 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.

2. If connecting to a GWAVA 6 server. A configuration file must be modified as root user on the GWAVA 6 server. 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. It should be of the form:

host all all <Secure Messaging Gateway IP Address>/<Subnet mask> password

For example, adding a remote connection:

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

3. If connecting to a GWAVA 6 network, determine and set allowed connection addresses.

Modifying the pg_hba.conf file correctly requires that the IP addresses of the remaining GWAVA 6 servers, if part of a GWAVA 6 network. 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.
Open port 5432 in the firewall.

4. 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

5. 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.

6. 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
-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
-rw-r--r-- 1 root gwava 407 May 26 10:48 install.lock
-rw-r--r-- 1 root gwava 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
## Configure new Secure Gateway server

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>gnuva153</td>
</tr>
<tr>
<td>Connection address</td>
<td>151.155.183.153</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>******</td>
</tr>
<tr>
<td>Re-type password</td>
<td>******</td>
</tr>
<tr>
<td>Primary domain</td>
<td>doc.mf.net</td>
</tr>
<tr>
<td>Contact email</td>
<td><a href="mailto:aiden@doc.mf.net">aiden@doc.mf.net</a></td>
</tr>
<tr>
<td>Mail relay server</td>
<td>151.155.183.147</td>
</tr>
<tr>
<td>Mail relay username</td>
<td></td>
</tr>
<tr>
<td>Mail relay password</td>
<td></td>
</tr>
<tr>
<td>Setup default system</td>
<td>✓</td>
</tr>
</tbody>
</table>

## Postgres Database Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB server address</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>DB name</td>
<td>SecureGateway</td>
</tr>
<tr>
<td>DB user name</td>
<td>postgres</td>
</tr>
<tr>
<td>DB password</td>
<td>******</td>
</tr>
</tbody>
</table>
h. Validate the server installation

**Migration Tasks**

**GWAVA 6 Migration Tool**


Select *System Management | GWAVA 6 Migration*

The migration tool is locked for security reasons. To unlock the tool, log into the SMG terminal and run the command: `/opt/gwava/assets/bin/linux/scripts/migration_enable`

There are 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 toll can be run as often as desired, so piecemeal migrations are acceptable.

For internal (sqlite) databases, you will need to upload the databases onto the Secure Gateway server so it can access the file directly. Uploading is easily done with the options provided in this toolkit. The files that are required can be located at the following locations on your GWAVA 6 server. On linux, [gwavaroot] will be /opt/beginfinite/gwava and on Windows it will be \Program Files\GWAVA\GWAVA.

- GWAVAMAN database file: [gwavaroot]/config/gwavaman.db
- QMS User database file: [gwavaroot]/services/qms/data/qms_user.db
- QMS Digest database file: [gwavaroot]/services/qms/data/qms_digest.db
- QMS User Exceptions Database file: [gwavaroot]/services/qms/data/user_exception.db. The user exceptions database is only stored in an SQLite database file and must be uploaded.

For postgres, provide the required information for the database connection.

If you are using the GWAVA 6 Appliance where postgres is the default use the following default values:

- Database name: GWAVA
- Database login name: gwava
- Database login password: gwava
Otherwise, provide the connection information to the database used by the GWAVA 6 server.

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

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.
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?

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

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

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 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 “SMTP Policy Creation With the Wizard” on page 169 or a Block and Quarantine with Exceptions policy “Creating a Block and Quarantine with Exceptions Policy” on page 206.

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.

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 Overview” on page 117
2. Scan engine. “Scan Engine Manager” on page 135
3. QMS. “QMS Module Manager” on page 139
5. Statistics. “Stats Module Manager” on page 140
6. Mail Relay module. “Mail Relay Module Manager” on page 136
7. Default OU to contain the tenant units. “Manage Organizations” on page 156
8. Default Policy within the default OU, new tenants will use this policy. “Policy Management” on page 166
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 101
10. Confirm each module can service the default OU.

**Securing the SMG Web UI**

To secure the Secure Messaging Gateway Web interface SSL must be enabled directly in apache. See the apache documentation (https://httpd.apache.org/docs/2.4/ssl/).

1. Go to /etc/apache2/sites-enabled/.
2. Create a new file (Name the config file something useful, like: smg.domain.com.conf) by typing: vi newfilename.conf.
3. Hit the Insert key to start editing it.
4. Copy this in the new file and make the necessary changes:

```xml
<VirtualHost *:443>
  ServerAdmin notify@domain.com
  ServerName server.domain.com
  DocumentRoot /opt/gwava/gwavaman/http

  SSLEngine on

  SSLProtocol ALL -SSLv2 -SSLv3
  SSLHonorCipherOrder On
  SSLCipherSuite
  ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AES
  GCM:RSA+AES:!aNULL:!MD5:!DSS:!3DES
  SSLCompression Off

  Header always set Strict-Transport-Security "max-age=63072000;
  includeSubdomains;"

  SSLCertificateFile /crt file
  SSLCertificateKeyFile /key file
  SSLCertificateChainFile /Intermediate file

  SSLUseStapling on
</VirtualHost>
```
ErrorLog ${APACHE_LOG_DIR}/error-ssl.log
CustomLog ${APACHE_LOG_DIR}/access-ssl.log combined

</VirtualHost>

5. Put the cert, key, and intermediate file on the server (an Intermediate file is not required but recommended).

6. Edit the path for each file above including the filename (case sensitive). If not using an Intermediate file you can comment this line out by putting a # in front of it.

7. Save by pressing the Escape key and then typing: :wq.

8. Run the command: a2enmod ssl.

9. Run the command: a2enmod headers.

10. Restart apache by typing: service apache2 restart

11. Test it by running this command: apachectl configtest

12. If you get a “Syntax ok” then you can restart apache again to beginning using SSL.

Once enabled the server can be configured under "Manage Servers" “Enabling SSL on Secure Messaging Gateway” on page 91 to be accessed via https://<smghost_address>
System Administration

System administration is made up of System Management, Module Management Chapter 5, “Module Administration,” on page 117, and Policy Management Chapter 6, “Policy Administration,” on page 143.

System Overview

Enter the IP address or Hostname of your Secure Messaging Gateway server.

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

Console Navigation Bar

The navigation bar at the top of the console show the product logo and name, and the product revision currently installed on the left.
On the right it shows who you are logged in as, the last login of this user, a link to the ideas portal, a link to the support website, and the logout button.

The Ideas portal (https://ideas.microfocus.com/MFI/mf-smg) is where you can enter suggestions and enhancement requests that will be reviewed for possible inclusion into SMG.

The “On-line help and knowledgebase” button links to the on-line support page (https://www.microfocus.com/support-and-services/). Enter “Secure Messaging Gateway” or “GWAVA” to receive links to the documentation, downloads, knowledge base, license keys and support forums.

The logout button logs you out of the console and returns you to the login page.

System Administration Console

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

The System Management section of System Administration allows you to license, update and otherwise control the SMG server(s) and interface.

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

Each server in your Micro Focus Secure Messaging Gateway network requires some information specific to its instance.

The server SSL settings provide default values for modules running on the local server.

These defaults can be overridden per-module, where SSL functionality is available in the individual module setting pages.

#### Prerequisites

Obtain from your registrar
- SSL certificate file
- SSL certificate chain file
- SSL key file
- SSL pass phrase

#### Procedure

- Log into the Secure Gateway server via TTY and upload the SSL 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.
**NOTE:** Warning: You **MUST** be logged in with the https URL or you will no longer be able to connect to the Secure Gateway server.

Reference

*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

OpenDKIM key folder: The folder the key is kept in. Default: /etc/opendkim/keys/

OpenDKIM key table: The key table file. Default: /etc/opendkim/key.table

OpenDKIM signing table: The signing table file. Default: /etc/opendkim/signing.table

OpenDKIM user:group: The user and group with DKIM rights. Default: opendkim:opendkim

System logs: Click the button to download the logs. Download the logs individually. Also found on the server in /opt/gwava/services/logs/
Web UI SSL redirect: The web UI can be redirected to a secure address. This is configured in apache, see "Securing the SMG Web UI". WARNING: Access to the system administration console may be lost if this option is not configured correctly.

Web SSL UI exceptions: IP address or range exceptions to the SSL UI redirect.

system.xml: Server information for recovering a Secure Messaging Gateway server.

```
<system.xml>
  <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>
</system.xml>
```
Recovering a Secure Messaging Gateway Server

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 to complete the recover server process.

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

Languages

Select the languages that the system will make available in the interface. The radio button will set the default language for the system. Enable other languages with the checkbox for each language.

A custom Organizational Unit (OU) may have a different default language as long as it is enabled here. Set the custom OU language under Organization/Policy Management | <Custom OU> | Settings | Default Language.

The child OU will use the parent OU language be default.

Templates for system emails are provided only for English. You can download the existing templates, translate the templates into other languages and upload them to the system under System Management | Templates.
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.
Service Dropdown menu

Select the service that will trigger the digest

- Delivery status notification
- Notify service
- Quarantine digest
- Quarantine forward
- Spam report
- System messages
- Ham Report Signature
- Spam Report Signature

Template variable keys

Available keys for personalizing digest messages are:

- SenderName
- Subject
- MessageText
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.

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.

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)

Accessibility and captcha:
Accessible CAPTCHA (https://www.section508.gov/blog/CAPTCHA)
The accessibility of Google’s 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.
Deploying a Database

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 Messing 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 Messing 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
Generic interface

Message Tracker
Message Tracker

Allow file path list:
/tracker/
/ui/tracker/

Deny file path list:

Role Assignment

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

Policy admin

Policy admin

Policy user
QMS interface

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.

Processing server: Which server will process the request

Encrypting an SMG 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 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.
1. Select the scan engine to process the message: from the drop down menu.
2. Provide the message to be scanned: by browsing to and uploading the file.
3. Paste MIME message: paste the MIME.822 in the text box.
4. 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

5. 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 License 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.

When your license is within 30 days of expiration reminder messages will be sent to the system administrator specified under System Administration | Organization/Policy Management | Settings | Administrator email address.

You will receive a Validation Key from Micro Focus Licensing.

1. Go to the Licensing portal (https://licenses.gwava.com/).
2. Select the product you are licensed for, for example “Secure Messaging Gateway (SMTP)”, enter the validations key, and select Next. Each interface type has its own license. Multiple may be active at a time.

3. Enter your information, and select Next.

4. Download the PEM file.

5. Browse to your SMG server and go to the Licensing section.

6. Click on Add License.
8. Press Install to upload the PEM file.

### Online Updates

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

You may select an update stream of Release (recommended) or Beta (should only be used under Support’s supervision). If you are on the beta stream, you can switch to the release stream when the release build is higher than the beta build. This is recommended to be done during the monthly release update on the last Thursday of the month.

To update the server click *Start Update*.

Once the update is complete the modules must be restarted “Starting and Stopping Modules” on page 117 manually.

Update History will show when the updates were installed on the server.
View Updates will show the versions installed on the server.
Revision: 200 - created 27-Apr-2017
Fx custom user digest setting not displaying correctly when set to EXCLUDED
Fx qms prune data/info options not displaying the correct state when items are disabled
Fx custom roles not able to be removed
Merge GWAV-1830 - Overwrite EHLO/HELO host
Fx 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 - Fx invalid path error in browser console when loading admin UI
GWAV-1499 - Upload large files through PHP

Revision: 189 - created 30-Mar-2017
Fx issue with HTTP upload process mapping source data type to incorrect method
Fx HTML signature populating TEXT signature in UI when reloading node
Add option to disable multi-threaded filters within an engine module
GWAV-1669 - Custom Roles
GWAV-1815 - Add move object button to domains management page
GWAV-1771 - Policies created with wizard can now be deleted/moved/renamed immediately after creation
Implement cipher list support for SMTP module SSL
GWAV-1502 - Allow 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 MINE 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-1776 - Fire warning event when the wizard was offered with a number if it's explicitly none would appear to
Module Administration

Module management is where the modules are configured and controlled.

Module Management

Module Status

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

* 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.

Starting and Stopping Modules

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 Overview

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

The SMTP interface defines the connection to an SMTP server.

3rd Party Integration defines the connection to other software.
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**: 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/gwsmtmp/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.
**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**

If the module's SSL settings are left blank the local server SSL configuration settings will be used, if configured. Enabling the SSL settings in the module will override the server SSL configuration. This allows specific localized SSL settings for the individual module.

**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 a list of ciphers to use.

For example, to enter a list of strong ciphers to use, in the SSL Cipher List field, paste:

```
EECDH+ECDSA+AESGCM
EECDH+aRSA+AESGCM
EECDH+ECDSA+SHA384
EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384
EECDH+aRSA+SHA256
EECDH+aRSA+RC4
EECDH
EDH+aRSA
RC4
aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4
```

These may need to be modified if a sender you want to receive from is not secure, but it is recommended to have the sender upgrade their system to something secure, rather than reducing the security of your system.

Ciphers can be tested at the SSL-Tools website [https://ssl-tools.net/mailservers](https://ssl-tools.net/mailservers).

**SSL protocol disable**: You may select which security protocol(s) are used by SMG. Check the box to disable a protocol. Default SSLv2 disabled (checked), SSLv3 disabled (checked), TLSv1 disabled (checked), TLSv1.1 enabled (unchecked), TLSv1.2 enabled (unchecked).

**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.

TLS fail recovery timeout (sec): Default 2 seconds

Enable outbound timeouts: Default enabled.

Server connection timeout (sec): Default 60 seconds.

Server protocol timeout (sec): Default 60 seconds.

SMTP banner: Enter a banner for the SMTP, this is required by some email systems to approval connections. The best practice is to enter the external fully qualified domain name of the server so when confirming the connection you know where it is. For example, mail.example.com

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 4000000.

NOOP interval (sec): Enter how long a “no operation” should last. Default 30 seconds.

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.

Address Transformation

Create address transformation rules from the Module Management | Address Transformation Manager page “Address Transformation Manager” on page 133.

Available transformation rules: A list of available transformation rules to the interface. Select from the drop-down menu.

You can remove or override the direction and address selections here.

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.

SMTP Module Troubleshooting

There are some troubleshooting actions you can take to resolve issues.

Outgoing “Pending” Messages

With GroupWise systems, users may experience “pending” status for messages sent to the Internet. If email was working before enabling SMG and the GWIA log shows:

"Attempting to connect to <SMG hostname>"

"Send Failure: 420 TCP read error"

A simple test is to telnet to the SMG and attempt sending an email from the telnet session. If there SMZG responds with 220 and no banner.

The issue would be that the GWIA requires an SMTP banner from SMG.

Configure the SMTP interface | Protocol and add an SMTP banner, for example, “GroupWise SMG server”.

IMAP Interface

IMAP can be scanned by SMG.
SMG can scan IMAP interfaces, either generic or GroupWise.

Reference

Host server: Select a Host Name.
Stats module: Select a Stats module, if desired.
Scan policy: Select policies.
Notes: Leave notes to your future self.
Enabled: Default enabled (checked).
Status: Status of the IMAP Interface.
IMAP server address: Provide the address of the IMAP server.
Use SSL: SSL can be enabled here, default disabled (unchecked).
IMAP service type: Choose between Generic IMAP user or GroupWise Post Office.

Generic IMAP user:
Mailbox name: User name of the generic IMAP user.
Mailbox password: Password of the generic IMAP user.

**GroupWise Post Office:**

Trusted application key: Paste the Trusted Application Key here.
Trusted application name: Enter the Trusted Application Name here, this is case sensitive.
Scan users: Default enabled (checked).
Scan resources: Default enabled (checked).
Scan trash: Default enabled (checked).
Expunge purged items: Default enabled (checked).

Scan frequency: Select between: On demand, Run once, Week days, or Monthly.
Date to run scan: Set when the scan should run, this option changes depending on the frequency chosen.
Run now: Becomes available when the scan frequency is configured.
Minimum message size: Enter a minimum message size, if desired.
Maximum message size: Enter a maximum message size, if desired.
Scan date range: Select between: Scan all messages, Number of days prior to scan start, Custom date range, or Messages since previous scan. Additional range fields will appear depending on the range selected.

**IMPORTANT:** The Scan date range can only grab up to the number specified for the imapreadlimit in GroupWise. For information on changing this setting, see `--imapreadlimit` in the *GroupWise 18 Administration Guide*.

Expunge purged items: Default enabled (checked).
Folder scope: Select between: Scan all folders, Limit to defined folder list, or Limit to all except defined folder list. Additional folder list field will appear depending on the option chosen.

**3rd Party Integration**

Secure Messaging Gateway can integrate with other software. These interfaces will show up under Limit Interface in Policy Management. Each interface is independent of the others, therefore a single message may appear multiple times in Message Tracker as the message encounters each interface.
On the Secure Messaging Gateway Server:

1. Go to Module Management | Interfaces | 3rd Party Application Manager.
2. Select Add New.
3. Select the Host Secure Messaging Gateway server, this will add the Server Address.
4. Select the Services OU set, this will create the Application key.
5. Press Save.
6. Refresh the screen and open the new 3rd Party Application to get the Application Key.

If you are operating a Secure Messaging Gateway cluster of multiple scan engines. You may set the Scanner Fault tolerance. If they are set to the same priority, then this will automatically send messages to be scanned to the servers in the cluster in Round Robin-style fault tolerance.

**GroupWise 18**

Secure Messaging Gateway can integrate with GroupWise.
GMS Scanning:

On the GroupWise Mobility Server:

1. Open the mobility configuration file at:

```
/etc/datasync/configengine/engines/default/pipelines/pipeline1/connectors/mobility/connector.xml
```

2. Add the following elements to the configuration file under the `<connector><settings><custom>` section.

```xml
<securegatewayEnable/>
<securegatewayHost/>
<securegatewayPort/>
<securegatewaySecure/>
<securegatewayAppkey/>
```

The values are as follows:

```xml
<securegatewayEnable/>
<securegatewayHost/>
```

1 - enabled. If enabled, all the other elements must be correct.

0 - disabled.
This is the DNS or IP address of the Secure Messaging Gateway.

<securegatewayPort/></securegatewayPort>

This is the port number for Secure Messaging Gateway.
80 for HTTP
443 for HTTPS

<securegatewaySecure/></securegatewaySecure>

1 - secure (HTTPS)
0 - non-secure (HTTP)

<securegatewayAppkey/></securegatewayAppkey>

This is the application key defined in the Secure Messaging Gateway WebAdmin under:
Module Management | Interfaces | REST Interface Manager | GMS | Application Key. Copy this key to the xml element.
For example, if you want to have Secure Messaging Gateway GMS scanning enabled, and it is on the smg.company.com host, using port 443, connecting via HTTPS with an Application Key of 365c2949-0fb3-4d81-9dd2-421727bf08e3:

<securegatewayEnable>1</securegatewayEnable>
<securegatewayHost>smg.company.com</securegatewayHost>
<securegatewayPort>443</securegatewayPort>
<securegatewaySecure>1</securegatewaySecure>
<securegatewayAppkey>365c2949-0fb3-4d81-9dd2-421727bf08e3</securegatewayAppkey>

**Webaccess Scanning (WASP):**

---

**NOTE:** WASP does not specify the direction of a message, so do not enable scan by message direction when creating a WASP policy.
---

On the GroupWise Web Access Server:
edit the file: /var/opt/novell/groupwise/webaccess/webacc.cfg
edit the following lines

```
#GWAVA Virus Scan
GWAVA.enabled=true
```
GWAVA.version=7
GWAVA.host=<Secure Messaging Gateway IP or Hostname> For example, 151.155.209.46
GWAVA.apiKey=<Secure Messaging Gateway Application Key(see above)> For example, ed89c7a4-840a-4b30-9477-ac1e57363d44

Example: If a webaccess policy is created that blocks messages that have a message size greater than 100k, then if a user attempts to send a message whose total size is greater than what the policy allows, then the webaccess client will alert the user with a dialog stating: “This mail cannot be sent for security reasons.” which is what WASP is limited to communicating.

The WASP log will be found on the GroupWise server under /var/opt/novell/groupwise/webaccess/logs

**MTA Scanning:**

On the MTA:

Edit the domain.mta file

Add the following lines to the end:

```bash
--vscan-EXCLUDE
--vstype-MESSAGE
--vsaction-DISCARD
--vsserver=<Secure Messaging Gateway Host> For example, 151.155.209.46
--vsdomain=<Your Domain> For example, jimmyhop125.com
--vsnamevalue=<gwavaman><mta_agent><id_object></id_object></mta_agent></gwavaman>
--vskey=<Secure Messaging Gateway Application Key(see above)> For example,"7de7780f-6ffb-47fb-af82-4f7c996d8ae3"
--vsnoadm
--vsnostatus
--vsport-7108
--vscanner="/opt/novell/groupwise/agents/bin/gwmtavs"
```

NOTE: The MTA does not have a user interface so will be unable to alert the client of issues. Configure the policy with notification to alert the user.

**IMAP Scanning:**

Scan IMAP. See “IMAP Interface” on page 123
IMAP Scanning

To configure IMAP scanning you will need to create and configure a Policy, then create and configure IMAP interfaces.

Create a Policy

Under Policy Management, add a new policy and give it a name, for example, "IMAP Policy".

Make sure that the policy is enabled.

To enable the policy you must enable either "Limit by interface type", or enter IMAP into "Matched interface type", or both.

Save the Policy.

Configure a Policy

Under Policy scan configuration add the desired filters, services and exceptions.

A recommended configuration is a Statistics Recorder and Message Tracker for all messages, and an Anti-Virus blocker.

Create IMAP interface

Under IMAP Interface Manager it is recommended to create two IMAP scanners one for the initial scan of the post office and another for regular scanning.

Initial scan interface: With an existing post office it will need to be scanned and that may take considerable time depending on the size of the post office.

Regular scan interface: Once the post office has been scanned it should be scanned regularly, either on a weekly or monthly schedule. A monthly scan will generally take longer than a more frequent scan.

Configure IMAP Interface

Host server: The server to host the interface.
Stats module: The Statistics engine to save the data.

Scan policy: Which scan policy to use.

Enabled: Make sure it is turned on.

IMAP server address: The address of the IMAP server. The default port is 143 or specify the port the IMAP server is using.

Use SSL: Enable if desired.

IMAP service type: This may be Generic IMAP user which requires a mailbox name and password, or GroupWise post office which requires the Trusted Application Key and Trusted Application Name.

Scan frequency: Sets how often the scanner runs.

On demand: Press Run Now button to start (best for initial scan).

Run Once: Set the date for the scanning to begin, for example over the weekend.

Week Days: Set the days of the week and start scan time (good for recurring scans).

Monthly: Set the day of the month and start scan time (good for recurring scans).

Minimum message size: Sets the smallest sized message to scan, and ignore smaller.

Maximum message size: Sets the largest sized message to scan, and ignore larger.

Scan date range:

Scan all messages: best for the initial scan.

Number of days prior to scan start.

Customer date range.

Messages since previous scan: best for regular scans.

Scan users (GW only)

Scan resources (GW only)

Scan trash (GW only)

Expunge purged items: remove items that are purged.

User scope: (GW only)

Scan all users (recommended)

Limit to defined user list

Limit to all except defined user list

Folder scope:

Scan all folders (recommended)

Limit to defined folders list

Limit to all except defined folders list
Address Transformation Manager

Address Transformation Manager allows you to transform an incoming or outgoing email address to a different email address. Very useful for mergers and acquisitions or other name changes.

Address Transformation Manager is not OU aware, it needs to know what the addresses are independently of the OU, we need all the address information. This does not change the MIME file, it just changes the SMTP transactions and routes to the new domain.

Address transformation appears to the interface only, not the filtering engine. The filter will get the original address. You may need to create a filter for both the original and target transformed recipient.

There are two parts: The transformation and the interface. Once a transformation has been created it needs to be enabled in an interface, currently only the SMTP interface is supported.

This feature is found under Module Management | Address Transformation Manager.

Add New: Click the “Add New” button to create a new address transformation.

Provide the transformation a name: For example, “gwava to microfocus” or “icecream2custard” or “left>right”.

Enable rewrite rule: Enable or disable the rule.

Notes: A text field for a reminder to your future self on why you set this up.
Serviced interfaces: Enable the interface the rule should be applied to or enable in the Interface.

Apply to the inbound mail: Enable to apply to inbound mail.

Apply to the outbound mail: Enable to apply to outbound mail.

Apply to sender: Enable to apply to senders.

Apply to recipient(s): Enable to apply to the recipient.

*Rewrite rules section*

The rule matches a pattern and then replaces the pattern according to the rules you set.

**Match pattern**

Patterns can be matched with a complete email address such as “user.oldLastName@myDomain.com” or with wildcards such as “*.yourDomain”. You may even use “*@*” to transform everything that comes in.

**Replace pattern**

The replace pattern depends on the match pattern you entered.

**Examples:**

Transform a Domain: If you merged with another company, you may find the need to transform the old email addresses to the new ones. You would use:

Match: *@oldDomain.com with Replace: $1@newDomain.com

Transforms user@oldDomain.com into user@newDomain.com

Transform a Single Email Address: If a user changed their name, you can transform any incoming mail to their old name to their new name.

Match: userOriginalAddress@myDomain.com with Replace: userNewAddress@myDomain.com

Transforms userOldLastName@myDomain.com into userNewLastName@myDomain.com

**Change Domain Case:** To change the case of your domain.

Match: *@DOMAIN.ORG with Replace: $1@domain.org

Transforms user1@DOMAIN.ORG into user1@domain.org. What is happening is $1 = the wildcard “**” and $2 = “@DOMAIN.ORG”.

**Change Domain TLD:** If you have changed your TLD you can transform the address and move the old TLD so you know who is still using the old address.

Match: user@Domain.* with Replace: $2/$1com to preserve domain case structure or $2/user@domain.com to also change the domain case structure at the same time.

Transforms user@Domain.org with org/user@Domain.com. What is happening is $1 = “user@Domain.” and $2 = the wildcard “**”.

**Transforming everything:** You may use wildcards in all parts of the email address for transformations. Each wildcard transition becomes a variable.

*   @   *   .   *
Save the changes.

Enable Address Transformation in the SMTP Interface “SMTP Interface” on page 118, if not enabled under Serviced Interfaces above.

Message direction can be controlled on a per interface level in the SMTP Interface Manager. You can have one SMTP interface handle all the transformations.

In the SMTP Interface Manager, you can control Inbound, Outbound, Sender, and/or Recipient and override on a per interface level.

In the Address Transformation Manager, you generally would have a single rule to handle all address transformations. You would create additional rules when you want a rule to apply to only a single interface to make change tracking easier.

**Scan Engine Manager**

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

![Scan Engine Manager Diagram]

**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” on page 156 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.

Send test message: Click button to send test message.
Module Administration

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.

Retry count: Number of times the message will be resent to the destination before failure. Default 8.

Retry Interval: Number of seconds between retry attempts. Default 900 seconds, or 15 minutes.

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.
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.
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.

**Serviced OU set**: Enable OUs to be serviced.
Policy Administration

Organization / Policy Management allows you to manage Users, Roles, Organizations, Domains and Policies on the system.

Policies are how you can control the flow of mail and spam into your system. Policies are the key concept in running your Secure Messaging Gateway system successfully. See also Chapter 7, “Policy Configuration Tips and Tricks,” on page 201

Organization / Policy Management Overview

When configured Overview shows the activity of the policy or policies.

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 configured (see Creating a Statistics and Tracking Policy “Creating a Statistics and Tracking Policy” on page 201), 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.

*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.
Policy Administration

**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

Policy Administrator
Policy User

- Overview
- Settings
- Manage Users
- Manage System Roles
- Manage Custom Roles
- Manage Organizations
- Domain Management
- Policy Management
- Policy scan configuration

- Role Members
  - admin

- Assigned User Interfaces
  - [Default] Full system access interface
  - Message Tracker interface
  - Quarantine system interface
QMS Administrator

- Overview
- Settings
- Manage Users
- Manage System Roles
- Manage Custom Roles
- Manage Organizations
- Domain Management
- Policy Management
- Policy scan configuration

**Role Members**

- admin

**Assigned User Interfaces**

- [Default] Full system access interface
- Message Tracker interface
- Quarantine system interface
QMS User

- Overview
- Settings
- Manage Users
- Manage System Roles
- Manage Custom Roles
- Manage Organizations
- Domain Management
- Policy Management
- Policy scan configuration

Role Members
- admin

Assigned User Interfaces
- [Default] Full system access interface
- Message Tracker interface
- Quarantine system interface
Message Tracker

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

![Manage Custom Roles](image)
**Group Management**

The System Administrator can assign a QMS Administrator to manage users and their quarantines. The System Administrator will have to create the group, and enable Expose as QMS Group. Then provide the rights to the QMS Administrator which will allow the QMS Administrator to manage that group. To prevent the QMS Administrator from managing that group without removing the group, the System Administrator can disable Expose as QMS Group.

Make sure that new users are automatically added to the group by enabling Domain Management | <domain> | Auto-provision roles | QMS User.

If you want different groups of users with different rights, a new group would need to be created.

**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 Organization

- **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 OU’s**: 1000000.
- **Maximum child OU depth**: 100.
- **User interface**: [Default] Full system access interface.
- **Default child user interface**: [Default] Full system access interface.

- **Role Availability**
- **Event Availability**
- **Service Availability**
- **Exception Availability**
- **Template Availability**
- **User Interface Availability**
Allow domain patterns: Default, enabled.

Require domain validation: Default, disabled.

Maximum child OU’s: 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
- 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**

The “Add New” button allows you to create a new domain. You will need at least one domain. This should be named after the fully qualified domain name of your email server.

You will need to set up what users can connect and what SMTP server the domain should connect to. You make also enter details for connecting to LDAP for user authentication and DKIM signing.
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 host messages will be directed to on each line.

- Target type
- SMTP server
- Discard
- Target host
- Priority
- Security
- Authentication
- Username
- Password
- Mail (Enable if the SMTP server handles mail)
- Auth (Enable if the SMTP server handles authentication)
- Line limit

A test button allows you to determine if the connection will function.

1. Enter a valid user email address.
2. Click “Start Test”

3. The dialog box will show the connection process to the SMTP server and whether it passed
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%))

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.

1. Enter the LDAP server address as the Target Host.
2. Provide the Distinguished Name and password of the user that has access to authenticate the other users.
3. Enable Auth.
4. Enter the DN Search base for the domain.
5. 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.
- 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.
• 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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAsBgKRxl5FsetvBRRsHN9GU
tylibmbfNwh1wqrY/03Nv8AlZEBFFq9doztZ/ktU155ZGoRX/TPdwrNinhD47qXVf7z6Wz8t2sIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69
Glop/HkeWytStjkk7nVHRXDprUY1/0XSuHFGTDIBK+Ci3yMN98qRcFzWS+kyWj"
   "g44Gt79Xzo/hqv1ESLo4SSdNQtb0VxwGFJ6kpO1LP2EJBqIBaWtYOAxrx9Kf2hvVCV6uhRV4iyzd5o9IrwedkIx7QyYdGu7C+I+B1h9bVd6VxuzX7gxxX722iYewA1h5iJBAAd7jwIDAQAB"

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

   ![Deployment Workbench](image)

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.

![Policy Management](image)

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 polices 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.

**Set the Policy Priority**

On the right side of the policy title bars are sorting arrows.

Messages move through policies from top to bottom. If you have more than one policy use the arrows on the right on the panel to move the policy up or down. A message will flow through until the first policy that it applies to triggers, then one subsequent policies will see the message as it has left the system. For example, if an outboard policy adds a signature based on a keyword in the message then no other lower policies with different signatures will scan the message.

You can organize policies by direction. An inbound message will only trigger on an inbound policy.

---

**NOTE:** It is recommended that there is at least one policy per interface.

---

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 be selecting items more options are revealed.
• **Enabled**: Default, checked

• **Bypass Scanning**: If enabled, if the message enters this policy, this policy will not scan the message and not allow the message to the next policy. Default, disabled.

• 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 in bytes
  • Maximum message size in bytes
- Limit by interface type
  - Invert interface type list: Reverses the effect of the listed items.
  - Matched interface types: Click on [type list] to get a list of supported interfaces.
- Limit interface
  - Invert interface list: Reverses the effect of the listed items.
  - A list of available interfaces will be available here.
- Limit by processing server
  - Invert server list: Reverses the effect of the listed items.
  - A list of processing server names will be available here.
  - *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.

**SMTP Policy Creation With the Wizard**

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

1. Under Policy Management, when creating a new policy you will have to choose if the policy is SMTP or IMAP.
2. Select the Message Flow Direction. You can choose Inbound and/or Outbound.

![New Policy Setup Wizard](image1)

**Message Flow Direction**
Welcome to the policy setup wizard. This wizard will assist you in configuring a new scan policy, installing the recommended base scan features based on your selections.

Which message directions should this policy scan mail for? This selection will determine the types of filters chosen for configuration by the wizard.

- [x] Inbound mail
- [x] Outbound mail

![Cancel Continue](image2)

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

![New Policy Setup Wizard](image3)

**Feature Selection**
Please select the main features you would like configured, then press the continue button

- [x] Anti-Virus
- [x] Anti-Spam

![Cancel Continue](image4)

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

![New Policy Setup Wizard](image5)

**Anti-Virus**
Virus prevention is best achieved by combining a variety of filters which prevent known viruses, and potential sources of viruses that might contain viruses that have not yet been classified.

- [x] Detect viruses by signature (recommended)
- [x] Block common attachment types that contain viruses

![Cancel Continue](image6)
5. Select if you want messages quarantined.

![Quarantine Screen]

Quarantine
From time to time, messages may be incorrectly identified with the mail filters. Because of this, it is recommended that the quarantine service is enabled to capture these messages for review.

Enabling this option will not allow detected viruses to be captured, and these will specifically be excluded from being placed in the quarantine.

☑ Enable quarantine

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

![Message Tracker Screen]

Message Tracker
We need to put text here to describe the message tracker option

Enabling this option will add the Message Tracker Service to the Received Message Filter so tracking information will be recorded for every message.

Only users with the message tracker role will be able to search or view this tracking information.

☑ Enable message tracker

7. A summary of what the wizard will do will appear.
8. In a moment, it will be done.

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

11. Set the Policy Priority

**IMAP Policy Creation With the Wizard**

Create a new policy with the wizard. Click on *Add with wizard*. 
1. Under Policy Management, when creating a new policy you will have to choose if the policy is SMTP or IMAP.

2. There will be another dialog box that provides an overview.

3. IMAP Scanning Overview
   The IMAP scanner service provides inspection and/or removal of messages stored on an IMAP server. To use this service you must have access to the interface management pages of the system. Once the policy is created, it can be selected as the provider of scan services for any IMAP interfaces.

4. Select Access Method
5. **Select Access Method**

Choose the type of scan to perform with this IMAP policy.

If this is your first time using the IMAP scanner, it is recommended that inspection mode is initially used. As inspection mode is non-destructive it will only report on items discovered in the IMAP server, leaving all data intact.

- **Inspection Mode**

  This operation mode will inspect the IMAP server for content based on defined filters, recording findings into the Message Tracker system and/or the administration quarantine. It is useful for discovering data or threats in an IMAP server without removing any items.

- **Cleanup Mode**

  This operation mode will inspect the IMAP server for defined threats and remove items that match. Be careful to be sure that the filters used in this mode are intended to remove data, as misconfiguration can result in a loss of data.

6. **Inspection Mode**
Install Summary

A sample configuration will be generated that includes anti-virus and text filters. The policy that will be created will be configured to work in the requested manner, with additional options for both inspection and scan mode made available but disabled to allow easy adjustment at a later time.

Use the items generated in the configured policy as a guide to create your own filtering and scanning options as necessary.

If you are happy with the list below, press continue to proceed with the setup procedure.

- Policy will provide virus, text, attachment type and fingerprint filters.
- Text filter will be empty, ready for population as required.
- Attachment and fingerprinting filters will be populated with common threat types.
- Virus, attachment and fingerprint filters will be configured to report to Message Tracker.
- Text filter will be configured to report to Message Tracker and place a copy in the admin quarantine.

7. Then you will get a message that the policy creation is complete.
8. Setup Complete

Your policy has been configured and is now active. To access and edit the policy, open the 'Policy Scan Configuration' folder in the navigation panel and select the policy from the list.

To activate this policy, an IMAP interface must be created in the system. From the IMAP interface, select the policy to be used for the scan from the 'Scan policy' option on that page.
IMAP Inspection Policy Reference

<table>
<thead>
<tr>
<th>Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>If disabled, the policy will be skipped. Default: enabled (checked).</td>
</tr>
<tr>
<td>Bypass scanning</td>
<td>If enabled, message scan requests will still be processed but the message will not be scanned. Default: disabled (unchecked).</td>
</tr>
<tr>
<td>Scan by message direction</td>
<td>If enabled, you can choose between:</td>
</tr>
<tr>
<td>- Handle inbound mail</td>
<td></td>
</tr>
<tr>
<td>- Handle outbound mail</td>
<td></td>
</tr>
<tr>
<td>- Handle internal mail</td>
<td></td>
</tr>
<tr>
<td>- Handle collected mail</td>
<td></td>
</tr>
<tr>
<td>Limit by source address</td>
<td>Allows you to limit what addresses to include or exclude. Default: disabled (unchecked).</td>
</tr>
<tr>
<td>Limit by recipient address</td>
<td></td>
</tr>
<tr>
<td>Limit by sender IP address</td>
<td></td>
</tr>
<tr>
<td>Limit by message size</td>
<td></td>
</tr>
<tr>
<td>Limit by interface type</td>
<td></td>
</tr>
<tr>
<td>Invert interface type list</td>
<td></td>
</tr>
<tr>
<td>Matched interface types</td>
<td>IMAP</td>
</tr>
<tr>
<td>Limit interface</td>
<td></td>
</tr>
<tr>
<td>Limit by processing server</td>
<td></td>
</tr>
<tr>
<td>Scan archives by default</td>
<td></td>
</tr>
<tr>
<td>Maximum archive scan depth</td>
<td>6</td>
</tr>
<tr>
<td>Maximum archive files</td>
<td>1000</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>

- Enabled: If disabled, the policy will be skipped. Default: enabled (checked).
- Bypass scanning: If this option is enabled, message scan requests will still be processed but the message will not be scanned. Should a scan request find a match to the policy then the message will NOT be passed to the next policy. Default: disabled (unchecked).
- Scan by message direction: If enabled, you can choose between:
  - Handle inbound mail
  - Handle outbound mail
  - Handle internal mail
  - Handle collected mail (only for IMAP interface)
- Limit by source address: Allows you to limit what addresses to include or exclude. Invert address list and Match address list options are revealed when enabled. Default: disabled (unchecked).
- Limit by recipient address: Allows you to limit what addresses to include or exclude. Invert address list and Match address list options are revealed when enables. Default, disabled (unchecked).
- Limit by sender IP address: Allows you to limit what addresses to include or exclude. Invert address list and Match address list options are revealed when enables. Default, disabled (unchecked).
- Limit by interface type: Select which interface types to be used. Default, disabled (unchecked). Invert interface type list and Matched interface types [type list]: Default, IMAP.
- Limit interface: Select which interface to use. Default, disabled (unchecked).
- Limit by processing server: Limit which processing servers the policy can use. Default, disabled (unchecked).
- Scan archives by default: Default, enabled (checked).
- Maximum archive scan depth: Depth of archive to scan. Default, 6.
- Maximum archive files: Maximum number of archive files to scan. Default, 1000.
- Notes: Reminders to your future self about why this was setup the way it was.

**Cleanup Mode**

Cleanup mode is identical to inspection mode, except that it will remove messages that meet the parameters.

**IMAP Policy Workbench**

The IMAP policy wizard will create an Inspection policy with Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, Named Executable Filers, and Text filters. This will track the messages, with an Admin Quarantine for the Text Filter.
The IMAP policy wizard will create an Inspection policy with Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, Named Executable Filers, and Text filters. This will track the messages, and block qualifying messages.
**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 with sends out 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 its 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.

**Clam Anti-Virus**

SMG can use Clam Anti-Virus malware definitions to scan items.

This filter is can be added manually to a profile. It is not added when using the wizard.

Under Manage Servers each configured server will show the Clam Anti-Virus service version, which is the time stamp of the definitions in use. New definitions are downloaded and updated throughout the day.
Clam Anti-Virus is used just like the Anti-Virus filter and can be run in parallel with the Anti-virus filter.

**Options**

This item does not require configuration.

**DKIM Verification**

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/). 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.

Some file types are subsets of other file types. For example MSOFFICEEX are all MS Office XML files, MSOFFICEXT are just MS Office Template files and would ignore non-template files and MSOFFICEXM are just MS Office XML documents that have macro enabled. If you want to filter all MS Office files the MSOFFICEEX would be the only file type you would need.

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.

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. i.e. 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. Treat ~all (softfail: allow mail whether or not it matches the record parameters) as -all (fail: only allow mail that matches at least one of the record parameters.) See OpenSPF. (http://www.openspf.org/SPF_Record_Syntax)

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.

**NOTE:** End users do not see these Admin Quarantine messages in their own Quarantine.

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).

DKIM Sign

The DKIM Sign allows for the signing of outgoing messages. See Enabling DKIM Signing “Enabling DKIM Signing” on page 218 for more information.

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).

Ham Reporting

Ham Reporting adds a link to a suspect message to allow the user to confirm that it is a valid (ham) message rather then an undesired (spam) message.

Options

Message size limit: Scan messages smaller than this limit. In bytes. Default, 131073.

Storage Duration: In days, 0 or less will purge on that day’s purge of data. Default, 4.

Signature template: Default, Spam Report Template (en).

Placement priority: Placement of signature priority in relation to other signatures. 0 is highest. Default, 0.

Release server URL: Does not normally need to be filled in. Default, the URL of the Report server.

Report server: Default, automatic.
**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. If you create a filter group and connect the Notify service only to the group then the only the group will be referenced in the message. If you connect all the filters in the group to the Notify service then they will each be referenced, if activated. This is useful if you want to hide a function such as a forward for record keeping purposes. If the forward is in a filter group then only the group will be seen.

For example, if an Attachment Size filter triggered because 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” on page 96.
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: There are a number of customizations that can be made and the text box to make them, see below for details.

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).

**Customization**

*SenderName*: Sender display name.

*Subject*: Notification subject.

*MessageText*: Text message body.

*MessageHTML*: HTML message body.

*HideFilterList*: This will hide what filters were activated be the message.

*IncludeRecipientDetail*: This will add a list of recipients to the notification message. You may want to consider adding this if you want a notification of what triggered a filter. You may not want this if you do not want the sender or recipients to know who may have received the message.

**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.

Spam Reporting

Spam Reporting adds a link to a suspect message to allow the user to confirm that it is an undesired (spam) message rather then a valid (ham) message.

Options

Message size limit: Scan messages smaller than this limit. In bytes. Default, 131073.
Storage Duration: In days, 0 or less will purge on that day's purge of data. Default, 4.
Signature template: Default, Spam Report Template (en).
Placement priority: Placement of signature priority in relation to other signatures. 0 is highest. Default, 0.
Release server URL: Does not normally need to be filled in. Default, the URL of the Report server.
Report server: Default, automatic.
Force SSL in report link: Linked to the release server URL. Default disabled.
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. (User-name 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.
Policy Configuration Tips and Tricks

Policies need to be created for Secure Messaging Gateway to filter messages.

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

The following are examples of policy implementations.

Creating a Statistics and Tracking Policy

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

1. Create the Policy
2. 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.

3. Set the Policy Message Direction
4. Open the panel and enable Scan by message direction then enable Handle inbound mail and Handle outbound mail.
5. Configure the Scanner

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

7. Add the Filter

8. 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.
9. **Add the Service**

10. 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.

11. 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.
12. Click on Save and the policy will become active immediately. All messages passing through Secure Messaging Gateway will have statistical data and message tracking.

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

14. View Results

15. Statistical data will appear under Organization / Policy Management | Overview

<table>
<thead>
<tr>
<th>Date</th>
<th>Subject</th>
<th>Sender</th>
<th>Recipient(s)</th>
<th>Detection</th>
<th>Block State</th>
<th>Sending IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>08-Jun-2017</td>
<td>Fruit flavors are used in this drink. 12634568901</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>The bad pattern on the brand was good. 49898908901</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>Whittings are small fish caught in nets. 2124345654</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>A thick coat of black paint covered all. 18238765030</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>The wolf is trying to chase a sheep. 34668987660</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>A rat built the nest to rebuild. 13576796800</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>none</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>The fly made its way along the wall. 826514929</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>full</td>
<td>198.135.183.142</td>
</tr>
<tr>
<td>08-Jun-2017</td>
<td>They fish guy whom the ship arrived in port. 239989891</td>
<td><a href="mailto:script@sf.grovia.net">script@sf.grovia.net</a></td>
<td><a href="mailto:test2@abc.net">test2@abc.net</a></td>
<td>internal</td>
<td>full</td>
<td>198.135.183.142</td>
</tr>
</tbody>
</table>
Creating a Block and Quarantine with Exceptions Policy

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

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.

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

Create the Policy

1. 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.
2. Set the Policy Message Direction
3. Open the panel and enable Scan by message direction then enable Handle inbound mail.

4. Configure the Scanner
5. Open the Policy scan configuration folder and select the policy. The workbench will be empty.
6. **Add the Filter**

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

8. **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.

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

10. **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.

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

12. For this example we will use the Message Test filter.

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

14. 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.
15. The filter will now scan messages for the word “unsubscribe”, but without one or more services nothing will be done with the message.

16. Add Service

17. 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.
18. 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.

19. Add the Quarantine Service

20. 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.
21. 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).

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

23. Add an Exception

24. 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.
25. 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 Message Direction

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

Configure the Scanner

1. Open the Policy scan configuration folder and select the policy. The workbench will be empty.
2. Add the Filter
   
   There are two filters that will block viruses: Anti-Virus and Zero Hour Virus.
3. 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.
4. Drag the filters to the Workbench.
5. The filter will now scan messages for the word “unsubscribe”, but without one or more services nothing will be done with the message.
6. Add Service
7. Select the Services tab.
8. 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.
9. Connect the Red Services pin to the service with drop and drop.

10. Press *Save*.
11. 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.
3. 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".

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.
Policy Configuration Tips and Tricks

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.

**Black List and White List QMS Configuration**

1. Log into the QMS as the System Administrator, or as a QMS Administrator with the ‘Expose as QMS group’ option enabled in Manage Custom Roles.
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.

Creating a DKIM Verification Policy

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. For more information on DKIM please see OpenDKIM.org. (http://opendkim.org/)

Blocking Messages Without a Valid DKIM Signature

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

1. 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.
2. 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.

3. 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.

4. 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.

Enabling DKIM Signing

DKIM signing is a DNS function. For more information on DKIM please see OpenDKIM.org (http://opendkim.org/).
Prerequisites

DKIM signing needs to be configured under the domain in Secure Messaging Gateway.

A public key needs to be created or configured in the domain. This key will need to be entered into your public DNS so that recipients may verify the signature.

For example:

```
20171003._domainkey IN TXT { "v=DKIM1; k=rsa; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCQAMMIIBCqRCAQESqRkKsStvBRRsHN9Gu
tyibmbFw1qwrtnAY/03Nn8A12Z8FFgb9doztz/ktU1552GoRX/
TvMrWInhD47qXVF7z6Wz8tZsIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3AreqjACtFt4+FQ69Glop/
HkeWyStjkk7nVHRXDprYU1/0XSuHFGTID1BK+C13yMN89qRcFzWS+kyWj""g44Gt79XZOh/
qv1ESLo4SGd8qtb0VwsGf6kO1LP2EJBq1BaWt=YOAzr9Kf2hvVCP6uhRV4iyzd5o9Irw
edkIx7QyDGu7cI+bh9bVd6VuxuX7gxx72iYewAhn5iJBAAd7jwIDAQAB" } ; ----- DKIM key
```

Setting up DKIM Signing

1. 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=MIIBIjANBgkqhkiG9w0BAQEFAAOCQAMMIIBCqRCAQESqRkKsStvBRRsHN9Gu
   tyibmbFw1qwrtnAY/03Nn8A12Z8FFgb9doztz/ktU1552GoRX/
   TvMrWInhD47qXVF7z6Wz8tZsIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3AreqjACtFt4+FQ69
   Glop/HkeWyStjkk7nVHRXDprYU1/0XSuHFGTID1BK+C13yMN89qRcFzWS+kyWj""g44Gt79XZOh/
   qv1ESLo4SGd8qtb0VwsGf6kO1LP2EJBq1BaWt=YOAzr9Kf2hvVCP6uhRV4iyzd5o9Irw
   edkIx7QyDGu7cI+bh9bVd6VuxuX7gxx72iYewAhn5iJBAAd7jwIDAQAB"

3. Finally, you need to create a DKIM signing service in Secure Messaging Gateway, either in an existing policy or in its own policy. No other configuration is necessary. In this example all mail will have DKIM signatures added. More sophisticated filters can be created if only some emails should be signed.
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.

Creating HAM and SPAM Reporting Policy

These policies allow users to report messages that are good that were quarantined (ham) and bad messages that were allowed through (spam).
Spam Reporting

To enable Spam Reporting, which adds a link to the recipient message so they can report spam that had gotten through the system to the spam scanning corpus.

1. On the workbench, add an Anti-Spam filter and enable Invert node logic, finally connect it to the Spam Reporting Service.
2. Inverting the node logic is important because that allows non-Spam message to pass. The Anti-Spam filter checks the message against the spam corpus to determine if it is spam or not. Without inverting the node logic we would already believe the message to be spam and there would be no reason to report it.
3. Anti-Spam Filter > Spam Reporting
4. Invert node logic: Is this known Spam? No > Attach Spam Reporting link. If not inverter this will not put a spam link on if the message is known spam.
5. When a user clicks on the link, they will be taken to a web page and told: Thank you for reporting the spam message, and the training corpus will be updated with the message. If they wait beyond the storage duration, they will be thanked, so as not to confuse them, and the message will not be able to be sent to the training corpus.

Ham Reporting

The opposite of Spam Reporting.

1. On the workbench, add an Anti-Spam filter, and connect it to the Ham Reporting Service.
2. This can be used with a Junk Folder. For example, on a smaller site without a quarantine for all users the Anti-Spam filter can be connected to a Add Header Line Service, to add a Junk Flag header that the mail client can have rules enabled for, a Message Tag to added a Spam header, and the Ham Reporting Service. If the user finds a non-spam message in their junk folder they can use the Ham Reporting link to report the false negative.

Adding Clam Anti-Virus

Clam Anti-Virus adds additional definitions for scanning. Clam Anti-Virus is used just like the Anti-Virus filter and can be run in parallel with the Anti-virus filter “Creating an Anti-Virus Policy” on page 211.
Solving “No policies were located to scan this message”

When creating a new policy on a new SMG server you may find that the policy may not work on a test message.

When you check the gwava log: /opt/gwava/services/logs/gwava-<#>/<date>.log you find:

[139685115610880] 2018-08-10 12:10:02 (ppst)<6> Processing scan requests
[139685115610880] 2018-08-10 12:10:02 (QUMN) No policies were located to scan this message
[139685115610880] 2018-08-10 12:10:02 (rrqs)<6> Sending response to client
[139685115610880] 2018-08-10 12:10:02 GWAVA client connection finished processing
[139685115610880] 2018-08-10 12:10:02 (chnd)<6> Closing gwava client handler

This tends to mean that the fully qualified domain name for your domain is not in place.

Go to the System Administration console | Organization \ Policy Management \ Domain Management and set the domain to the fully qualified domain name of your email server.

Block Outbound Messages Not From Your Domain

A policy can be created to prevent messages from leaving your domain that are claiming to be from another domain, if a mailbox in your domain is compromised. Adding an email filter that allows only messages coming from your domain to leave the system prevents someone from sending emails from your domain while claiming to be from another domain.

1. Create an outbound message policy, and set it to the top of the list so it activates first.
2. Add an Email Address filter.
3. Invert the node logic.
4. Enable Scan sender address
5. Enter your domain as the search criteria with a leading wild-card. For example, *company.com.
6. Connect the filter to a Message Block service.
Quarantine System

The quarantine is where suspicious messages are stored until someone can deal with them or they are removed because they have been in quarantine too long.

Quarantine

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.

As the System Administrator all quarantined messages will be shown.

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

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.
**Forward Messages**

- **Forward message as attachment**
- **Forward from original sender**
- **Forward from** [alpha@sf.gwava.net]
- **Forward to** [test6@sf.gwava.net]
- **Subject** [Forwarded message from GWAVA quarantine system]

You may insert a comment into the forwarded message

[Forward] [Cancel]

**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 to 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?**

[OK] [Cancel]

**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?**

[OK] [Cancel]

**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.
Quarantine Options

The Options tab provides access to setting information.

Core Settings

Core Setting are the user definable options available.

**CORE SETTINGS**

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

Login name test0@doc.mf.net

**My User Interface Options**

Maximum number of messages returned from a search: All.
Number of messages per page: 20.
Number of days to search: Last 3 days.
Inactivity Timeout: 10 minutes.

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.

Mail from addresses that match the sender and recipient pairs in the white list will bypass all filters associated with the quarantine white list.

Items may be removed from the white list by selecting and pressing the Delete button.
A sender/recipient pair may be added by pressing the Add 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.

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 whitelist.
Quarantine Digest

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

Enable global 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.
### Manual Release Tab

Beyond the standard digest setup, certain custom options can be set.
**Digest release period**

The current digest time period starts at 01:00:00 PM Thu on 22 Feb 2018

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: 22 Feb 2018

**Custom digest release**

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

Start date: 22 Feb 2018
End date: 22 Feb 2018

Select users:
- admin
- QMS_Admin
- test1@doc.mf.net
- test2@doc.mf.net
- test3@doc.mf.net
- test4@doc.mf.net

- 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.

Quarantine Users

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

Quarantine Groups

Users can be organized into Groups to make management easier.

Groups are created by the System Administrator as a Custom Role “Creating a Group” on page 155.

Quarantine Settings

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

User Interface Options

- Maximum number of messages returned from a search: All
- Number of messages per page: 20
- Number of days to search: Last 3 days
- Inactivity Timeout: 10

Default User

User Interface Options
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

<table>
<thead>
<tr>
<th>Quarantine</th>
<th>Options</th>
<th>Digest</th>
<th>Users</th>
<th>Groups</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message Retention</td>
<td>Forward From Quarantine</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Message Retention Policy

Enable quarantine message pruning:

- Check box

Days to retain messages in quarantine:

- 60

Prune message information:

- Check box

Delete stored messages:

- Check box
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**

<table>
<thead>
<tr>
<th>Quarantine</th>
<th>Options</th>
<th>Digest</th>
<th>Users</th>
<th>Groups</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default User</td>
<td>Message Retention</td>
<td>Forward From Quarantine</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Forward From Quarantine**

- Forward as an attachment template: Default, Forward From Quarantine (en).
- Preferred forward as an attachment language: Default, English (en).

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

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

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

Message Tracker interface

Select the Message Tracker when logging in to view.

Each column can be sorted by clicking on the arrows.

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.

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.

Date Range

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

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
This User guide will make you familiar with the Quarantine management system so you can manage suspicious messages that are attempting to come to you and do things like black list email addresses that you know are bad and white list email addresses you know are good.

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.

If you believe the message was quarantined in error, you can allow delivery to be completed by selecting the Release action under the Action column.

If this is from a legitimate sender and you want the sender to always be allowed through, you can allow delivery for this and all other messages by selecting the Whitelist action under the Action column.

If this is from a sender that you never want to see again, you can block all messages by selecting the Blacklist action under the Action column.

You can also manage your quarantine by clicking on the "Manage my Quarantine" button, which will open your browser to the Secure Messaging Gateway server.
Quarantine Management System

You can manage your quarantine by logging into the Quarantine Management System (QMS) using your email credentials.

This brings you to the main quarantine screen in the QMS.

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.
- **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.

A sender may be added by pressing the Add 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.

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 whitelist.