

Secure Messaging Gateway Administrator and User Guide

September 2025

Legal Notices

Copyright 2025 OpenText.

The only warranties for products and services of OpenText and its affiliates and licensors ("OpenText") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. OpenText 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	9
1 Overview	11
OpenText Secure Messaging Gateway Overview	11
Overview	11
Key Concepts	11
OpenText GWAVA Family of Message Handling Products	12
2 Release Notes	13
3 Installing Secure Messaging Gateway	15
System Requirements	15
Hardware Requirements	15
Installing SMG	16
SLES OS Modifications Reference	19
Configuring SMG	21
Post-Installation Tasks	28
On the Secure Messaging Gateway server	28
On the Email Server	31
Installing Additional Servers into an Existing Network	32
Overview	32
Setup	32
Setting up a Multi-Tenant System	35
Securing the SMG Web UI	35
Customizing the Login Screen	37
4 System Administration	39
System Overview	39
System Administration Console	39
Console Navigation Bar	40
System Management	41
Manage Servers	41
Enabling SSL on Secure Messaging Gateway	43
Reference	44
Recovering a Secure Messaging Gateway Server	45
Languages	46
Templates	46
Custom Templates	47
User Interfaces	50
URI Association	51
Database Connections	52
Supported databases	53
Deploying a Database	53

File System Rights	54
Password Control	58
Encrypting an SMG Password:	58
System Alerts	58
Alert Test	59
Scanner Diagnostic	59
Licensing	61
Online Updates	62

5 Module Administration 65

Module Management	65
Module Status	65
Starting and Stopping Modules	65
Interfaces Overview	65
SMTP Interface	66
SMTP Module Troubleshooting	71
IMAP Interface	72
IMAP Interface Manager	72
Reference	72
3rd Party Integration	75
GroupWise 18	76
IMAP Scanning	79
Address Transformation Manager	81
Scan Engine Manager	83
Load Balancing	84
Fault Tolerance	84
Organizational Units	84
Message Filter engine	85
Mail Relay Module Manager	85
QMS Module Manager	87
Stats Module Manager	89
Message Tracker Module Manager	90

6 Policy Administration 91

Organization / Policy Management Overview	91
Settings	92
Manage Users	93
Manage System roles	95
Roles	96
Manage Custom Roles	101
Create Custom Role	102
Creating a Group	103
Group Management	104
Manage Organizations	104
Add New Organization	105
Domain Management	108
Add New	109
Policy Management	114
Set the Policy Priority	115
Manual Policy Creation	116

SMTP Policy Creation With the Wizard	117
IMAP Policy Creation With the Wizard	122
Importing and Exporting Policies	130
Policy Scan Configuration	132
Component Settings	135
Filters	137
Anti-Spam	137
Anti-Virus	138
Attachment Name	138
Attachment size	138
Black List	138
Clam Anti-Virus	139
DKIM Verification	139
Email Address	139
Filter Group	140
Fingerprint	140
IP Address	140
IP Reputation	141
Message Received	141
Message Size	141
Message Text	142
RBL	142
SMTP Envelope	143
SPF	143
SURBL	143
Zero Hour Virus	143
Services	144
Add Header Line	144
Admin Quarantine	144
Block	145
Carbon Copy	145
DKIM Sign	145
Event Writer	145
Ham Reporting	148
Interface Control	149
Message Signature	149
Message Tag	149
Message Tracker	150
Notify	150
Quarantine	151
Quarantine Control	152
Spam Reporting	152
Statistics Recorder	153
Exceptions	153
Email Address	153
Exception Group	153
IP Address	154
Message Text	154
SMTP Envelope	154
White List	155
7 Policy Configuration Tips and Tricks	157
Creating a Statistics and Tracking Policy	157

Creating a Block and Quarantine with Exceptions Policy	162
Creating a policy manually involves:	162
Create the Policy	162
Creating an Anti-Virus Policy	167
Create the Policy	168
Set the Policy Message Direction	168
Configure the Scanner	168
Enabling Black List and White List	169
Configure Black list:	170
Configure White list:	172
Black List and White List QMS Configuration	172
Creating a DKIM Verification Policy	173
Blocking Messages Without a Valid DKIM Signature	173
Sending a Notification That a Message Has a Valid DKIM Signature	174
Enabling DKIM Signing	174
Prerequisites	175
Setting up DKIM Signing	175
Creating HAM and SPAM Reporting Policy	176
Spam Reporting	177
Ham Reporting	177
Adding Clam Anti-Virus	177
Solving “No policies were located to scan this message”	178
Block Outbound Messages Not From Your Domain	178

8 Quarantine System 181

Quarantine	181
Quarantine Options	184
Core Settings	184
White List	185
Rights	185
Owned Addresses	186
Delegated Access	186
Quarantine Digest	187
Settings Tab	188
Schedule Tab	189
Manual Release Tab	190
Quarantine Users	192
User Rights	193
User Options	193
Group Membership	194
Quarantine Groups	194
Quarantine Settings	194
Default User	194
Message Retention	195
Forward from Quarantine	196

9 Message Tracker 197

Message Tracker interface	197
Search	198
Date Range	198
Message Details	199

10 SMTP Authentication	201
Introduction	201
SMTP Authentication Settings	203
Interface Settings	204
OU Level Settings	206
Configuration Scenarios	214
Email Address Spoofing Prevention	214
Simplified Filter Control	215
External Relay	216
Targeted User/Address Authentication	216
Shared Login	217
 11 User Guide	 219
Quarantine Management System	219
Quarantine Email	219
Quarantine Management System	220
 12 Migrating Secure Messaging Gateway	 225
Migrating SMG from the Appliance to a New Server	225
Prerequisites and Considerations	225
Migrating to a New Server	226
Migrating to SMG from Another Message Processing Product	229

Preface

About This Guide

This OpenText 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 OpenText Technical Support at <https://www.microfocus.com/support-and-services/> (<https://www.microfocus.com/support-and-services/>)

Sales

OpenText contact information and office locations: www.opentext.com (<http://www.opentext.com>)

To contact a OpenText sales team member, please call (866) 464-9282, or +1 (514) 639-4850 in North America.

1 Overview

OpenText Secure Messaging Gateway Overview



OpenText Secure Messaging Gateway (SMG) provides inbound & outbound protection for your company's enterprise network & messaging system, including antivirus, anti-spam, cybercrime protection, and DDOS protection.

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

Overview

Secure Messaging Gateway (SMG) is designed to run the SMTP scanner for any email system in the market. The SMTP scanner and SMG 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 SMG 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 SMG, which scans then sends clean email to the MTA. Mail sent from your domain will pass through the normal system, but the SMTP Gateway will send the mail to Secure Messaging Gateway, which sends the email to the internet.

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 108](#).
2. The interfaces to be scanned will need to be configured [“Interfaces Overview” on page 65](#).

3. Scanning policies will need to be created so messages will be scanned [“Organization / Policy Management Overview” on page 91.](#)
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 187.](#)

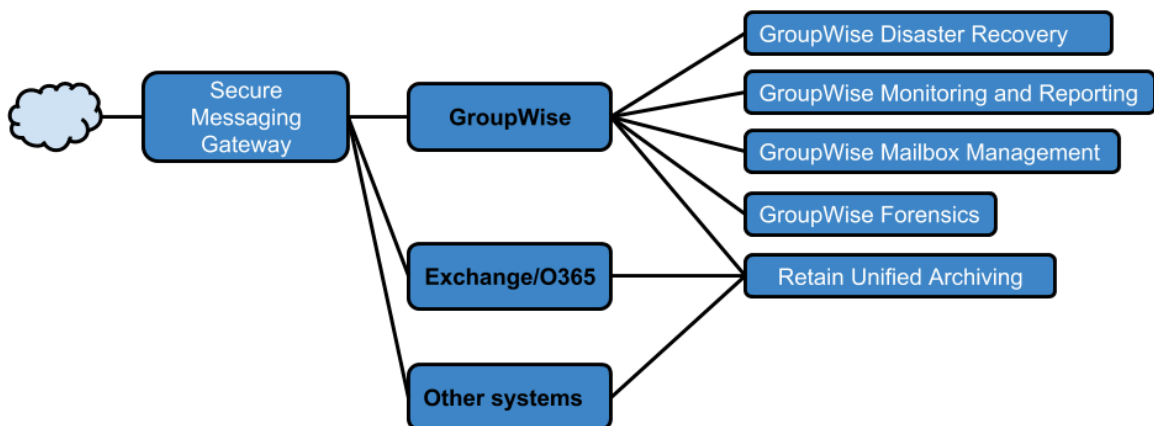
For normal use of SMG, the sysadmin should be familiar with:

- ♦ Creating and Managing Policies [Chapter 7, “Policy Configuration Tips and Tricks,” on page 157.](#)
- ♦ Using the Quarantine System [“Quarantine” on page 181.](#)
- ♦ Using the Message Tracker [Chapter 9, “Message Tracker,” on page 197.](#)

OpenText GWAVA Family of Message Handling Products

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

- ♦ *OpenText 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.



2 Release Notes

New Features in 25.3

- ♦ Added support for SLES 15 SP6
- ♦ The **Manage Servers > Remote AUTH min SSL protocol** has been set by default to TLS 1.2

3 Installing Secure Messaging Gateway

- ♦ [“System Requirements” on page 15](#)
- ♦ [“Installing SMG” on page 16](#)
- ♦ [“Configuring SMG” on page 21](#)
- ♦ [“Post-Installation Tasks” on page 28](#)
- ♦ [“Installing Additional Servers into an Existing Network” on page 32](#)
- ♦ [“Setting up a Multi-Tenant System” on page 35](#)
- ♦ [“Securing the SMG Web UI” on page 35](#)
- ♦ [“Customizing the Login Screen” on page 37](#)

System Requirements

Hardware Requirements

SMG is provided through an installation script that enables access to a download repository. The hardware requirements to download the SMG repository are as follows:

- ♦ SLES 15 SP5 and SP6 or openSUSE LEAP 15.5 and 15.6
- ♦ 1 CPU
- ♦ 8 GB RAM
- ♦ 120 GB Hard Drive (for base OS and SMG)

NOTE: Storage capacity requirements will vary and may need to be larger depending on your specific requirements. The main factors that affect storage requirements are as follows:

- ♦ Peak number of messages processed per minute.
 - ♦ Average message size processed.
 - ♦ Number and duration of messages stored in the quarantine.
-

IMPORTANT: If you are installing a new SMG server to migrate from an older SMG system to SMG 24.3 or later, you must have the same (or more) CPU, RAM, and disk space on your new server as you do on your old server in order to run the migration.

Installing SMG

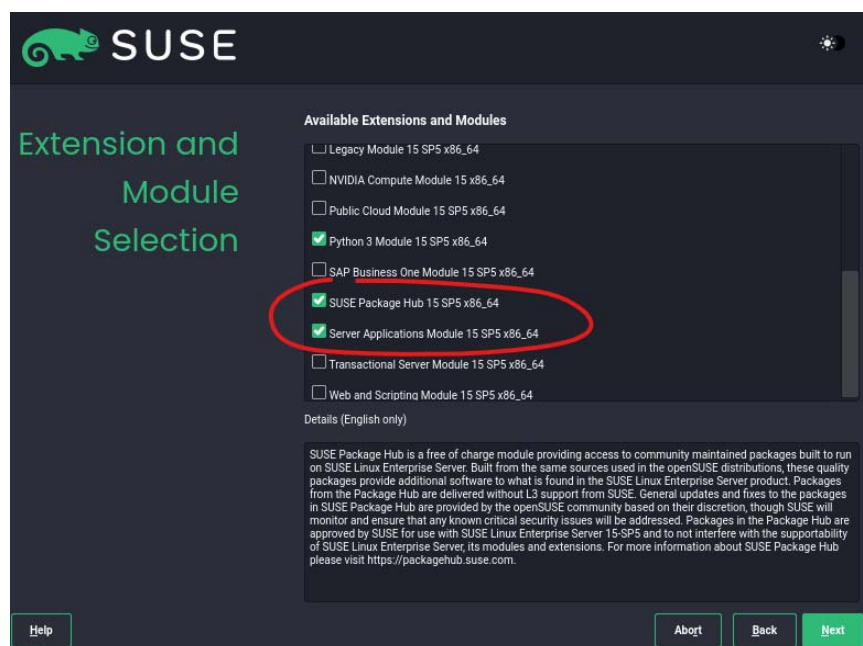
SMG is installed on a SLES 15 or openSUSE 15 server. The steps take you thorough installing the necessary components on your server and then installing SMG.

- 1 Download and install SLES 15 or openSUSE 15 on your server and make sure to do the following during your install:

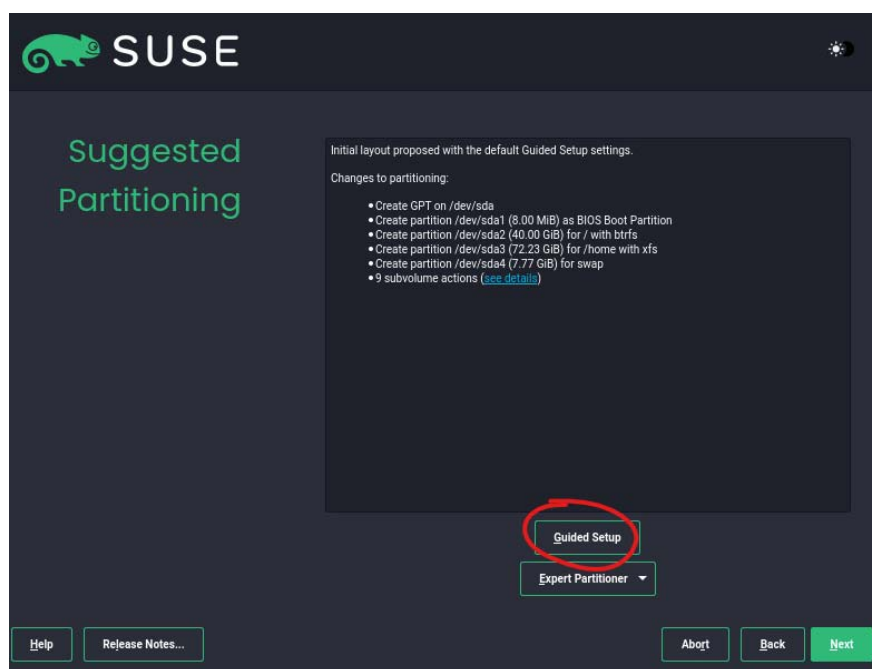
NOTE: The images shows in the steps below are take from SLES 15. If you are installing on openSUSE, your interface will be different.

1. **Skip this step if you are installing on openSUSE.**

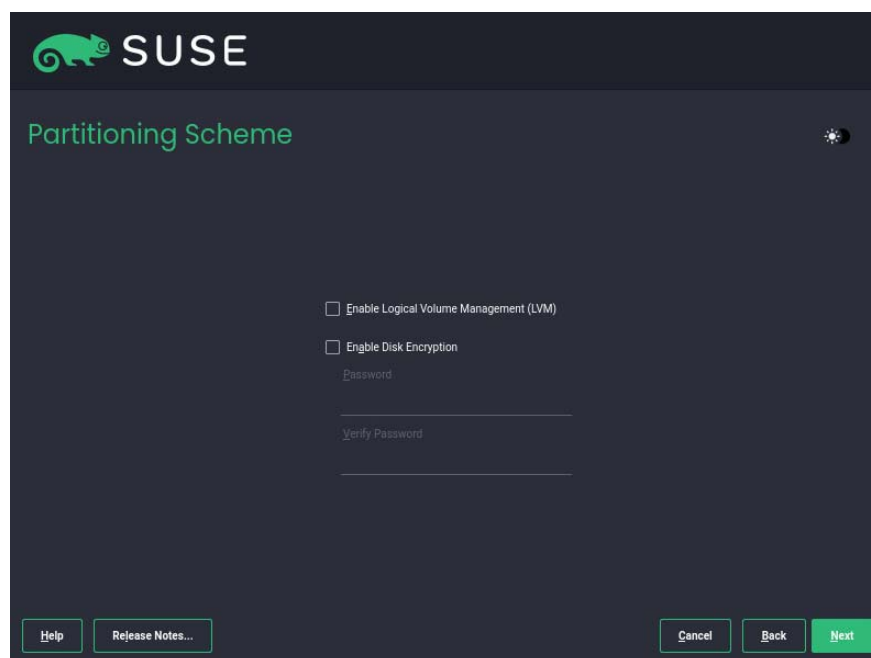
On SLES 15, when prompted for the extensions to install, make sure **SLES Package Hub**, **Basesystem Module**, and **Server Applications Module** are selected.



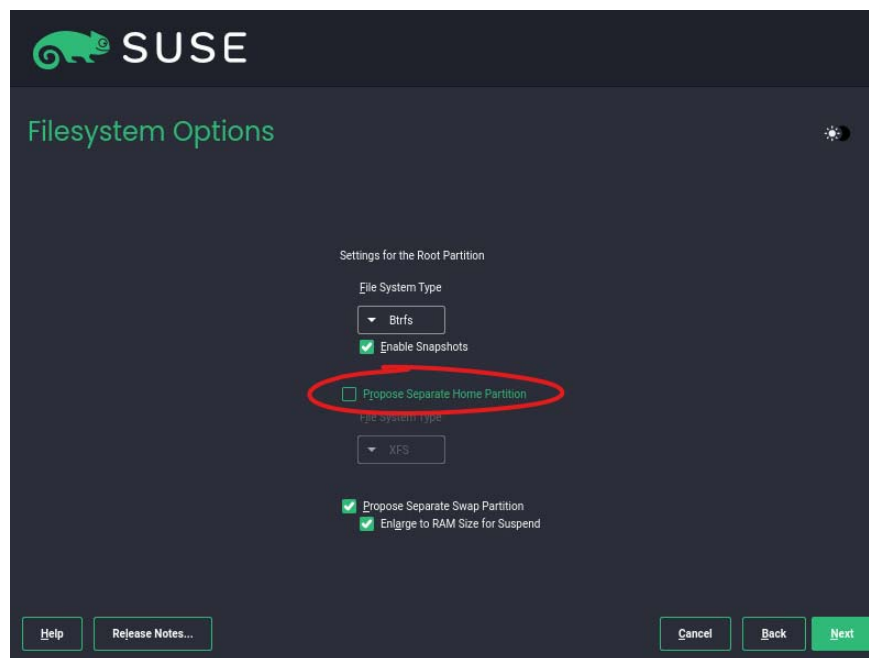
- When the setup wizard reaches **Suggested Partitioning**, select **Guided Setup** and do the following:



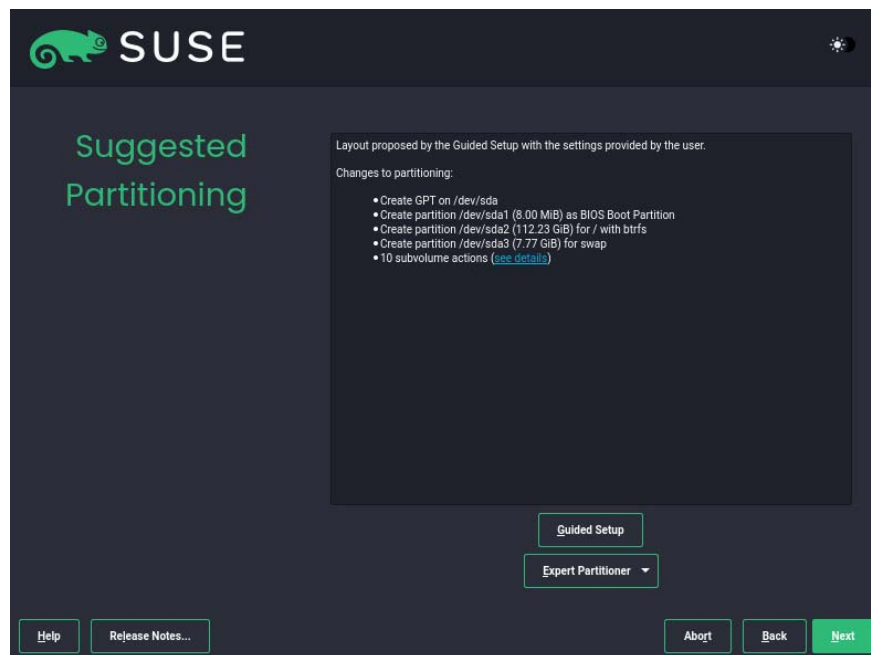
- ◆ Leave the **Partitioning Scheme** with the default settings or adjust them if you have preferences here (SMG has no requirements for these options).



- ♦ On the **Filesystem Options** page, turn off **Propose Separate Home Partition**. Turning this off makes it so most of the disk space is available for SMG. You can change the file system type if you have a preference, otherwise leave it as the default.



The resulting partitioning should look similar to the example below. The partition for / should be the size of most of your disk space.



IMPORTANT: If you already have SLES 15 or openSUSE 15 installed and don't want to install a new server, please make sure that it is updated to at least SP5 and has the **Base System Package** and **Package Hub** extensions installed.

- 2 (Optional) By default, SMG is installed to `/opt/opentext/smg`. If you want to install SMG to a different physical storage location, create a mount point for `/opt/opentext/smg` to the desired location.
- 3 Make sure you are logged into the SLES server as `root` and launch the Terminal application.
- 4 Login to your SLD account and download the following items:
 - ♦ `smg-init-x.x.x.tar.bz2` (download to your server)
 - ♦ SMG license PEM
 - ♦ SMG registration code
- 5 Navigate to where you put the `smg-init-x.x.x.tar.bz2` file in the terminal and run the following commands to extract and run the installer:

```
tar -xf smg-init-x.x.x.tar.bz2
cd smg-init-x.x.x
./smg-init.sh
```

- 6 Follow the instructions in the wizard to install SMG. The install script makes changes to the SLES OS. Some of the changes are optional. Please configure your server to suit your needs. For a list of the changes see [“SLES OS Modifications Reference” on page 19](#).

NOTE: During the installation process, you might see an error that says “Repository ‘SMG-2024-04-BASE’ is invalid”. This error occurs during the registration process that will run again. The error can be disregarded if the install script reports that it completes successfully.

- 7 Continue with [“Configuring SMG” on page 21](#).

SLES OS Modifications Reference

The following changes are made to the SLES OS by the SMG install script. All the changes are optional. Please configure your server to suit your needs and processes.

- ♦ [“Services \(optional changes\)” on page 19](#)
- ♦ [“Apache Configuration \(optional change\)” on page 20](#)
- ♦ [“Postgresql hba File Changes \(required change\)” on page 20](#)
- ♦ [“Postgresql user password \(required change\)” on page 20](#)
- ♦ [“Disable Postfix \(optional change\)” on page 20](#)
- ♦ [“OpenDKIM \(optional change\)” on page 20](#)
- ♦ [“Firewall \(required changes\)” on page 20](#)

Services (optional changes)

The following services are enabled and started:

- ♦ **apache2** - The web server used to access the web management components of SMG, such as the installation wizard, administration console, and quarantine service.
- ♦ **postgresql** - The database server that contains the configuration of SMG.
- ♦ **opendkim** - The service used to manage DKIM mail signing services.

Apache Configuration (optional change)

The `/etc/apache2/listen.conf` file is modified to ensure that the web server is available to browsers on both port 80 and port 443 (secure).

Postgresql hba File Changes (required change)

The `/var/lib/pgsql/data/pg_hba.conf` file is adjusted to allow TCP/IP access to the local database using md5 authentication, required by SMG.

Postgresql user password (required change)

A password is set for the postgres user. This is necessary for SMG to gain privileges to run database creation scripts.

Disable Postfix (optional change)

Postfix is an email server application that is enabled by default. It conflicts with the SMTP server that runs inside SMG. If you want or need to use Postfix, you must configure it to run on a different IP interface or port to prevent conflicts with SMG.

OpenDKIM (optional change)

The `/etc/openssl/openssl.conf` file is adjusted to allow the SMG admin UI to synchronize its configuration and use the service with the following options:

- ♦ SOCKET inet: 4932@localhost
- ♦ Canonicalization relaxed/relaxed
- ♦ Mode sv
- ♦ KeyTable refile: `/etc/optendkim/key.table`
- ♦ SigningTable refile: `/etc/openssl/signing.table`
- ♦ InternalHosts refile: `/etc/openssl/trusted.hosts`
- ♦ ExternalIgnoreList refile: `/etc/openssl/trusted.hosts`

Firewall (required changes)

The following ports are opened for public access:

- ♦ http - web server traffic
- ♦ https - secure web server traffic
- ♦ smtp - email traffic
- ♦ smtps - secure email traffic'
- ♦ postgresql - database server connectivity
- ♦ dns - Hostname lookups
- ♦ 4928 - SMG supervisor application install communications

- ♦ 4929 - SMG scanner application internal communications
- ♦ 4930 - SMG scanner application install communications (secure)
- ♦ 4932 - DKIM API access
- ♦ 3310 - ClamAV traffic

Configuring SMG

- 1 On completion of the initial install, you should now be able to access your SMG web interface by connecting to your server IP address or hostname with a web browser.
- 2 Select **SMG User Interface** to run the SMG install.



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

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 32.

The screenshot shows the 'SERVER INSTALLATION' wizard for Micro Focus Secure Gateway. The 'Role' step is active, showing two options: 'This is the first or only Secure Gateway server' (selected) and 'Connect this server to an existing Secure Gateway network'. The first option includes a checkbox for 'Enable GWAVA 6 migration tools'.

Micro Focus® Secure Gateway

SERVER INSTALLATION

Welcome **Role** Configure Validate Install

Choose the Secure Gateway server role

Secure Gateway is designed to cater for all sizes of systems from small single server mail filtering services up to enterprise grade multi-server environments providing performance and security with fault tolerance and load balancing capabilities.

Please tell me what the role of this server will be in your system.

- ☒ **This is the first or only Secure Gateway server**
 - ☐ Enable GWAVA 6 migration tools
- ☐ **Connect this server to an existing Secure Gateway network**

4 Configure the server:

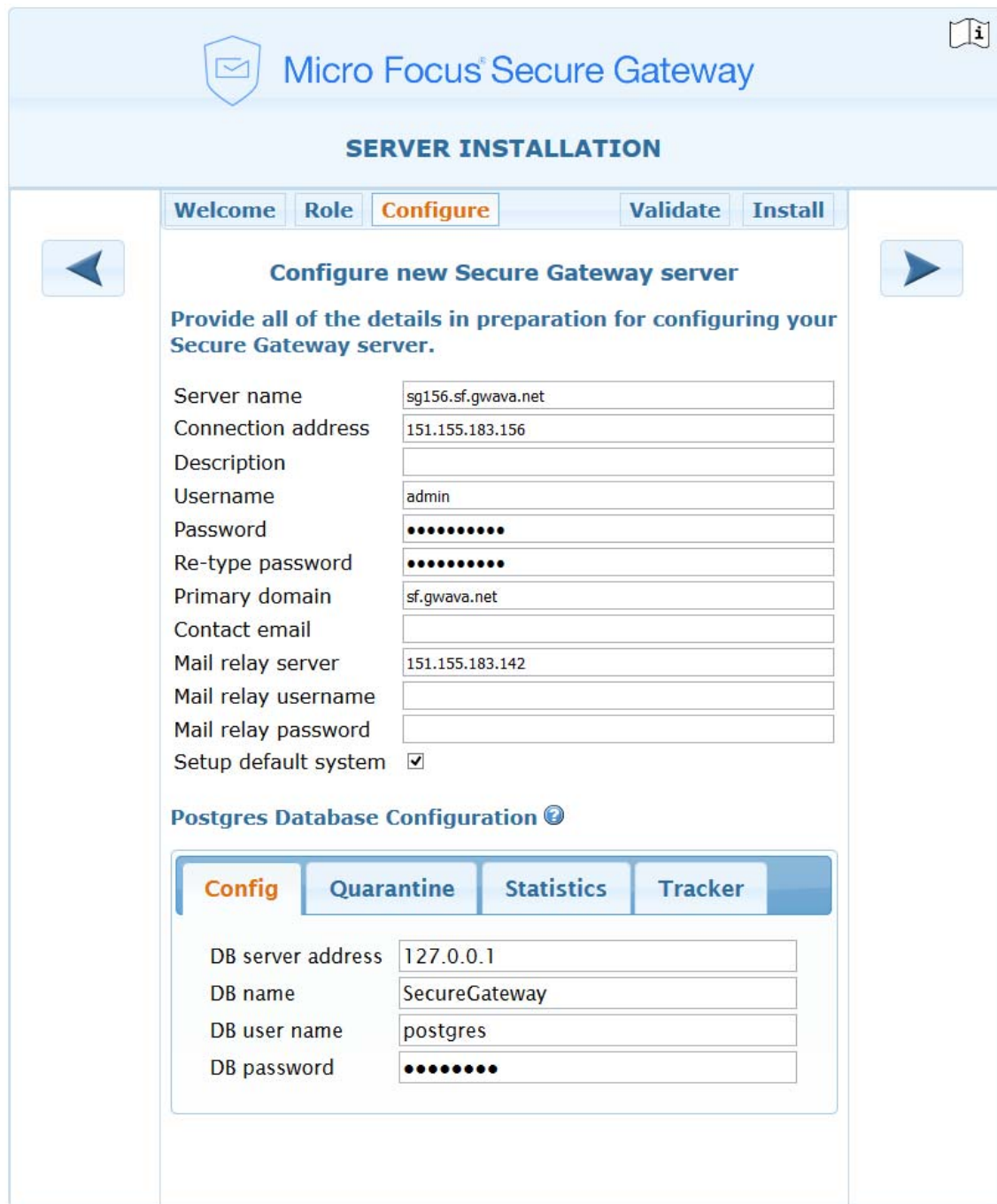
Update the Server name and address.

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.



The screenshot shows the 'Micro Focus Secure Gateway' SERVER INSTALLATION window. The 'Configure' tab is selected, showing fields for server name, connection address, description, username, password, re-type password, primary domain, contact email, mail relay server, mail relay username, mail relay password, and a checkbox for 'Setup default system'. Below this is the 'Postgres Database Configuration' section with tabs for 'Config', 'Quarantine', 'Statistics', and 'Tracker'. The 'Config' tab is active, showing fields for DB server address, DB name, DB user name, and DB password.

Micro Focus® Secure Gateway

SERVER INSTALLATION

Welcome Role **Configure** Validate Install

Configure new Secure Gateway server

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

Server name sg156.sf.gwava.net

Connection address 151.155.183.156

Description

Username admin

Password

Re-type password

Primary domain sf.gwava.net

Contact email

Mail relay server 151.155.183.142

Mail relay username

Mail relay password

Setup default system ☒

Postgres Database Configuration

Config Quarantine Statistics Tracker

DB server address 127.0.0.1

DB name SecureGateway

DB user name postgres

DB password

Postgres Database Configuration

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

- ♦ Config

Postgres Database Configuration

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

- ◆ Quarantine

Postgres Database Configuration

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

- ◆ Statistics

Postgres Database Configuration

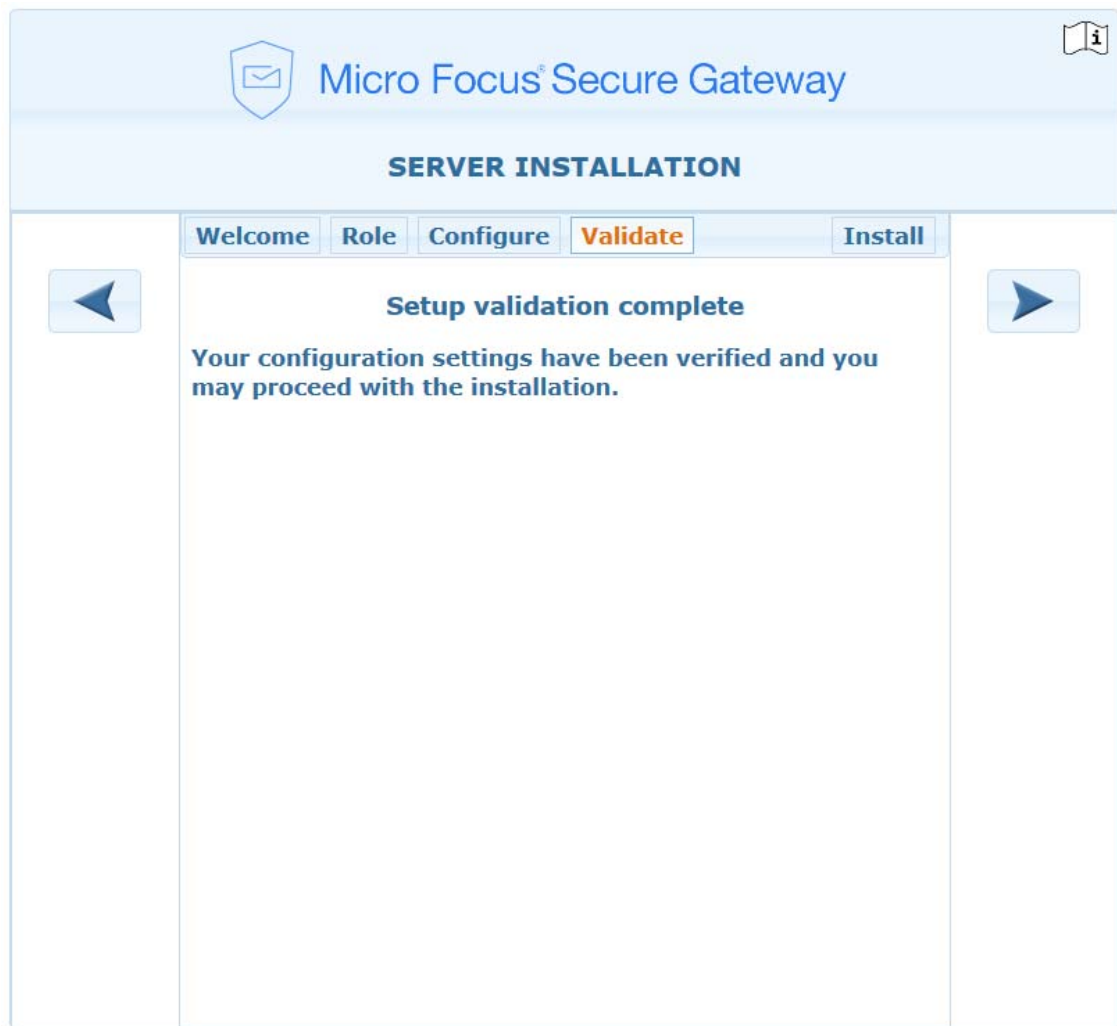
Config	Quarantine	Statistics	Tracker
Create this database <input checked="" type="checkbox"/>			
DB server address		<input type="text" value="127.0.0.1"/>	
DB name		<input type="text" value="SecureGatewayStats"/>	
DB user name		<input type="text" value="postgres"/>	
DB password		<input type="password"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

◆ Tracker

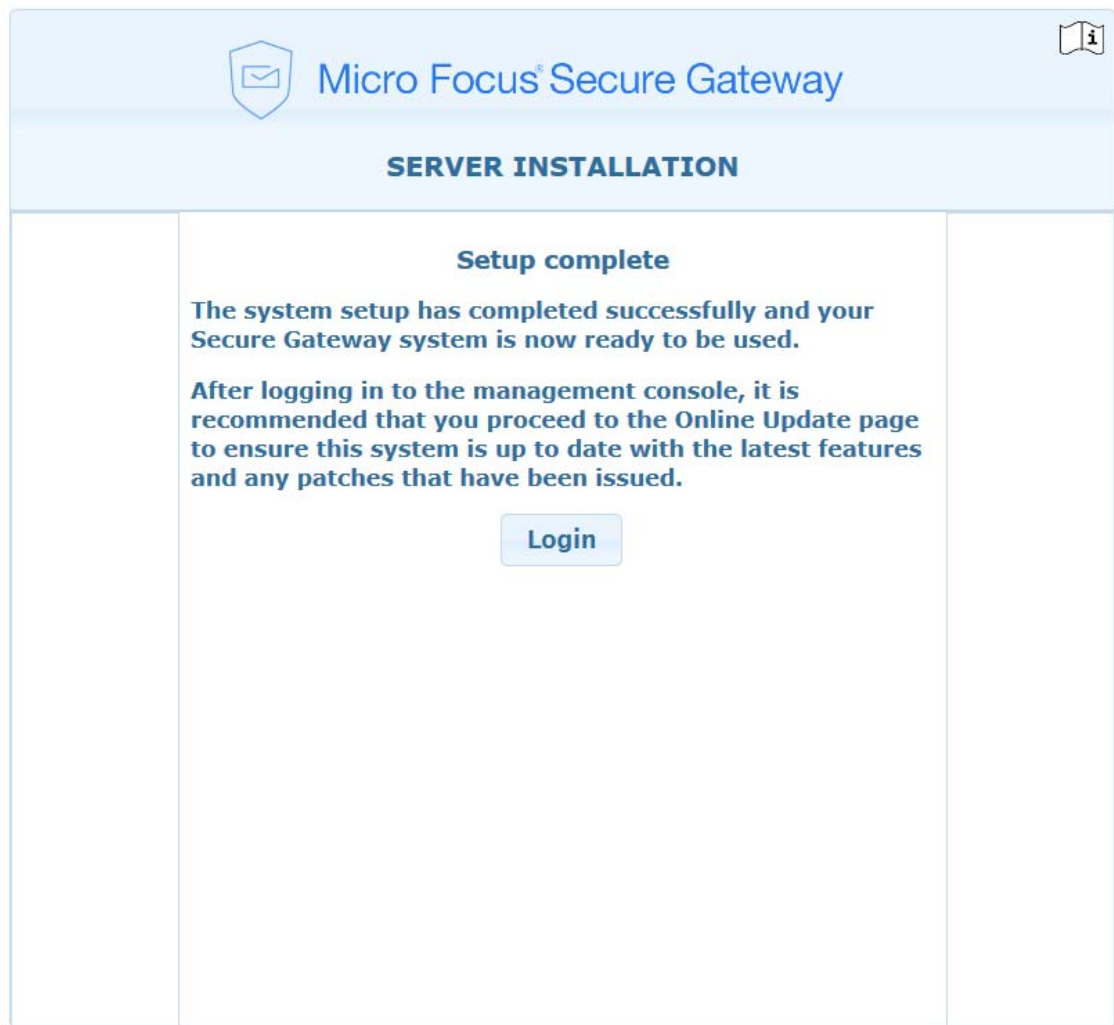
Postgres Database Configuration

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

- 5 Validate. The installer will validate the entered settings.




- 6 Select the forward arrow to 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 Log into the Secure Messaging Gateway.

Micro Focus® Secure Gateway



Login name

Password

Login

Login help

- 8 Continue with [Post-Installation Tasks](#).

Post-Installation Tasks

Once Secure Messaging Gateway is installed and 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

Manage Domains

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

▼ **doc.mf.net**

Enable user auto-provisioning ☒

Auto-provision roles

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

Additional Host Pattern Matches

SMTP Hosts

Target type: SMTP server ▼

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

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

▼ **sf.gwava.net**

Enable user auto-provisioning ☒

Auto-provision roles

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

Additional Host Pattern Matches

SMTP Hosts

Target type: SMTP server ▼

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

LDAP Hosts

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

Notes

2. Create a Policy:

Create at least one policy [“Policy Management” on page 114](#) 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:

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

Quarantine	Options	Digest	Users	Groups	Settings
Settings		Schedule	Manual Release		
Enable global digest services <input checked="" type="checkbox"/>					
Contact email address	<input type="text"/>				
Digest Template	<div>Digest (en) ▼</div>				
Preferred digest language	<div>English (en) ▼</div>				
Maximum digest rows	<div>50</div>				
Release button address	<input type="text"/>				
Digest recipients	<div>Send digest to all users ▼</div>				
Custom address list	<div> <input type="text"/> <input type="button" value="Remove selected"/> <input type="button" value="Add new"/> </div>				

- 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.

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

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:

On the **GroupWise Administration > Internet Agents > SMTP/MIME > Settings** page, set the **Relay Host for outbound messages** to the GWAVA/Secure Messaging Gateway server and set the **Intervals to retry a deferred message** to 5, 5, 10, 20, 60.

- ♦ Exchange:
 - In **Exchange Admin Center > Mail flow > Send connectors** set the send connector to route to the GWAVA/Secure Messaging Gateway server.
- 2. A new SMTP IP address won't be trusted. Add to trusted relays under SMTP Interface > Relay/Host Protection > Allowed relay sources "**SMTP Interface**" on page 66.

Installing Additional Servers into an Existing Network

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

Overview

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

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

Setup

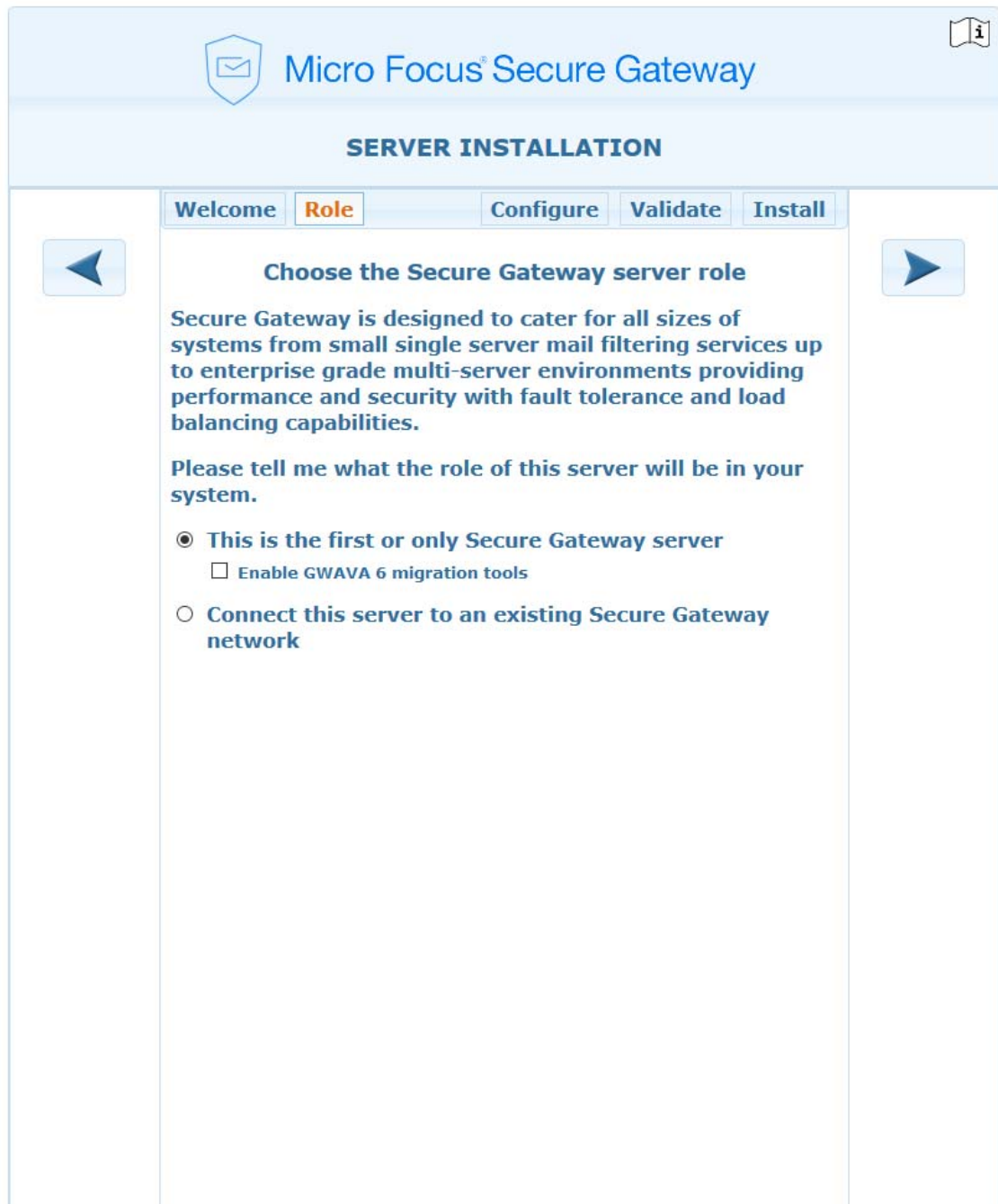
In order for the databases to be accessible to all Secure Messaging Gateway servers, Postgres must be configured to allow remote connections.

1. In a browser, open the VAAdmin Console by going to `https://<ip or dns of SMG server>:9443` and login using `vaadmin` and the password and configure Postgres to allow remote connections.
 - ♦ Enable connections to Postgresql by going to **Configure Postgresql** and entering the IP Address of the SMG server in **Allowed Connections**.
2. Restart Postgres by going to the **System Services**, select **PostgreSQL > Action > Restart**.

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.

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.

3. Install the next Secure Messaging Gateway server. Select **Connect this server to an existing Secure Messaging Gateway network**.



The image shows the 'Role' configuration step of the Micro Focus Secure Gateway server installation. The window has a title bar with the Micro Focus logo and 'Secure Gateway'. Below the title bar is a header section with 'SERVER INSTALLATION' in bold. A navigation bar contains five tabs: 'Welcome', 'Role' (highlighted in orange), 'Configure', 'Validate', and 'Install'. The main content area is titled 'Choose the Secure Gateway server role'. It contains a paragraph describing the gateway's capabilities, followed by a prompt to select the server's role. Two radio button options are presented: 'This is the first or only Secure Gateway server' (selected) and 'Connect this server to an existing Secure Gateway network'. A checkbox for 'Enable GWAVA 6 migration tools' is nested under the first option. Navigation arrows are visible on the left and right sides of the main content area.

Micro Focus® Secure Gateway

SERVER INSTALLATION

Welcome **Role** Configure Validate Install

Choose the Secure Gateway server role

Secure Gateway is designed to cater for all sizes of systems from small single server mail filtering services up to enterprise grade multi-server environments providing performance and security with fault tolerance and load balancing capabilities.

Please tell me what the role of this server will be in your system.

☒ **This is the first or only Secure Gateway server**
☐ Enable GWAVA 6 migration tools

☐ **Connect this server to an existing Secure Gateway network**

4. Configure next Secure Messaging Gateway server.

The screenshot shows the 'Configure' step of the Micro Focus Secure Gateway server installation. The interface has a light blue header with the Micro Focus logo and the text 'Micro Focus® Secure Gateway'. Below the header is a dark blue bar with the title 'SERVER INSTALLATION'. The main content area has a navigation bar with tabs: 'Welcome', 'Role', 'Configure' (highlighted in orange), 'Validate', and 'Install'. On either side of the main content area are blue arrow buttons pointing left and right. The main content area is titled 'Connect to existing Secure Gateway network' and contains the following text: 'Provide all of the details in preparation for configuring your Secure Gateway server.' and 'Additional server configuration may be necessary prior to running this process. Click the information icon in the upper right corner of this page to view the online guide for full details.' Below this text are four input fields: 'Server name' (containing 'sg156'), 'Connection address' (containing '151.155.183.156'), 'Description' (empty), and 'System key' (empty, with a help icon). Below these fields is a section titled 'Postgres Database Configuration' with four input fields: 'DB server address' (containing '127.0.0.1'), 'DB name' (containing 'SecureGateway'), 'DB user name' (containing 'postgres'), and 'DB password' (containing seven dots).

Server name: The name of this server will use.

Connection address: The IP address of this server.

Description: An optional field to describe this server.

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

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

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

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

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

DB name: The name of the database from above.

DB user name: The username for the database.

DB password: The password for the database.

5. Validate and install the server.
6. Login and configure the server. See Post-install Tasks.

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 65](#)
2. Scan engine. [“Scan Engine Manager” on page 83](#)
3. QMS. [“QMS Module Manager” on page 87](#)
4. Message tracker. [“Message Tracker Module Manager” on page 90](#)
5. Statistics. [“Stats Module Manager” on page 89](#)
6. Mail Relay module. [“Mail Relay Module Manager” on page 85](#)
7. Default OU to contain the tenant units. [“Manage Organizations” on page 104](#)
8. Default Policy within the default OU, new tenants will use this policy. [“Policy Management” on page 114](#)
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 51](#)
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:

```

<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 /cert file
    SSLCertificateKeyFile /key file
    SSLCertificateChainFile /Intermediate file

    SSLUseStapling on

    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 43](#) to be accessed via `https://<smghost_address>`

Customizing the Login Screen

The SMG login screen can be customized to use your companies' logo, colors, and style. Most of the default login page must exist in your customized version. There are two ways to customize your login screen: copy the default login.php and make your changes to the copy or create your own login page.

NOTE: If you create your own custom login page, most of the functional parts of the login.php page are required in your own page (like function names and field ids) or the login process won't work.

You can further customize your login screen if you want separate login screens based on role type or organization.

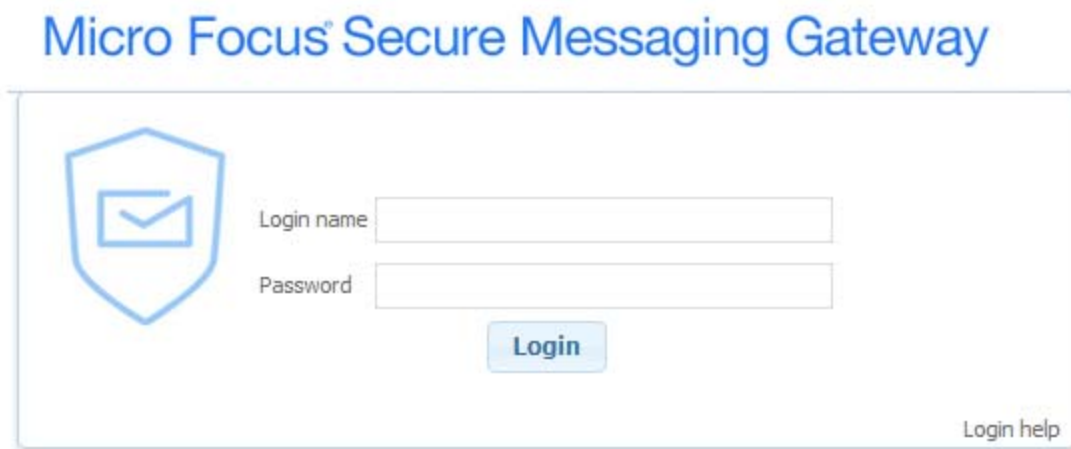
Instructions for all the options can be found in `/opt/opentext/smg/smg-supervisor/http_cgi/skins/README-skinning.txt`.

4 System Administration

System administration is made up of System Management, Module Management [Chapter 5, “Module Administration,” on page 65](#), and Policy Management [Chapter 6, “Policy Administration,” on page 91](#).

System Overview

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



The image shows the login interface for the Micro Focus Secure Messaging Gateway. At the top, the title "Micro Focus® Secure Messaging Gateway" is displayed in blue. Below the title is a login form with a shield icon containing an envelope. The form includes two input fields: "Login name" and "Password". A blue "Login" button is positioned below the password field. In the bottom right corner of the form, there is a link labeled "Login help".

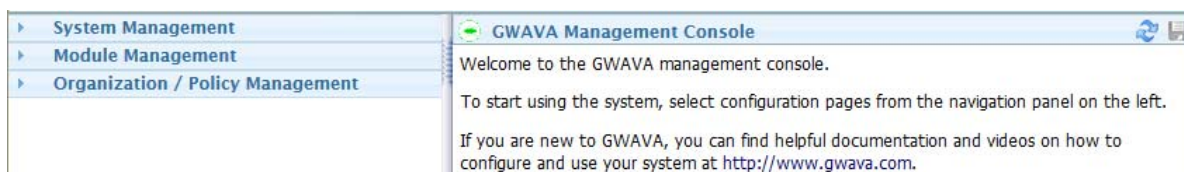
Log into the OpenText Secure Messaging Gateway server and select System Administration.



The image shows a "Select Interface" dialog box with a blue header bar and a close button (X) in the top right corner. The dialog box contains three buttons stacked vertically: "System Administration", "Quarantine System", and "Message Tracker". The "System Administration" button is highlighted with a blue border.

System Administration Console

This takes you to the OpenText Secure Messaging Gateway Management Console

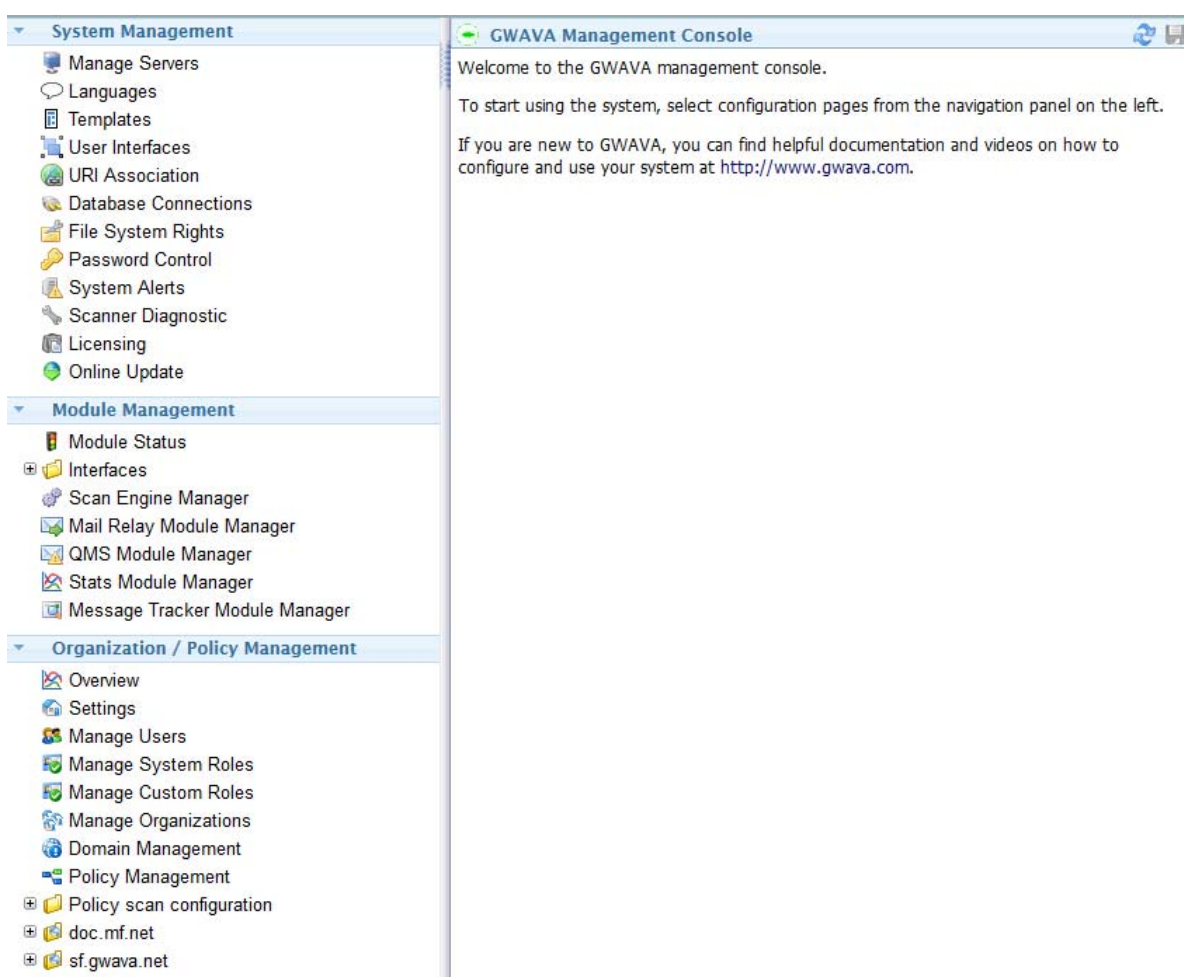


From here you can access the administrative functions of OpenText Secure Messaging Gateway.

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.



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” 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 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 OpenText 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.

The screenshot shows the 'Manage Servers' interface with the following configuration for server 'prv-gwdoc7':

- Database schema version: 213
- Application root path: /opt/microfocus/smg/
- AV signature DB date: Waiting for server to upload data
- Known threat count: Waiting for server to upload data
- ClamAV service version: Waiting for server to upload data
- Description: (empty text box)
- Connection address: prv-gwdoc7.provo.novell.com
- Module auto-recovery: ☒
- Enable log file: ☒
- Days to retain log files: 7
- Maximum log file size (Mb): 10
- Enable SysLog logging: ☐
- SSL certificate file: (empty text box)
- SSL certificate chain file: (empty text box)
- SSL key file: (empty text box)
- SSL pass phrase: (empty text box)
- System logs: Download button
- Admin notify test: Test This Server, Test All Servers buttons
- Web UI SSL redirect: ☒
- Web SSL UI exceptions: 10.*.*.*
172.16.*.*
192.168.*.*
127.*.*.*
- system.xml: [click to view]

- ♦ To recover a server, install a new OpenText 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 OpenText Secure Messaging Gateway programs.

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

The screenshot shows the 'Manage Servers' interface with a server name 'SF145.gwava.com' highlighted in a text box, indicating it is being edited or renamed.

Enabling SSL on Secure Messaging Gateway

Each server in your OpenText 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.

WARNING: You MUST be logged in with the https URL or you will no longer be able to connect to the SMG server.

Manage Servers

Add new
Delete selected
Instructions

▼
☐
prv-gwdoc7

Database schema version	213
Application root path	/opt/microfocus/smg/
AV signature DB date	Waiting for server to upload data
Known threat count	Waiting for server to upload data
ClamAV service version	Waiting for server to upload data
Description	<input type="text"/>
Connection address	<input type="text" value="prv-gwdoc7.provo.novell.com"/>
Module auto-recovery	<input checked="" type="checkbox"/>
Enable log file	<input checked="" type="checkbox"/>
Days to retain log files	<input type="text" value="7"/>
Maximum log file size (Mb)	<input type="text" value="10"/>
Enable SysLog logging	<input type="checkbox"/>
SSL certificate file	<input type="text"/>
SSL certificate chain file	<input type="text"/>
SSL key file	<input type="text"/>
SSL pass phrase	<input type="text"/>
System logs	<input type="button" value="Download"/>
Admin notify test	<input type="button" value="Test This Server"/> <input type="button" value="Test All Servers"/>
Web UI SSL redirect	
Web SSL UI exceptions	<input type="text" value="10.*.*.*"/> <input type="text" value="172.16.*.*"/> <input type="text" value="192.168.*.*"/> <input type="text" value="127.*.*.*"/>
system.xml	[click to view]

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 OpenText 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.

System logs: Click the button to download the logs. Download the logs individually. Also found on the server in /opt/gwava/services/logs/

Admin notify test: Click [Test This Server](#) or [Test All Servers](#) to test that administrator notification is functioning on this server (using [Test This Server](#)) or all servers (using [Test All Servers](#)).

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

[Review the page instructions for details on usage of this information](#)

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

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 OpenText 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 OpenText 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 by 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.

System Management

- Manage Servers
- Languages**
- Templates
- User Interfaces
- URI Association
- Database Connections
- File System Rights
- Password Control
- System Alerts
- Scanner Diagnostic
- Licensing
- Online Update

Language Management

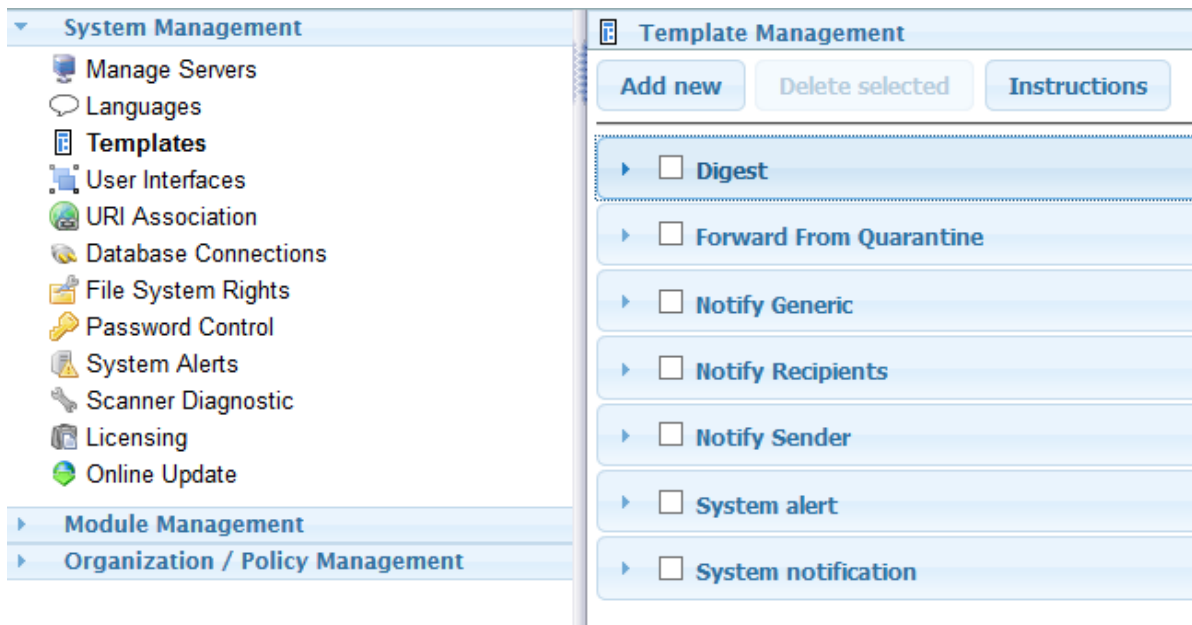
Identify languages that can be offered on this system.

Please note that this list does not set the language of the system. Items enabled here will appear in language selections boxes to provide selections where localized versions of files have been added to the system.

<input type="checkbox"/> Abkhaz (ab)	<input type="checkbox"/> Divehi (dv)	<input type="checkbox"/> Javanese (jv)	<input type="checkbox"/> Norwegian (nn)	<input type="checkbox"/> Swedish (sv)
<input type="checkbox"/> Afar (aa)	<input type="checkbox"/> Dutch (nl)	<input type="checkbox"/> Kabailaut (kl)	<input type="checkbox"/> Norwegian (no)	<input type="checkbox"/> Tagalog (tl)
<input type="checkbox"/> Afrikaans (af)	<input type="checkbox"/> Dzongkha (dz)	<input type="checkbox"/> Kannada (kn)	<input type="checkbox"/> Norwegian (nb)	<input type="checkbox"/> Tahitian (ty)
<input type="checkbox"/> Akan (ak)	<input checked="" type="radio"/> English (en)	<input type="checkbox"/> Kanuri (kr)	<input type="checkbox"/> Nuosu (ii)	<input type="checkbox"/> Tajik (tg)
<input type="checkbox"/> Albanian (sq)	<input type="checkbox"/> Esperanto (eo)	<input type="checkbox"/> Kashmiri (ks)	<input type="checkbox"/> Occitan (oc)	<input type="checkbox"/> Tamil (ta)
<input type="checkbox"/> Amharic (am)	<input type="checkbox"/> Estonian (et)	<input type="checkbox"/> Kherme (km)	<input type="checkbox"/> Ojibwe (oj)	<input type="checkbox"/> Telugu (te)
<input type="checkbox"/> Arabic (ar)	<input type="checkbox"/> Ewe (ee)	<input type="checkbox"/> Kikuyu (ki)	<input type="checkbox"/> Old Church Slavonic (cu)	<input type="checkbox"/> Thai (th)
<input type="checkbox"/> Aragonese (an)	<input type="checkbox"/> Faroese (fo)	<input type="checkbox"/> Kinyarwanda (rw)	<input type="checkbox"/> Oriya (or)	<input type="checkbox"/> Tibetan (bo)
<input type="checkbox"/> Armenian (hy)	<input type="checkbox"/> Fijian (fj)	<input type="checkbox"/> Kirundi (rn)	<input type="checkbox"/> Oromo (om)	<input type="checkbox"/> Tigrinya (ti)
<input type="checkbox"/> Assamese (as)	<input type="checkbox"/> Finnish (fi)	<input type="checkbox"/> Kongo (kg)	<input type="checkbox"/> Ossetian (os)	<input type="checkbox"/> Tonga (to)
<input type="checkbox"/> Avestan (ae)	<input type="checkbox"/> French (fr)	<input type="checkbox"/> Korean (ko)	<input type="checkbox"/> Pali (pi)	<input type="checkbox"/> Tsonga (ts)
<input type="checkbox"/> Aymara (ay)	<input type="checkbox"/> Fula (ff)	<input type="checkbox"/> Kurdish (ku)	<input type="checkbox"/> Panjabi (pa)	<input type="checkbox"/> Tswana (tn)
<input type="checkbox"/> Azerbaijani (az)	<input type="checkbox"/> Galician (gl)	<input type="checkbox"/> Kwanyama (kg)	<input type="checkbox"/> Pashto (ps)	<input type="checkbox"/> Turkish (tr)
<input type="checkbox"/> Bambara (bm)	<input type="checkbox"/> Ganda (lg)	<input type="checkbox"/> Lao (lo)	<input type="checkbox"/> Persian (fa)	<input type="checkbox"/> Turkmen (tk)
<input type="checkbox"/> Bashkir (ba)	<input type="checkbox"/> Georgian (ka)	<input type="checkbox"/> Latin (la)	<input type="checkbox"/> Polish (pl)	<input type="checkbox"/> Twi (tw)
<input type="checkbox"/> Basque (eu)	<input type="checkbox"/> German (de)	<input type="checkbox"/> Latvian (lv)	<input type="checkbox"/> Portuguese (pt)	<input type="checkbox"/> Ukrainian (uk)
<input type="checkbox"/> Belarusian (be)	<input type="checkbox"/> Greek (el)	<input type="checkbox"/> Limburgish (li)	<input type="checkbox"/> Quechua (qu)	<input type="checkbox"/> Urdu (ur)
<input type="checkbox"/> Bengali (bn)	<input type="checkbox"/> Guarani (gn)	<input type="checkbox"/> Lingala (ln)	<input type="checkbox"/> Romanian (ro)	<input type="checkbox"/> Uyghur (ug)
<input type="checkbox"/> Bihari (bh)	<input type="checkbox"/> Gujarati (gu)	<input type="checkbox"/> Lithuanian (lt)	<input type="checkbox"/> Romanysh (rm)	<input type="checkbox"/> Uzbek (uz)
<input type="checkbox"/> Bielman (bi)	<input type="checkbox"/> Hausa (ht)	<input type="checkbox"/> Luba-Katanga (lu)	<input type="checkbox"/> Russian (ru)	<input type="checkbox"/> Venda (ve)
<input type="checkbox"/> Bosnian (bs)	<input type="checkbox"/> Hausa (ha)	<input type="checkbox"/> Luxembourgish (lb)	<input type="checkbox"/> Sanskrit (sa)	<input type="checkbox"/> Volapuk (vo)
<input type="checkbox"/> Breton (br)	<input type="checkbox"/> Hebrew (he)	<input type="checkbox"/> Macedonian (mk)	<input type="checkbox"/> Sanskrit (sa)	<input type="checkbox"/> Vietnamese (vi)
<input type="checkbox"/> Bulgarian (bg)	<input type="checkbox"/> Hierro (hz)	<input type="checkbox"/> Malagasy (mg)	<input type="checkbox"/> Sardinian (sc)	<input type="checkbox"/> Visayan (wa)
<input type="checkbox"/> Burmese (my)	<input type="checkbox"/> Hindi (hi)	<input type="checkbox"/> Malay (ms)	<input type="checkbox"/> Scottish Gaelic (gd)	<input type="checkbox"/> Welsh (cy)
<input type="checkbox"/> Catalan (ca)	<input type="checkbox"/> Hiri Motu (ho)	<input type="checkbox"/> Malayalam (ml)	<input type="checkbox"/> Serbian (sr)	<input type="checkbox"/> Western (fy)
<input type="checkbox"/> Chuvash (cv)	<input type="checkbox"/> Hungarian (hu)	<input type="checkbox"/> Maltese (mt)	<input type="checkbox"/> Shona (sn)	<input type="checkbox"/> Xhosa (xh)
<input type="checkbox"/> Czech (cs)	<input type="checkbox"/> Icelandic (is)	<input type="checkbox"/> Manx (gv)	<input type="checkbox"/> Sindhi (sd)	<input type="checkbox"/> Yiddish (yi)
<input type="checkbox"/> Danish (da)	<input type="checkbox"/> Ido (io)	<input type="checkbox"/> Māori (mi)	<input type="checkbox"/> Sinhala (si)	<input type="checkbox"/> Yngö tî sîngö (yg)
	<input type="checkbox"/> Igbo (ig)	<input type="checkbox"/> Marathi (mr)	<input type="checkbox"/> Slovak (sk)	<input type="checkbox"/> Yoruha (yo)
	<input type="checkbox"/> Indonesian (id)	<input type="checkbox"/> Marshalese (mh)	<input type="checkbox"/> Slovene (sl)	<input type="checkbox"/> Zhuang (za)
	<input type="checkbox"/> Interlingua (ia)	<input type="checkbox"/> Mongolian (mn)	<input type="checkbox"/> Somali (so)	<input type="checkbox"/> Zulu (zu)
	<input type="checkbox"/> Interlingue (iu)	<input type="checkbox"/> Nauruan (na)	<input type="checkbox"/> Southern (st)	<input type="checkbox"/> Kazak (kk)
	<input type="checkbox"/> Inuktitut (iu)	<input type="checkbox"/> Navajo (nv)	<input type="checkbox"/> Southern (nr)	<input type="checkbox"/> Komo kare (kv)
	<input type="checkbox"/> Inupiaq (ik)	<input type="checkbox"/> Ndonga (ng)	<input type="checkbox"/> Spanish (es)	<input type="checkbox"/> Kopriva (ky)
	<input type="checkbox"/> Irish (ga)	<input type="checkbox"/> Nepali (ne)	<input type="checkbox"/> Sundanese (su)	<input type="checkbox"/> Tatar Tene (tt)
	<input type="checkbox"/> Italian (it)	<input type="checkbox"/> Northern (nd)	<input type="checkbox"/> Swahili (sw)	
	<input type="checkbox"/> Japanese (ja)	<input type="checkbox"/> Northern Sans (sa)	<input type="checkbox"/> Swati (se)	

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.

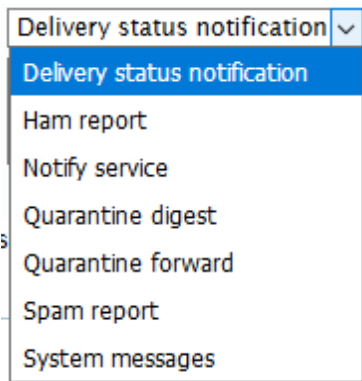
Custom Templates

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

System messages

Ham Report Signature

Spam Report Signature

Template variable keys

Available keys for personalizing digest messages are:

SenderName

Subject

MessageText

AlertSeverity

AlertDetail

MessageText

MessageHTML

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

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

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

To create a custom digest template

1. Go to the Digest panel and Download the Current File: digest_master_en.php to your workstation.

2. Rename the template to something straightforward such as `digest_custom_en.php`.
3. Open the template in a text editor, customize the template as needed, and save when complete.
4. Upload the new template to the next available Upload and select the Default radio button.
5. Press Save to make it available.

The screenshot shows the 'Template Management' window with a 'Digest' tab selected. The 'Service' dropdown is set to 'Quarantine digest'. The 'Template variable keys' field is empty. Under the 'Upload' section, there are three 'Browse...' buttons, all showing 'No file selected.'. The 'Current File' section lists two files: 'digest_master_en.php' and 'digest_custom_en.php'. The 'Default Language' section has three radio buttons, all set to 'English (en)'.

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.

The screenshot shows the 'Template Management' window. At the top, there are three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below these, there is a section for the 'Digest' template, which is currently selected. The 'Service' dropdown is set to 'Quarantine digest'. The 'Template variable keys' field is empty. Below this, there is a table with three columns: 'Upload', 'Current File', and 'Default Language'. The 'Upload' column has four 'Browse...' buttons, each followed by 'No file selected.'. The 'Current File' column shows three files: 'digest_master_en.php', 'digest_custom_en.php', and 'digest_master_de.php'. The 'Default Language' column has three radio buttons and three dropdown menus. The first two radio buttons are selected, and the first two dropdown menus are set to 'English (en)'. The third radio button is unselected, and the third dropdown menu is set to 'German (de)'. The fourth dropdown menu is set to 'English (en)'.

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

User Interfaces

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

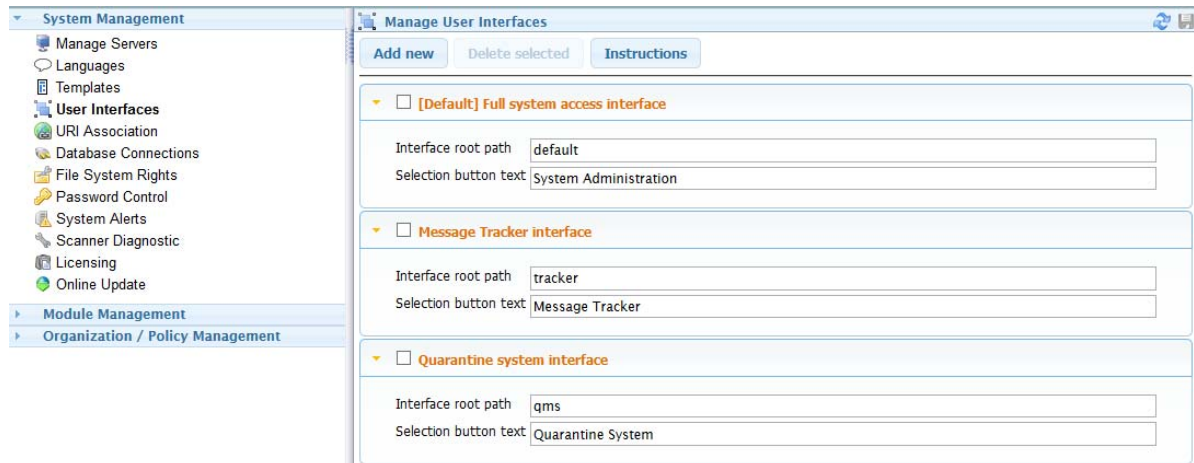
If an administrator wants to modify or customize the login pages and text for either the management console or the QMS interface, this is where the pages and text would be specified.

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

The screenshot shows the 'Manage User Interfaces' window. On the left, there is a sidebar with a tree view of system management options. The 'User Interfaces' option is selected. The main area of the window shows a list of user interfaces. At the top, there are three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below these, there is a list of user interfaces, each with a checkbox and a right-pointing arrow. The list includes: '[Default] Full system access interface', 'Message Tracker interface', and 'Quarantine system interface'. All checkboxes are currently unchecked.

User Interface
<input type="checkbox"/> [Default] Full system access interface
<input type="checkbox"/> Message Tracker interface
<input type="checkbox"/> Quarantine system interface

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



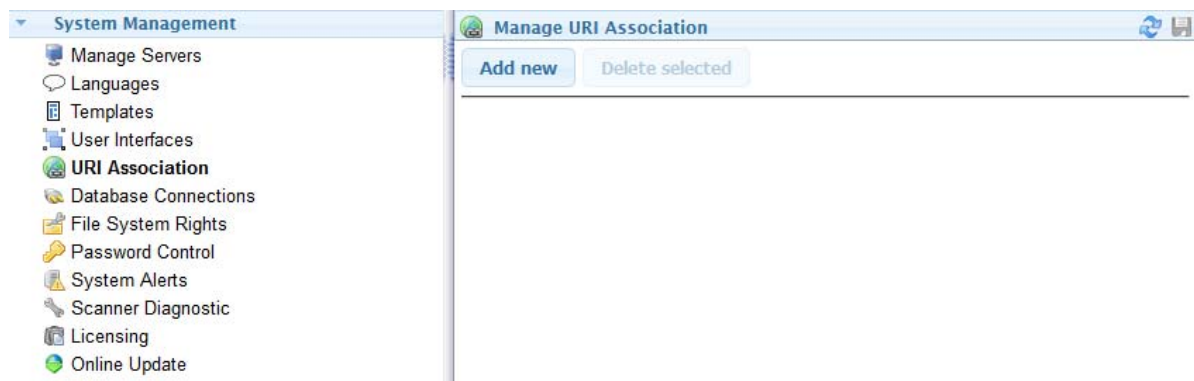
The *Interface root path* changes which section (default for system administration, tracker for message tracker and QMS for quarantine management system) of GWAVA the button logs the user into.

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

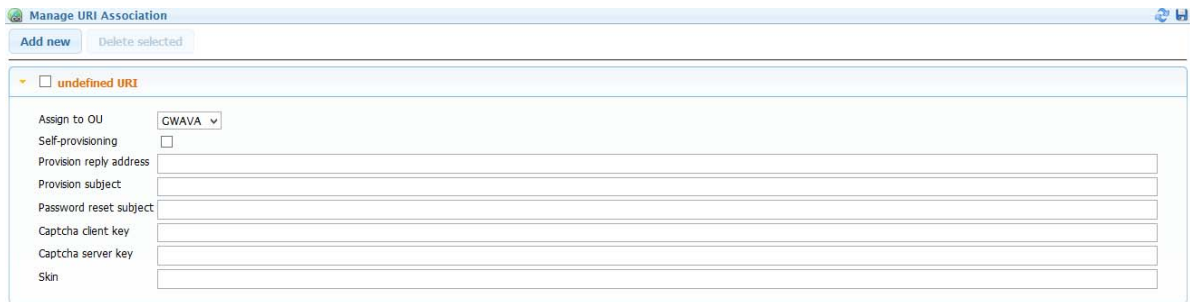


URI Association

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 OpenText 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

System Management

- Manage Servers
- Languages
- Templates
- User Interfaces
- URI Association
- Database Connections**
- File System Rights
- Password Control
- System Alerts
- Scanner Diagnostic
- Licensing
- Online Update

Module Management

Organization / Policy Management

Manage Database Connections

Add new **Delete selected** **Instructions**

☐ **Message Tracker**

Database content: Tracker
Database host server: 127.0.0.1
Database name: GWAVATRACKER
Database login name: postgres
Database login password:

☐ **Quarantine**

Database content: QMS
Database host server: 127.0.0.1
Database name: GWAVAQMS
Database login name: postgres
Database login password:

☐ **Statistics**

Database content: Stats
Database host server: 127.0.0.1
Database name: GWAVASTATS
Database login name: postgres
Database login password:

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

Tracker
[undefined]
QMS
Stats
Tracker

- ♦ 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

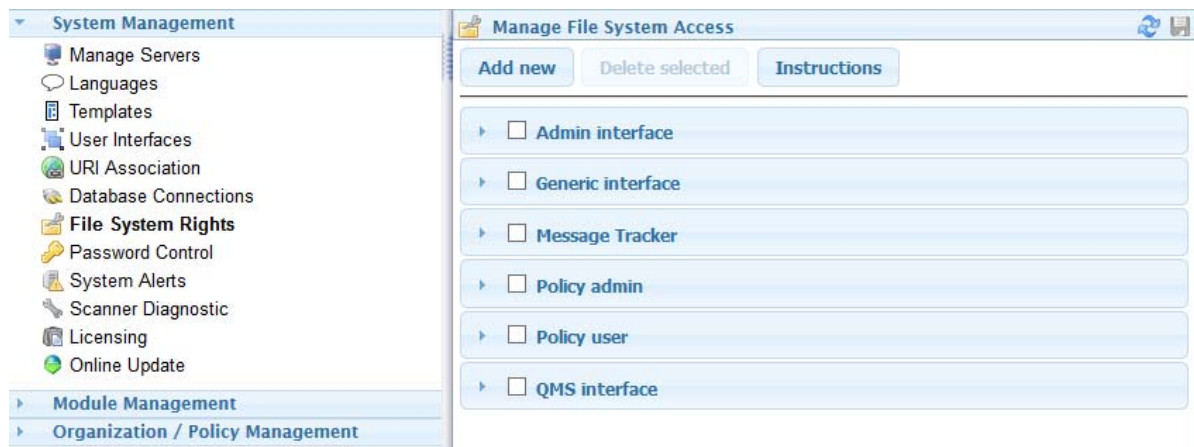
In OpenText Secure Messaging Gateway, roles define what abilities and rights any user has. The File Access Manager is the method by which the roles are fine tuned. File access determines which web pages any specific role can access.

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

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

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

File System Rights Interface



Admin interface

☐ **Admin interface**

Allow file path list

Deny file path list

Role Assignment

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

Generic interface

☐ **Generic interface**

Allow file path list

Deny file path list

Role Assignment

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

Message Tracker

Message Tracker

Allow file path list

/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

Allow file path list

/admin/contents/ou/policy/
/admin/contents/scanner/
/admin/navigation/

Deny file path list

Role Assignment

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

Policy user

☐ **Policy user**

Allow file path list

Deny file path list

Role Assignment

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

QMS interface

☐ **QMS interface**

Allow file path list

Deny file path list

Role Assignment

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

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

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

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

Message Tracker

OU Supervisor

Policy Administrator

Policy User

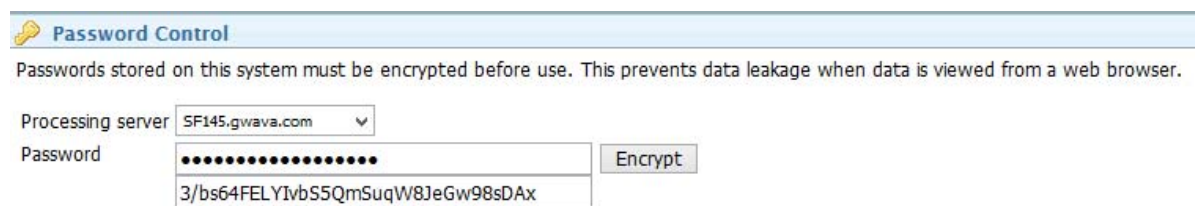
QMS Administrator

QMS User

System Administrator

Password Control

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



Password Control

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

Processing server: SF145.gwava.com

Password: **Encrypt**

3/bs64FELYIvbS5QmSuqW8JeGw98sDAX

Processing server: Which server will process the request

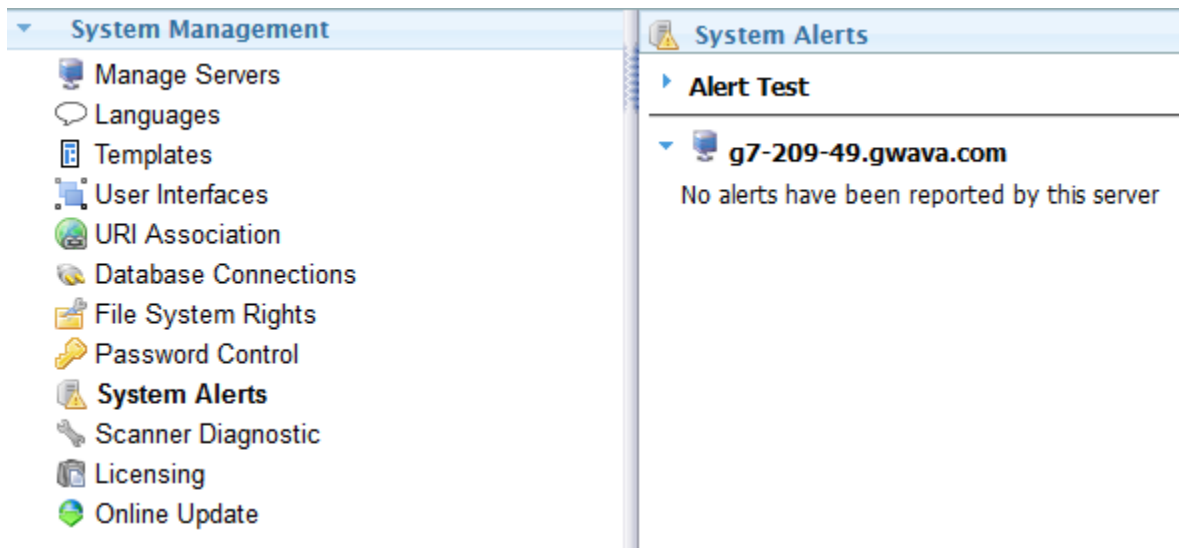
Encrypting an SMG Password:

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 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.

System Management

- Manage Servers
- Languages
- Templates
- User Interfaces
- URI Association
- Database Connections
- File System Rights
- Password Control
- System Alerts
- Scanner Diagnostic**
- Licensing
- Online Update

► **Module Management**

► **Organization / Policy Management**

Scan Diagnostics

Select the scan engine to process the message

Message filter engine ▼

Provide the message to be scanned

☒ Browse... No file selected.

☐ Paste MIME message

Date: Thu, 4 May 2017 12:47:20 -0600 (MDT)
 From: Example Sender <sender@example.com>
 To: Example Recipient <recipient@example.com>
 Subject: An example message
 Message-ID: <20170504124720.example@example.com>
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="-----7D285853744A42B2130FD624"

This is a multi-part message in MIME format.
 -----7D285853744A42B2130FD624

Add applicable message envelope information

Sender email address

Recipient email address(es)

Source IP address

Message direction

Interface type

Interface

Connection SSL secure ☐

Connection used STARTTLS ☐

Client authenticated ☐

Verbose response ☐

Show request ☐

Scan Message

Scan Results

Waiting for scan

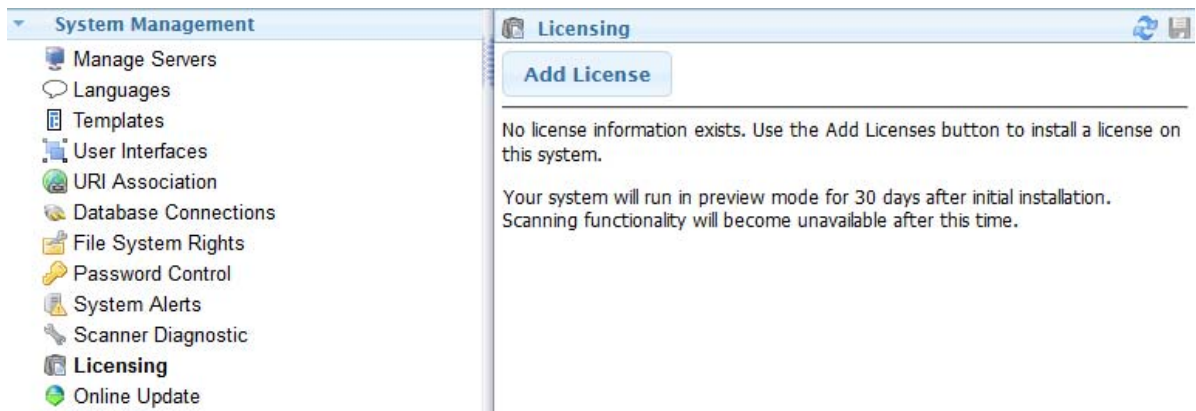
1. Select the scan engine to process the message: from the drop down menu.
2. Provide the message to be scanned: by browsing to and uploading the file.
3. Paste MIME message: paste the MIME.822 in the text box.
4. Add applicable message envelope information:
 - ◆ Sender email address
 - ◆ Recipient email 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 OpenText Secure Messaging Gateway is restarted.



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

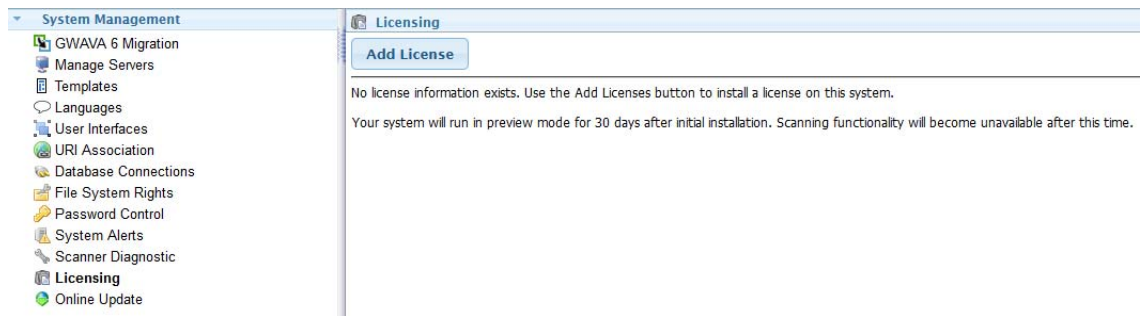
No license information exists. Use the **Add License** button to install a license on this system.

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

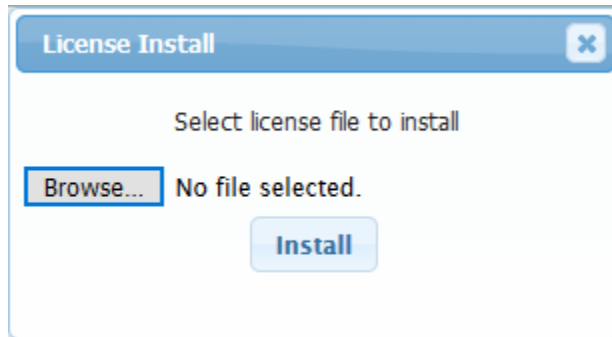
When your license is within 30 days of expiration reminder messages will be sent to the system administrator specified under **System Administration | Organization/Policy Management | Settings | Administrator email address**.

You will receive a Validation Key from OpenText Licensing.

1. Go to the Licensing portal.
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 it's 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.



7. Browse to the PEM file.

8. Press Install to upload the PEM file.

Online Updates

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

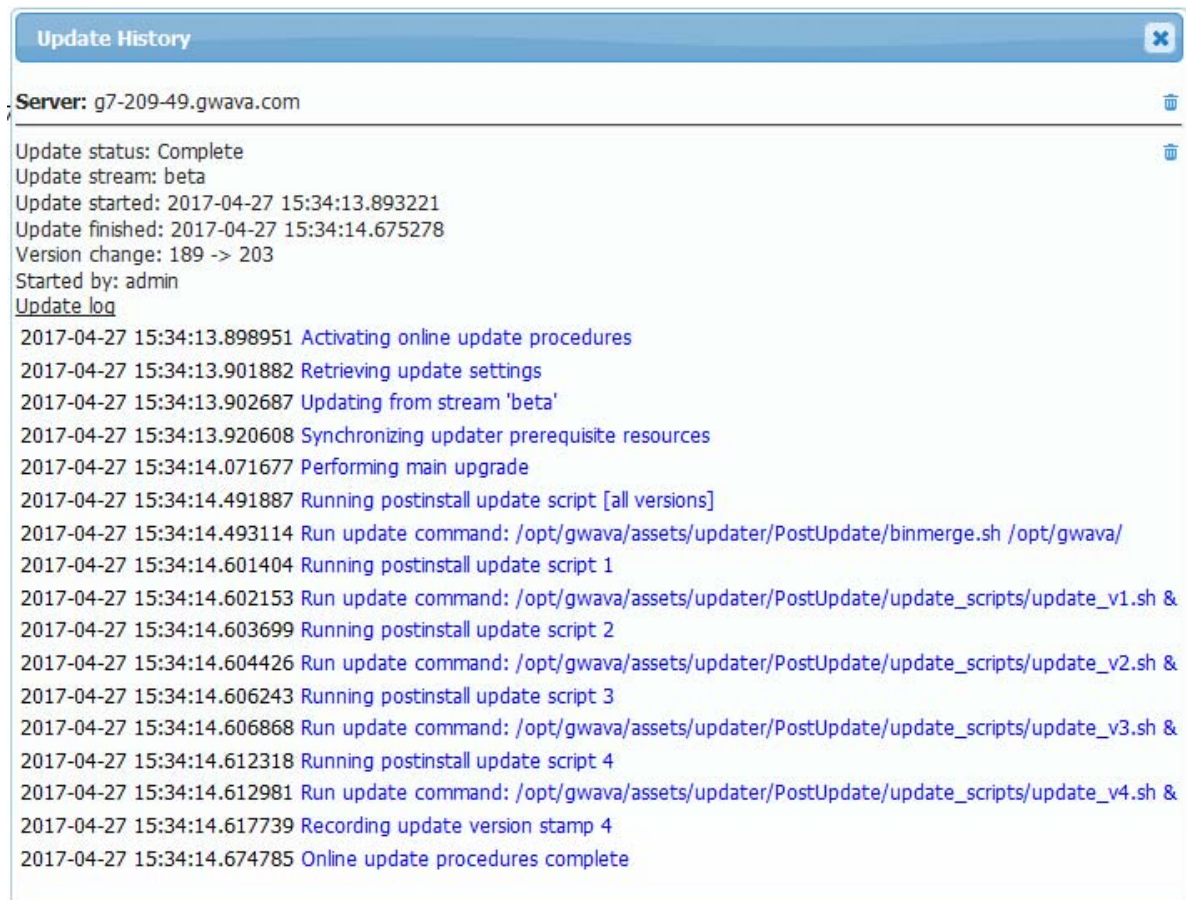
You may select an update stream of Release (recommended) or Beta (should only be used under Support's supervision). If you are on the beta stream, you can switch to the release stream when the release build is higher than the beta build. This is recommended to be done during the monthly release update 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 65 manually.

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



View Updates will show the versions installed on the server.



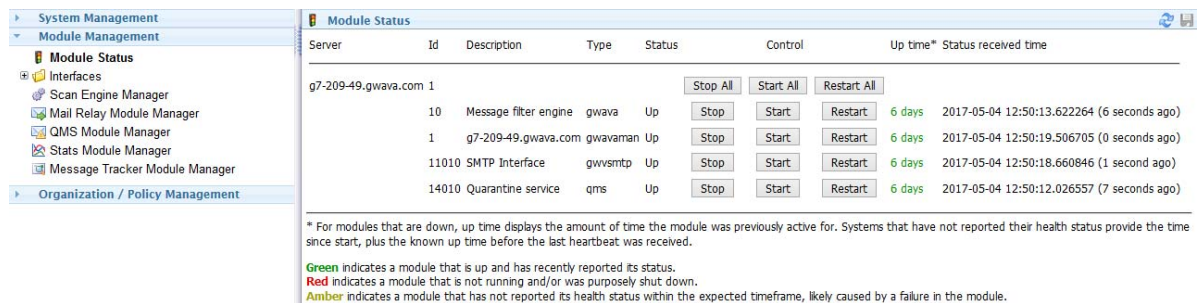
5 Module Administration

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.



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

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

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

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

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

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 OpenText 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.

Manage SMTP Interfaces

Add new

Delete selected

Instructions

Clone selected

☐

SMTP Interface

Host server

smg140.gwava.com

Stats module

Statistics engine

Serviced organizational unit (OU) set

☒ [root]

Scan failure action

Delay messages (451)

Notes

Server

External Delivery

SSL

Protocol

Exploit Detection

Relay/Host Protection

Connection Drop Services

Message Tracking Services

Denial Of Service Prevention

Scanner Fault Tolerance

Address Transformation

Dagnostic

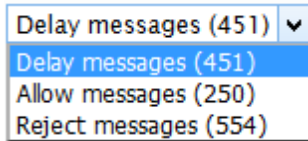
Create a new Interface by clicking *Add New*.

Host server: Select the host server

Stats module: Select the Statistics engine

Serviced OU set: Select the OU to service

Scan failure action: Select the action to take on failure:



Delay messages (451) ▼
Delay messages (451)
Allow messages (250)
Reject messages (554)

Delay messages (451)

Allow messages (250)

Reject messages (554)

License Failsafe mode: Select the action to take when a license issue occurs: Delay Messages (451), Allow Messages (250), or Reject Messages (554).

Notes: Enter notes about the module, if desired.

Server

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

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

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

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

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

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

External Delivery

Connection Security: Set the security protocol.

None (Default)

auto

tls

ssl

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

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

Relay targets:

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

Priority: Enter the priority, 1 is highest.

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

none

auto

tls

ssl

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

None
auto
plain
login
cram-md5

Username: Enter the SMTP relay username, if needed.

Password: Enter the SMTP relay password, if needed.

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

SSL

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 OpenText Secure Messaging Gateway server.

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

SSL key file: Enter the path to the file on the OpenText 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>.

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 OpenText Secure Messaging Gateway server.

Protocol

Enable inbound timeouts: Default enabled.

Client connection timeout (sec): Default 15 seconds.

Client protocol timeout (sec): Default 5 seconds.

Client DATA command timeout (sec): Default 10 seconds.

Client DATA payload timeout (sec): Default 10 seconds.

TLS negotiation timeout (sec): Default 15 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.

Server DATA 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.

Disable A-record fallback: Default disabled.

SMTP Authentication: Default disabled.

Enable SIZE limit: Default enabled.

SIZE limit (bytes): Default 40000000.

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 81](#).

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.

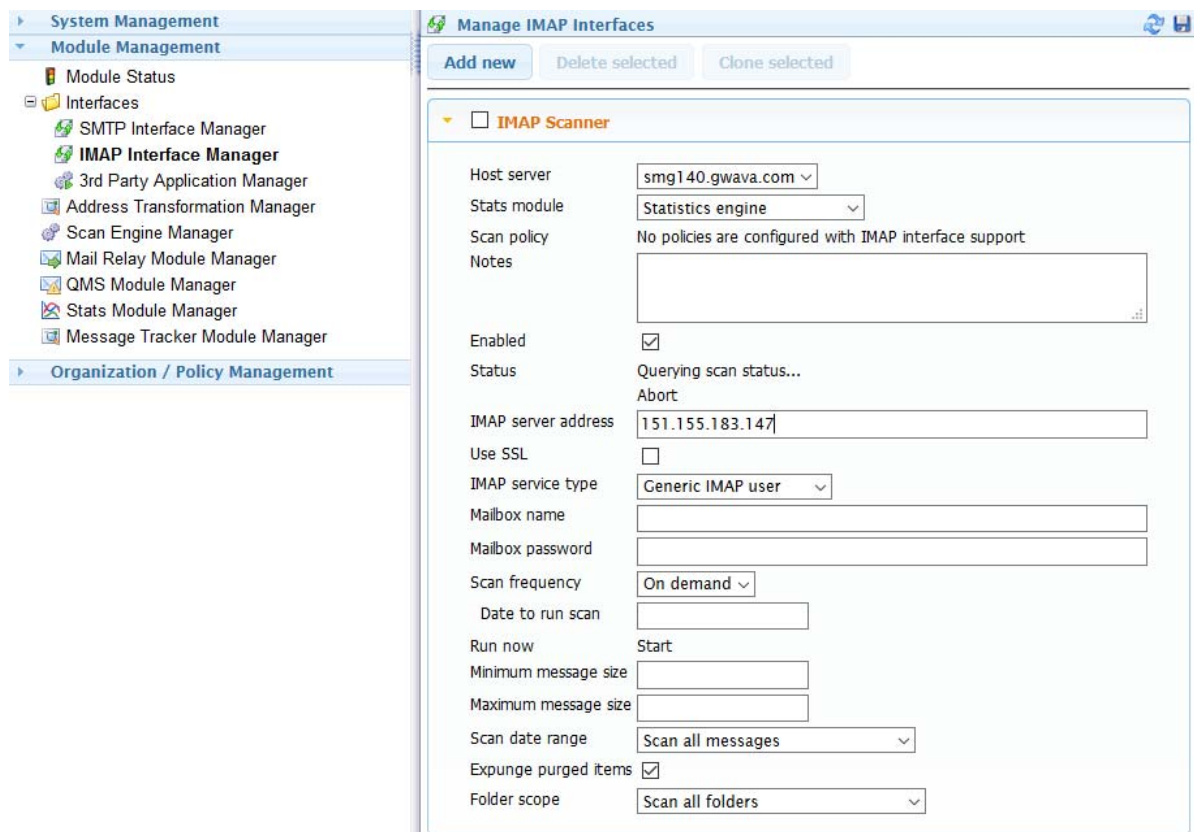
The issue would be that the GWIA requires an SMTP banner from SMG.

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

IMAP Interface

IMAP can be scanned by SMG.

IMAP Interface Manager



System Management

- Module Management**
 - Module Status
 - Interfaces
 - SMTP Interface Manager
 - IMAP Interface Manager**
 - 3rd Party Application Manager
 - Address Transformation Manager
 - Scan Engine Manager
 - Mail Relay Module Manager
 - QMS Module Manager
 - Stats Module Manager
 - Message Tracker Module Manager
- Organization / Policy Management**

Manage IMAP Interfaces

Add new Delete selected Clone selected

☐ **IMAP Scanner**

Host server smg140.gwava.com

Stats module Statistics engine

Scan policy No policies are configured with IMAP interface support

Notes

Enabled ☒

Status Querying scan status...
Abort

IMAP server address 151.155.183.147

Use SSL ☐

IMAP service type Generic IMAP user

Mailbox name

Mailbox password

Scan frequency On demand

Date to run scan

Run now Start

Minimum message size

Maximum message size

Scan date range Scan all messages

Expunge purged items ☒

Folder scope Scan all folders

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:

IMAP service type	Generic IMAP user ▾
Mailbox name	<input type="text"/>
Mailbox password	<input type="password"/>
Scan frequency	On demand ▾
Date to run scan	<input type="text"/>
Run now	Start
Minimum message size	<input type="text"/>
Maximum message size	<input type="text"/>
Scan date range	Scan all messages ▾
Expunge purged items	<input checked="" type="checkbox"/>
Folder scope	Scan all folders ▾

Mailbox name: User name of the generic IMAP user.

Mailbox password: Password of the generic IMAP user.

GroupWise Post Office:

IMAP service type	GroupWise Post Office ▾
Trusted application key	<input type="text"/>
Trusted application name	<input type="text"/>
Scan frequency	On demand ▾
Run now	Start
Minimum message size	<input type="text"/>
Maximum message size	<input type="text"/>
Scan date range	Scan all messages ▾
Scan users	<input checked="" type="checkbox"/>
Scan resources	<input checked="" type="checkbox"/>
Scan trash	<input checked="" type="checkbox"/>
Expunge purged items	<input checked="" type="checkbox"/>
User scope	Scan all users ▾
Folder scope	Scan all folders ▾

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.

The screenshot shows a configuration form for an 'Unnamed interface'. It includes a dropdown for 'Host server' (currently '[no server assigned]'), checkboxes for 'Require SSL connection' and 'Serviced OU set' (with a '[root]' dropdown), a text field for 'Allowed client addresses', and a 'Notes' text area. Below these is a section titled 'Scanner Fault Tolerance' which contains labels for 'Server address', 'Application key', 'Application type', and 'Client address'.

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**

Host server

smg-qa2.gwava.com ▼

Require SSL connection

☐

Serviced OU set

☒ [root]

Allowed client addresses

Notes

► **Scanner Fault Tolerance**

Server address

151.155.209.46

Application key

365c2949-0fb3-4d81-9dd2-421727bf08e3

Application type

gms

Client address

151.155.209.44

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.

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

The values are as follows:

```
<securegatewayEnable></securegatewayEnable>
```

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

0 - disabled.

```
<securegatewayHost></securegatewayHost>
```

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:

```
--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 72](#)

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.

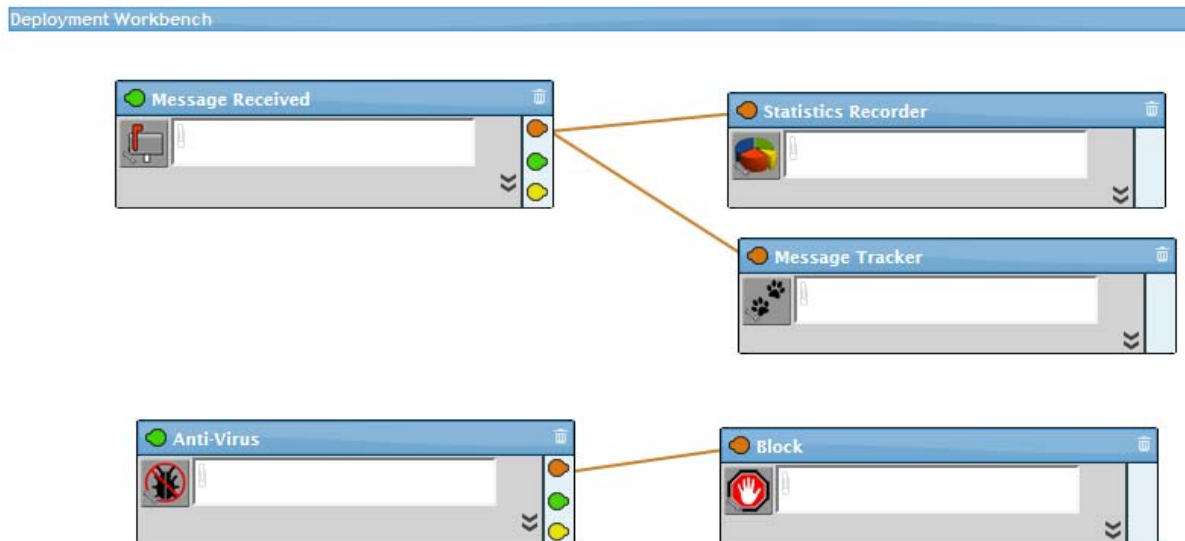
To enable the policy you must enable either "Limit by interface type", or enter IMAP into "Matched interface type", or both.

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

The screenshot shows the 'Address Transformation Manager' web interface. At the top, there are three buttons: 'Add new', 'Delete selected', and 'Instructions'. Below these is a dropdown menu showing 'gwava>microfocus'. The main configuration area includes several checkboxes: 'Enable rewrite rule' (checked), 'Notes' (with a text area), 'Serviced interfaces' (checked, with 'SMTP Interface' selected), 'Apply to inbound mail' (checked), 'Apply to outbound mail' (checked), 'Apply to sender' (checked), and 'Apply to recipient(s)' (checked). Below these is a section titled 'Rewrite rules' containing a table with two columns: 'Match pattern' and 'Replace pattern'. The first row shows a match pattern of '*@gwava.com' and a replace pattern of '\$1@microfocus.com'. There are also icons for deleting and favoriting rules.

Match pattern	Replace pattern
*@gwava.com	\$1@microfocus.com

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.

```
*      @      *      .      *  
[$1][$2][$3][$4][$5]
```

Save the changes.

Enable Address Transformation in the SMTP Interface ["SMTP Interface" on page 66](#), 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.

Micro Focus Secure Messaging Gateway

System Management

- Module Management
 - Module Status
 - Interfaces
 - Address Transformation Manager
 - Scan Engine Manager**
 - Mail Relay Module Manager
 - QMS Module Manager
 - Stats Module Manager
 - Message Tracker Module Manager
- Organization / Policy Management

Manage Scan Engines

Add new Delete selected Instructions

☐ **Message filter engine**

Notes

Enable REST Service ☒

Enable REST Service (SSL) ☐

Require client verification ☒

Restrict client addresses

Host server SMG-Primary

Connection address smg-227008

Bind address 0.0.0.0

Bind address SSL 0.0.0.0

SSL certificate file

SSL certificate chain file

SSL key file

SSL cipher list

SSL pass phrase

Fault tolerance priority 1

Multi-threaded scanning ☒

OpenDKIM services 127.0.0.1:4932

Serviced OU set ☒ [root]

Average message size (bytes) 4111 (past min)
[no data] (past hr)
[no data] (past 24hr)

Average scan time (seconds) 0 (past min)
[no data] (past hr)
[no data] (past 24hr)

Load Balancing

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

Fault Tolerance

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

Organizational Units

Scan engines may be created to service specific organization units. A new organization [“Manage Organizations” on page 104](#) 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.

Enable REST Service (SSL): Enable this option to set the REST service to use SSL. Selecting this option disables the **Enable REST Service** option and the **Bind address** and enables the **Bind address SSL** option.

Require client verification: Prevents the smg-scanner process from being accessed by external requests. This option is generally only used for troubleshooting purposes and should be left on.

Restrict client addresses: Add addresses to limit access to the smg-scanner service to only the listed addresses. You can add addresses as text patterns or as IP addresses in CIDR format.

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.

Bind address SSL: Default 0.0.0.0. This option is used if you have the **Enable REST Service (SSL)** option enabled.

Fault tolerance priority: Default 1. 1 is highest.

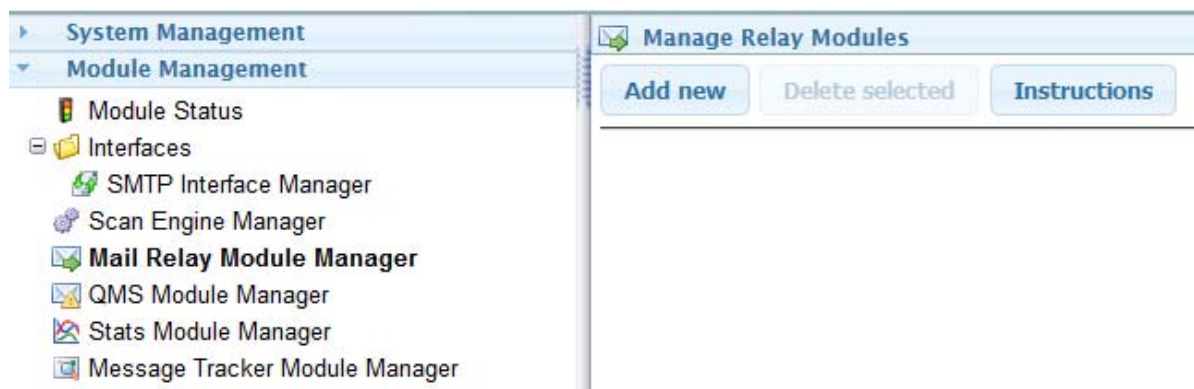
Multi-threaded scanning: Default enabled.

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

OpenText 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 OpenText 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.

Relay Service

Send test message

Message test

Host server

209-49.gwava.com

Message queue location

gwvrelay/queue_21010/

Maximum SMTP threads

32

Retry count

8

Retry interval

900

Delivery targets

☒ Defined domains

☒ Relay targets

☐ MX targets

SMTP Relay Target List

Host Address	Auth	Auth Username	Auth Password	Security	Priority
<div><div></div>151.155.209.48</div>	none			none	1
<div></div>	none			none	1

Send test message: Click button to send test message.

Mail Relay Test Message

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

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

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

Sender address

Recipient address

Send

Cancel

Host server: Select the server to host the module.

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

Maximum SMTP threads: Default 32.

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

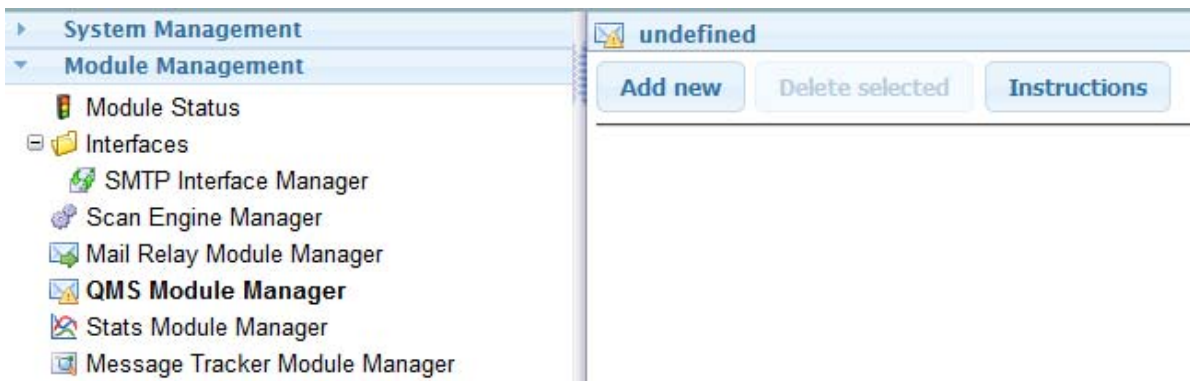
tls

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 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 OpenText 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.

6 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 157

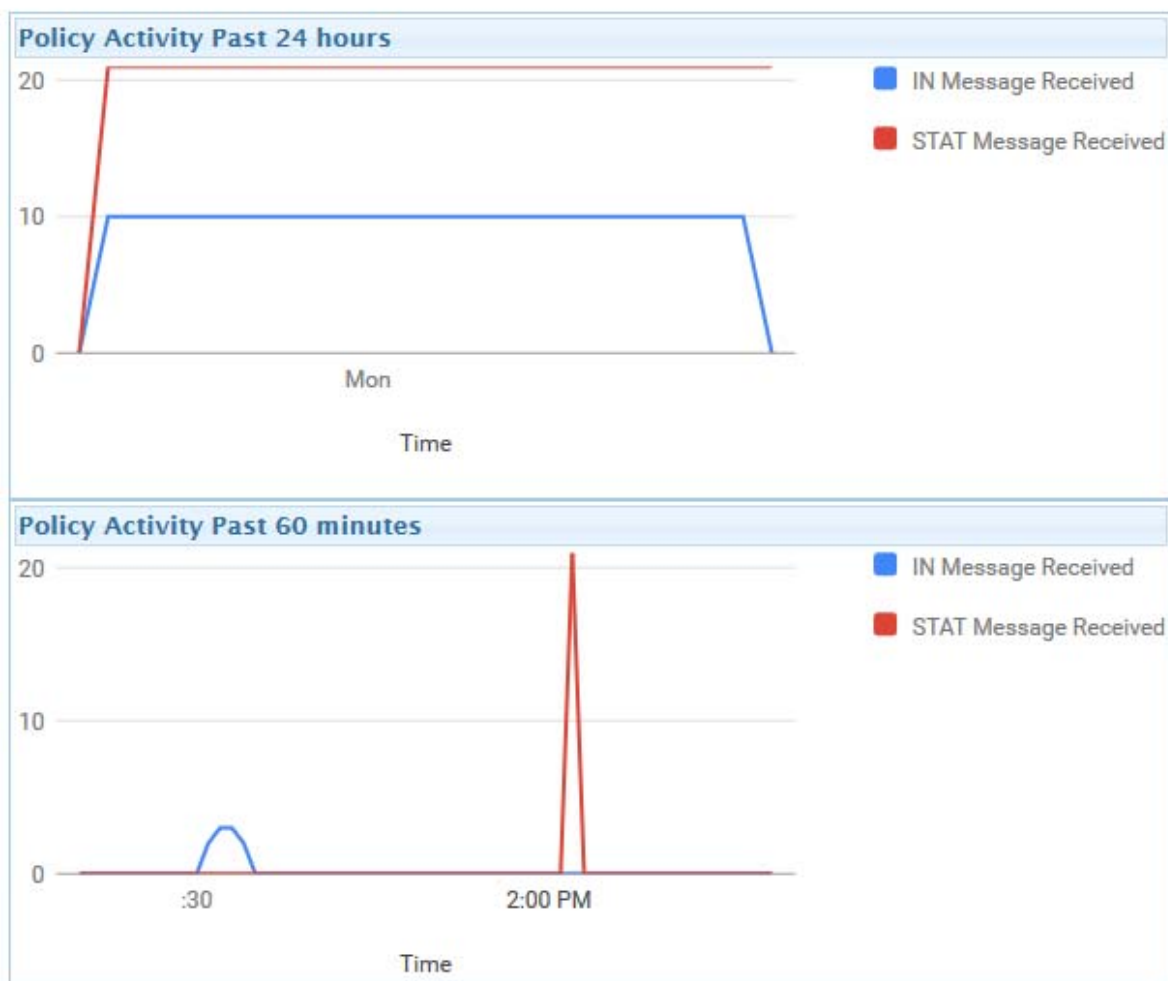
Organization / Policy Management Overview

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 157), 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.

System Management	Organization Settings
Module Management	Administrator email address <input type="text"/>
Organization / Policy Management	New child OU template <input type="text" value="[no template]"/>
Overview	Message tracking data retention days <input type="text" value="30"/>
Settings	Attached interfaces SMTP Interface
Manage Users	Attached scan engines Message filter engine
Manage System Roles	Attached statistics service Statistics engine
Manage Custom Roles	Attached quarantine service Quarantine service
Manage Organizations	Account details are not configured for this organizational unit
Domain Management	
Policy Management	
Policy scan configuration	

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.

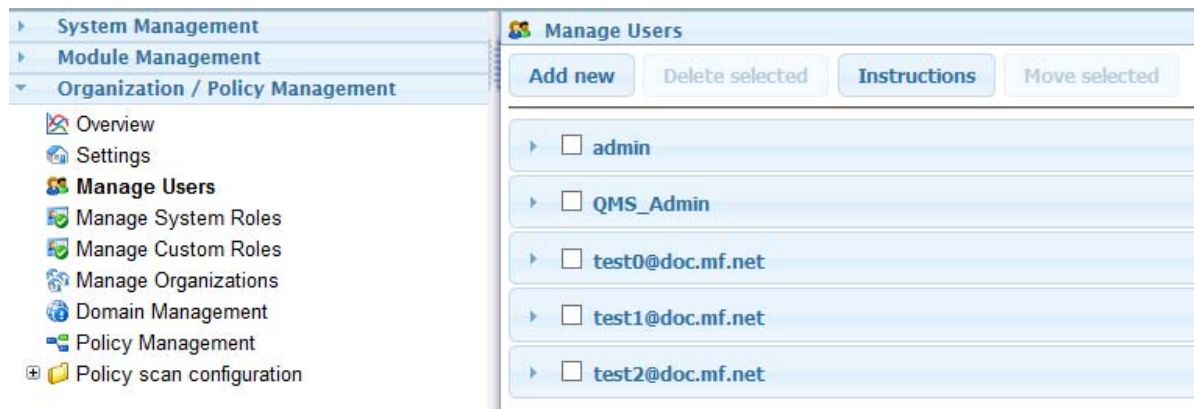
Attached statistics service: The statistics service attached to this organization.

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 populate with users that have logged into their quarantine. These users can also be granted additional rights called Roles.



Role membership defines what a User is allowed to do. For example, a user can be granted the role **QMS Administrator** to manage the quarantine to help the system administrator.

The following image shows a user and the settings that are available for users:

The screenshot shows a web interface titled "Manage Users". At the top, there are four buttons: "Add new", "Delete selected", "Instructions", and "Move selected". Below these buttons, there is a list of users. The first user is "admin" with a checkbox. The second user is "jdoe@acme.com" with a checkbox. The "jdoe@acme.com" user is selected, and its settings are displayed below. The settings include: "Last login" (Tue, 13 Jun 2017 15:55:07 -0600 from 137.65.60.85), "Enabled" (checked), "Management" (System), "Enable for SMTP AUTH" (checked), "Password" (empty field), and "Contact email" (empty field). Below the settings, there is a section titled "Role Membership" with a list of roles: Message Tracker, OU Supervisor, Policy Administrator, Policy User, QMS Administrator, QMS User, and System Administrator. Each role has a checkbox next to it.

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

Enabled: Login for this user can be disabled. It is enabled by default.

Management: Set the level the user can manage: **System** or **Domain Provisioning**. **System** is the default.

Enable for SMTP AUTH: If SMTP authentication is enabled for an SMTP interface, you can enable this user to be used for SMTP authentication. Enabling a user for SMTP authentication means that user's credentials can be used to lookup SMG accounts for authentication.

IMPORTANT: The user must have the **Management** option set to **System** for SMTP authentication. If it is set to **Domain Provisioning**, the user is authenticated against the email server that owns the email address instead of SMG.

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.

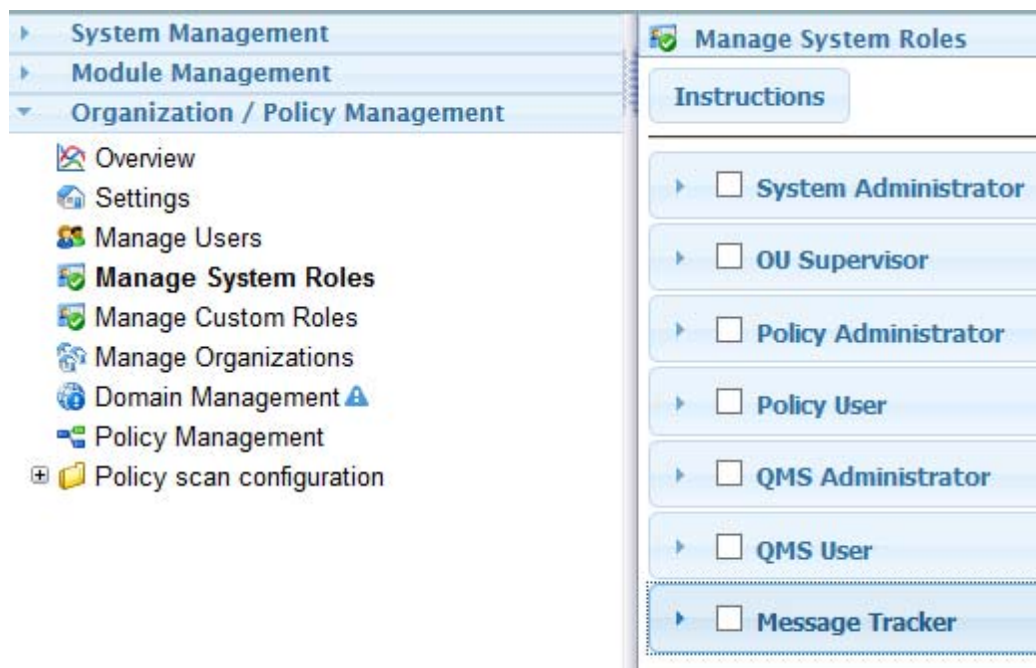
Manage System roles

Roles provide access to features of the OpenText 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 OpenText 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:

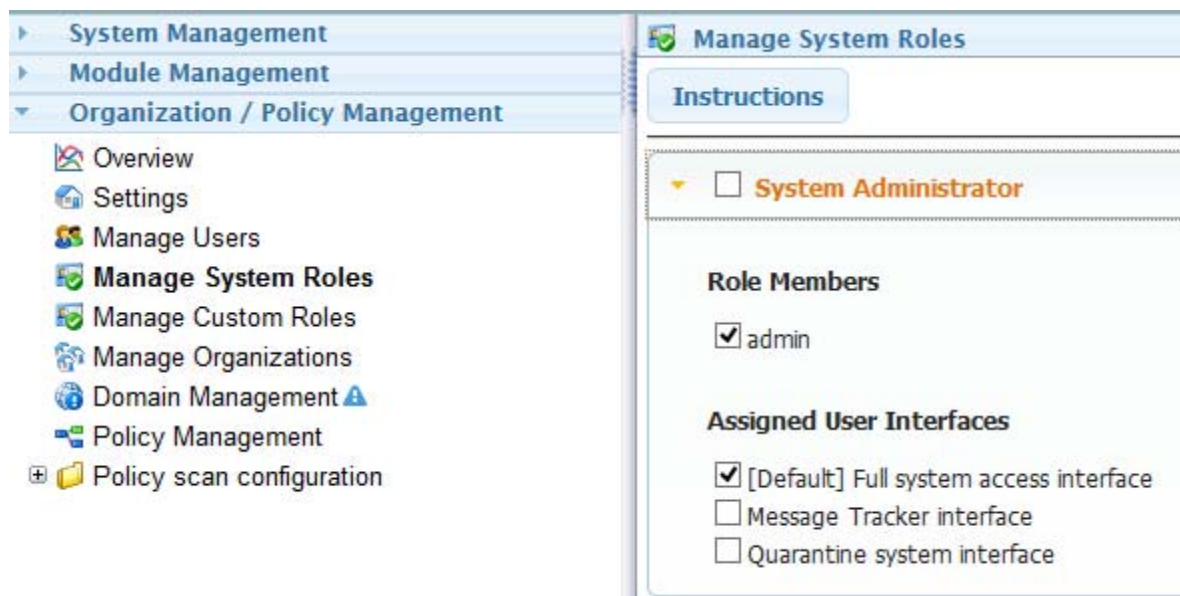
- ♦ System Administrator
- ♦ OU Supervisor
- ♦ Policy Administrator
- ♦ Policy User
- ♦ QMS Administrator
- ♦ QMS User
- ♦ Message Tracker

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

The screenshot displays the 'Manage System Roles' window. On the left, a navigation pane shows a tree structure with 'Organization / Policy Management' expanded, listing options like Overview, Settings, Manage Users, Manage System Roles, Manage Custom Roles, Manage Organizations, Domain Management, Policy Management, and Policy scan configuration. The main panel is titled 'Manage System Roles' and includes an 'Instructions' button. Below this, there are three role entries: 'System Administrator' (disabled), 'OU Supervisor' (selected and highlighted in orange), and 'Policy Administrator' (disabled). The 'OU Supervisor' role is expanded to show its configuration. Under 'Role Members', the 'admin' user is listed with an unchecked checkbox. Under 'Assigned User Interfaces', three options are shown: '[Default] Full system access interface' (checked), 'Message Tracker interface' (unchecked), and 'Quarantine system interface' (unchecked).

System Management

Module Management

Organization / Policy Management

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

Manage System Roles

Instructions

- ☐ System Administrator
- ☒ **OU Supervisor**
- ☐ Policy Administrator

Role Members

- ☐ admin

Assigned User Interfaces

- ☒ [Default] Full system access interface
- ☐ Message Tracker interface
- ☐ Quarantine system interface

Policy Administrator

This screenshot is similar to the one above, showing the 'Manage System Roles' window. The navigation pane on the left is identical. In the main panel, the 'Policy Administrator' role is now selected and highlighted in orange, while 'OU Supervisor' is no longer highlighted. The 'Policy Administrator' role is expanded to show its configuration. Under 'Role Members', the 'admin' user is listed with an unchecked checkbox. Under 'Assigned User Interfaces', the same three options are shown: '[Default] Full system access interface' (checked), 'Message Tracker interface' (unchecked), and 'Quarantine system interface' (unchecked).

System Management

Module Management

Organization / Policy Management

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

Manage System Roles

Instructions

- ☐ System Administrator
- ☐ OU Supervisor
- ☒ **Policy Administrator**

Role Members

- ☐ admin

Assigned User Interfaces

- ☒ [Default] Full system access interface
- ☐ Message Tracker interface
- ☐ Quarantine system interface

Policy User

The screenshot displays a web-based management interface. On the left is a navigation pane with a tree structure. The main area on the right is titled 'Manage System Roles' and contains a list of roles with checkboxes, a section for role members, and a section for assigned user interfaces.

Navigation Pane:

- System Management
- Module Management
- Organization / Policy Management
 - Overview
 - Settings
 - Manage Users
 - Manage System Roles**
 - Manage Custom Roles
 - Manage Organizations
 - Domain Management ⚠
 - Policy Management
 - Policy scan configuration

Manage System Roles Panel:

Instructions

- ☐ System Administrator
- ☐ OU Supervisor
- ☐ Policy Administrator
- ☐ **Policy User**

Role Members

- ☐ admin

Assigned User Interfaces

- ☒ [Default] Full system access interface
- ☐ Message Tracker interface
- ☐ Quarantine system interface

QMS Administrator

The screenshot displays the 'Manage System Roles' configuration page in the QMS Administrator. The left sidebar contains a navigation menu with the following items: System Management, Module Management, Organization / Policy Management (expanded), Overview, Settings, Manage Users, Manage System Roles (highlighted), Manage Custom Roles, Manage Organizations, Domain Management (with a warning icon), Policy Management, and Policy scan configuration (with a plus icon). The main content area is titled 'Manage System Roles' and includes an 'Instructions' button. Below this, there is a list of roles with checkboxes: System Administrator, OU Supervisor, Policy Administrator, Policy User, and QMS Administrator (highlighted in orange). Under the 'QMS Administrator' role, there are two sections: 'Role Members' with a checked checkbox for 'admin', and 'Assigned User Interfaces' with checkboxes for '[Default] Full system access interface', 'Message Tracker interface', and 'Quarantine system interface' (checked).

System Management

Module Management

Organization / Policy Management

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

Manage System Roles

Instructions

- ☐ System Administrator
- ☐ OU Supervisor
- ☐ Policy Administrator
- ☐ Policy User
- ☒ **QMS Administrator**

Role Members

- ☒ admin

Assigned User Interfaces

- ☐ [Default] Full system access interface
- ☐ Message Tracker interface
- ☒ Quarantine system interface

QMS User

The screenshot displays a web-based interface for managing system roles. On the left is a navigation pane with a tree structure. The main area on the right is titled 'Manage System Roles' and contains a list of roles with checkboxes, a section for role members, and a section for assigned user interfaces.

Navigation Pane:

- System Management
- Module Management
- Organization / Policy Management
 - Overview
 - Settings
 - Manage Users
 - Manage System Roles**
 - Manage Custom Roles
 - Manage Organizations
 - Domain Management
 - Policy Management
 - Policy scan configuration

Manage System Roles Panel:

Instructions

- ☐ System Administrator
- ☐ OU Supervisor
- ☐ Policy Administrator
- ☐ Policy User
- ☐ QMS Administrator
- ☒ **QMS User**

Role Members

- ☐ admin

Assigned User Interfaces

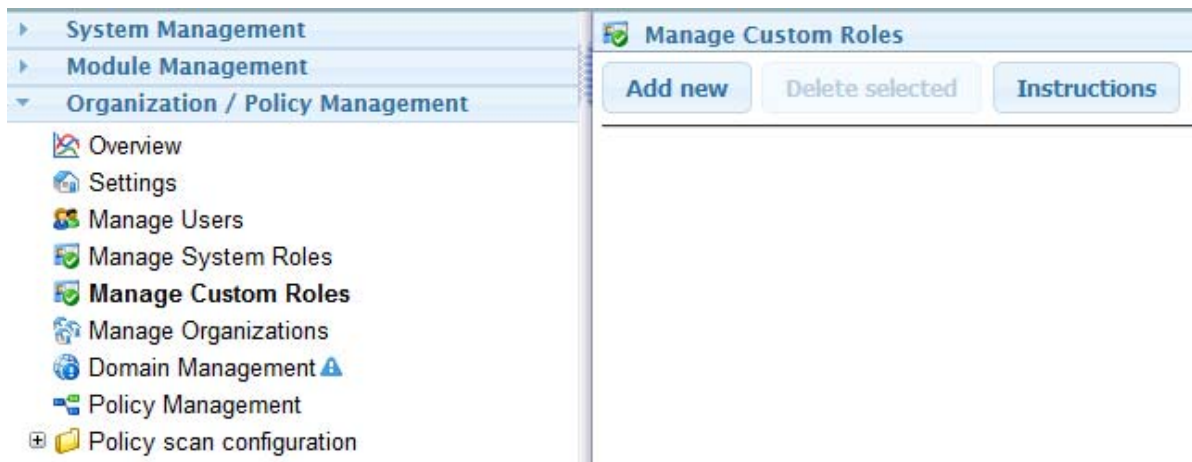
- ☐ [Default] Full system access interface
- ☐ Message Tracker interface
- ☒ Quarantine system interface

Message Tracker

The screenshot displays the 'Manage System Roles' interface. On the left, the navigation pane includes 'System Management', 'Module Management', and 'Organization / Policy Management'. Under 'Organization / Policy Management', options like 'Overview', 'Settings', 'Manage Users', 'Manage System Roles' (selected), 'Manage Custom Roles', 'Manage Organizations', 'Domain Management', 'Policy Management', and 'Policy scan configuration' are listed. The main content area is titled 'Manage System Roles' and contains an 'Instructions' tab. Below this, a list of roles is shown with checkboxes: 'System Administrator', 'OU Supervisor', 'Policy Administrator', 'Policy User', 'QMS Administrator', 'QMS User', and 'Message Tracker' (highlighted in orange). Under the 'Message Tracker' role, the 'Role Members' section shows 'admin' with a checked checkbox. The 'Assigned User Interfaces' section includes three options: '[Default] Full system access interface' (unchecked), 'Message Tracker interface' (checked), and 'Quarantine system interface' (unchecked).

Manage Custom Roles

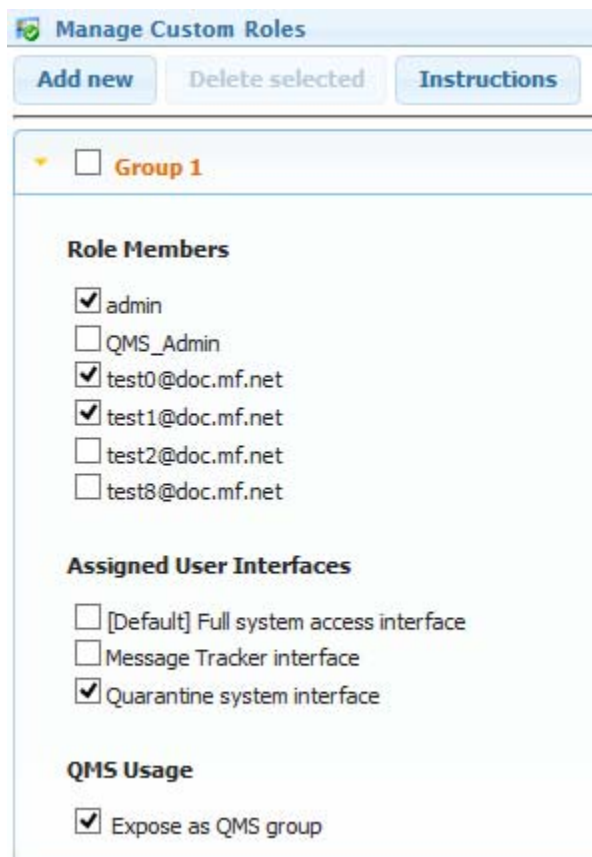
Roles provide access to features of the OpenText Secure Messaging Gateway system to users, and controls the actions of role dependent features found throughout the system. Custom roles allow creation of customized roles at any level in the OpenText Secure Messaging Gateway OU system. Roles created at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



Create Custom Role

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

Roles can be renamed by clicking on the role name.



Role Members

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

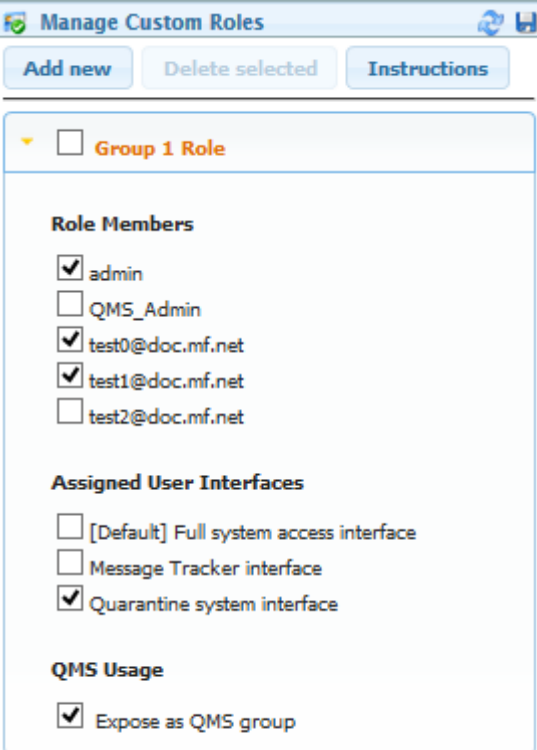
Assigned User Interfaces

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

Creating a Group

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

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



The screenshot shows a web application window titled "Manage Custom Roles". At the top, there are three buttons: "Add new", "Delete selected", and "Instructions". Below these buttons is a section for "Group 1 Role". This section contains three sub-sections: "Role Members", "Assigned User Interfaces", and "QMS Usage".

Role Members
<input checked="" type="checkbox"/> admin
<input type="checkbox"/> QMS_Admin
<input checked="" type="checkbox"/> test0@doc.mf.net
<input checked="" type="checkbox"/> test1@doc.mf.net
<input type="checkbox"/> test2@doc.mf.net

Assigned User Interfaces
<input type="checkbox"/> [Default] Full system access interface
<input type="checkbox"/> Message Tracker interface
<input checked="" type="checkbox"/> Quarantine system interface

QMS Usage
<input checked="" type="checkbox"/> Expose as QMS group

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.

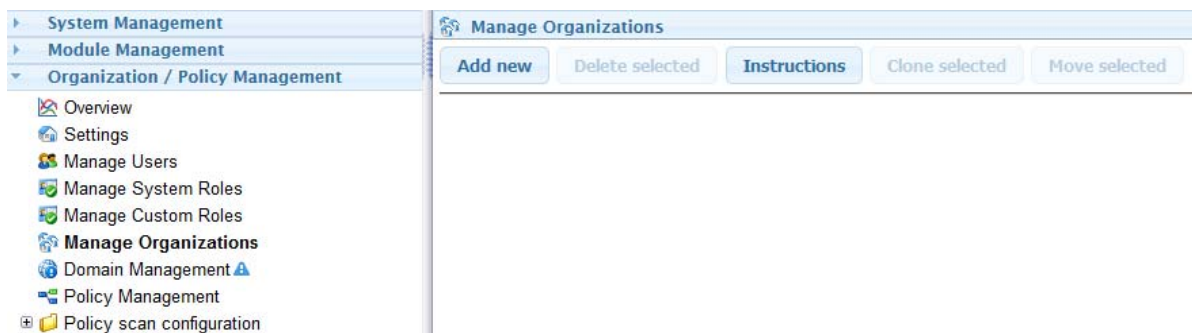
Make sure that new users are automatically added to the group by enabling Domain Management | <domain> | Auto-provision roles | QMS User.

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

 **Manage Organizations**

Add newDelete selectedInstructionsClone selectedMove selected

▼ ☐ **Unnamed organization**

Enabled☒

Expires☐

Expiry date

Enable user limit☐

User limit

Force address tracking☐

Require domain in username☐

Allow domain patterns☒

Require domain validation☐

Maximum child OU's

Maximum child OU depth

User interface

Default child user interface

► **Role Availability**

► **Event Availability**

► **Service Availability**

► **Exception Availability**

► **Template Availability**

► **User Interface Availability**

Enabled: Default, enabled.

Expires: Default, disabled.

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

Enable user limit: Default, disabled.

User limit: Limit number of users. Default 1.

Force address tracking: Default, disabled.

Require domain in username: Default, disabled.

Allow domain patterns: Default, enabled.

Require domain validation: Default, disabled.

Maximum child 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

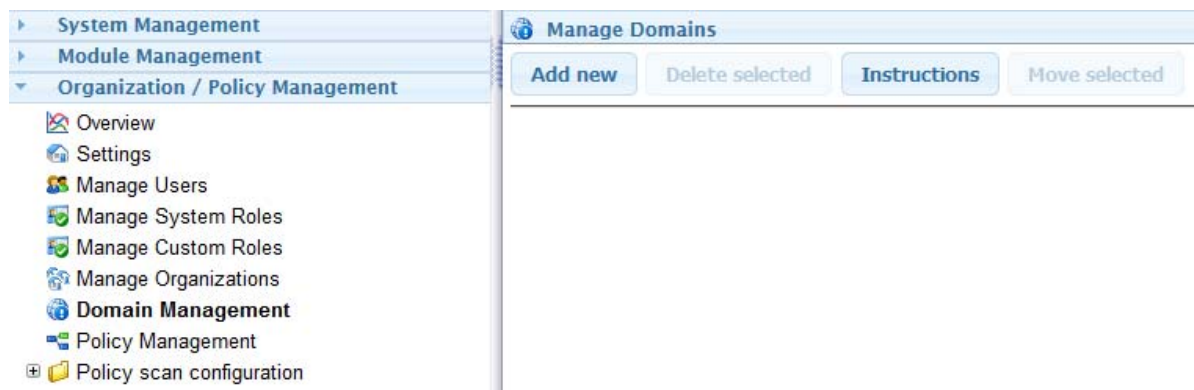
User Interface Availability

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

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



Adding domains to the OpenText 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 need at least one domain. This should be named after the fully qualified domain name of your email server.

You also need to set up what users can connect and what SMTP server the domain should connect to. You may also enter details for connecting to LDAP for user authentication and DKIM signing.

The screenshot shows the configuration page for a new domain named 'acme.com'. The interface includes several sections for setting up domain policies and connections.

- Enable user auto-provisioning:** A checkbox that is currently unchecked.
- Auto-provision roles:** A list of roles with checkboxes: System Administrator, OU Supervisor, Policy Administrator, Policy User, QMS Administrator, QMS User, and Message Tracker. All are currently unchecked.
- Require inbound SMTP domain authentication:** A checkbox that is checked.
- Require SMTP sending domain authentication:** A checkbox that is unchecked.
- SMTP authentication exception mode:** A dropdown menu set to 'Allow'.
- SMTP authentication exceptions:** A text input field containing '10.10.10.1'.
- Additional Host Pattern Matches:** An empty text input field.
- SMTP Hosts:** A table with columns: Target host, Priority, Security, Authentication Username, Password, Mail Auth, and Line limit. One entry is shown with Priority '1', Security 'none', and Line limit '1000'.
- LDAP Hosts:** A table with columns: Target host, Priority, Security, Username, Password, Auth, Validate, Scope, DN template / DN search base, and Search pattern. One entry is shown with Priority '1', Security 'none', and Scope 'template'.
- DKIM Signing:** A table with columns: Domain and Selector. One entry is shown with Domain '20210415'.
- Notes:** An empty text input field.

- ♦ **Enable user auto-provisioning:** This is disabled by default.
- ♦ **Auto-provision roles:** If auto-provisioning is enabled on the domain, you can specify which roles are given to auto-provision users: System Administrator, OU Supervisor, Policy Administrator, Policy User, QMS Administrator, QMS User, Message Tracker. For more information about roles, see [“Manage System roles” on page 95](#).
- ♦ **Require inbound SMTP domain authentication:** Requires inbound SMTP authentication to the domain. Only users with SMTP AUTH enabled can authenticate.
- ♦ **Require SMTP sending domain authentication:** Requires outbound SMTP authentication from the domain. Only users with SMTP AUTH enabled can authenticate.
- ♦ **SMTP authentication exception mode:** Specify whether listed SMTP AUTH exceptions are allowed or denied.

- ♦ **SMTP authentication exceptions:** Specify the IP addresses for client that are exempted from any enforcement settings for SMTP AUTH and can send messages without being authenticated. IP addresses can be entered as string/regex patterns or in CIDR format.

NOTE: A client whose IP address is in the list is not considered authenticated unless they choose to authenticate. This is important to consider when using the SMTP Envelope filter in a scan policy (which has the option to test whether the client is authenticated).

- ♦ **Additional Host Pattern Matches:** Enter the IP address range or host names with wildcards of appropriate hosts.

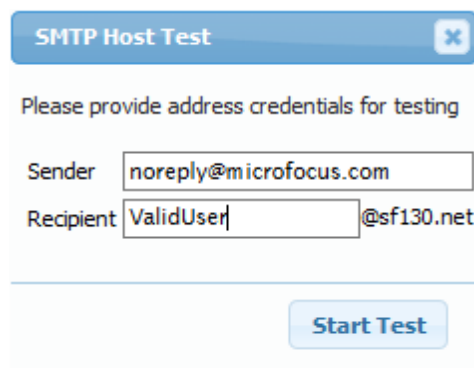
SMTP Hosts

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”



The image shows a dialog box titled "SMTP Host Test" with a close button (X) in the top right corner. Below the title bar, the text "Please provide address credentials for testing" is displayed. There are two input fields: "Sender" with the value "noreply@microfocus.com" and "Recipient" with the value "ValidUser@sf130.net". At the bottom of the dialog box, there is a blue button labeled "Start Test".

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

Test Results

Interface:

SMTP Interface

Test status:

test complete

Test result:

success 

Transaction log:

info : Connection to host 151.155.211.130 successful
recv : 220 GW130.DOC.MF.NET GroupWise Internet Agent 14.2.0 Copyright (c) 1993-2015 Novell, Inc. All rights reserved. Ready
send : EHLO microfocus.com
recv : 250-GW130.DOC.MF.NET
recv : 250-AUTH LOGIN
recv : 250-8BITMIME
recv : 250-SIZE
recv : 250-DSN
recv : 250 STARTTLS
send : MAIL FROM:<noreply@microfocus.com>
recv : 250 Ok
send : RCPT TO:<test1@SF.DOC.MF.NET>
recv : 250 Ok

or failed.

Test Results


Interface:

SMTP Interface

Test status:

test complete

Test result:

fail 

Transaction log:

info : Connection to host 151.155.211.130 successful
recv : 220 GW130.DOC.MF.NET GroupWise Internet Agent 14.2.0 Copyright (c) 1993-2015 Novell, Inc. All rights reserved. Ready
send : EHLO microfocus.com
recv : 250-GW130.DOC.MF.NET
recv : 250-AUTH LOGIN
recv : 250-8BITMIME
recv : 250-SIZE
recv : 250-DSN
recv : 250 STARTTLS
send : STARTTLS
recv : 220 Ready to start TLS
info : STARTTLS switched into encrypted mode successfully
send : EHLO microfocus.com
recv : 250-GW130.DOC.MF.NET
recv : 250-AUTH LOGIN
recv : 250-8BITMIME
recv : 250-SIZE
recv : 250 DSN
Error : Authentication failed: 501 Authentication failed

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%))

LDAP Hosts

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

DKIM Signing

DKIM Signing

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

- ♦ 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.

DKIM Public Key

The public key is provided in a format suitable for inclusion in DNS configuration files. If your DNS is hosted by a 3rd party, you should create a TXT record for your domain and copy the data portion of the record, removing quotes and spacing within the base64 portion of the data.

```

20171003._domainkey IN TXT ( "v=DKIM1; k=rsa; s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsBgKRxlt5FsetvBRRsHN9GUtyiibmbfNwhlw
qrtAY/O3Nv8Al2E8FFqb9doztZ/ktU155ZGoRX
/TpMrWInhD47qXVf7z6Wz8tZsIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69Glop
/HkeWyStjkk7nVHRXDprUY1/0XSuHFGID1BK+Ci3yMN98qRcFzWS+kyWj"
"q44Gt79XZ0h/qv1ESLo4SGdNQtb0VxwGFJ6kp01LP2EJBqiBaWtYOAxrz9Kf2hvVCF6uhRV4iyzd5c9Irw
edkIx7QyYdGu7cI+blh9bVd6VxuzX7gxxV722iYewAlh5iJBAAd7jwIDAQAB" ) ; ----- DKIM key
20171003 for doc.mf.net

```

- Create Keys button: This button will create a set of private and public keys for DKIM signing.
- Upload Keys button: If you already have keys you wish to use, they can be uploaded here. A dialog box will appear.

DKIM Key Upload

Private Key

Public Key DNS record

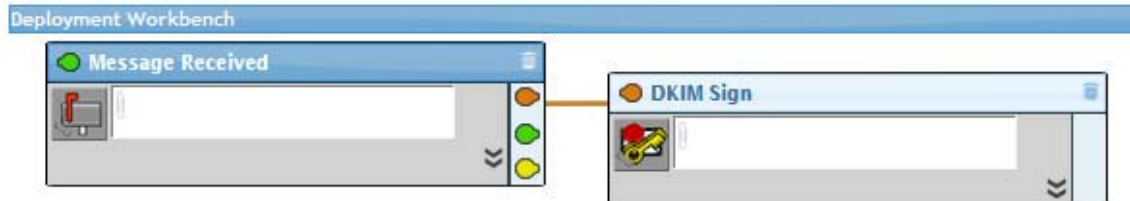
Upload

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*.

- 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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsBgKRxlt5FsetvBRRsHN9GUtyiibmbfNwhlwqrtAY/O3Nv8AlZE8FFqb9doztZ/ktU155ZGoRX/TpMrWInhD47qXVf7z6Wz8tZsIF5w0uvJcWXOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69Glop/HkeWyStjkk7nVHRXDprUY1/0XSuhFGTD1BK+Ci3yMN98qRcFzWS+kyWj" "g44Gt79XZOh/qv1ESLo4SGdNQtb0VxwGFJ6kp0lLP2EJBqiBaWtYOArxz9Kf2hvVCF6uhRV4iyzd5o9IrwedkIx7QyYdGu7cI+blh9bVd6VxuzX7gxxV722iYewAlh5iJBAA7jwIDAQAB"
- Finally, you need to create a DKIM signing service in Secure Messaging Gateway, either in an existing policy or in its own policy.



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

Notes

Enter any notes about the domain.

Policy Management

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



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

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

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

Set the Policy Priority

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

The policy used to scan a message is selected by comparing the qualifications of each of the policies in the list, in the order displayed, from top to bottom. Qualifications are conditions of the policy such as message direction, type of interface, etc. as shown below in the Manual Policy Creation section. The selected policy, and only that policy, is then used to perform the message scan. This trickle down selection is typically used to separate completely different rule sets for different classes of email. For example, inbound and outbound mail will generally have very different filtering requirements. Creating a policy for each direction, and defining the policy qualification based on message direction allows for independent configurations for the direction mail is flowing. You might also, for example, want messages from a specific IP address to completely bypass all of the rules. This would be possible by creating a policy at the top of the stack, qualified by IP address.

For the purpose of understanding, it is helpful to consider each policy as a single, complete and stand alone message filter. This means that messages do not, and can not, be scanned by multiple policies. The logic for testing a message with multiple filters, deciding what to do with the outcome of filtering and applying exceptions is all encapsulated within the individual policy. Any and all logic for scanning a class of message, i.e. inbound or outbound, must exist within the policy itself. Easy ways to understand why multiple policies are not applied is to consider what happens if the result of two policies are conflicted. If policy A would block a message but policy B would allow a message, the outcome is undecided. If policy A would block an IP address and policy B would have an exception for the same IP address, the outcome is undecided. If policy A would send a message to quarantine and policy B would block a message from being quarantined, the outcome is undecided. All of these logic decisions are accommodated within each individual policy, so that's where these types of configurations are intended to be managed.

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 by selecting items more options are revealed.

☐ **Mail Filter Policy**

Enabled

☒

Bypass scanning

☐

Scan by message direction

☐

Limit by source address

☐

Limit by recipient address

☐

Limit by sender IP address

☐

Limit by message size

☐

Limit by interface type

☐

Limit interface

☐

Limit by processing server

☐

Scan archives by default

☒

Maximum archive scan depth

Maximum archive files

Notes

- ♦ *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

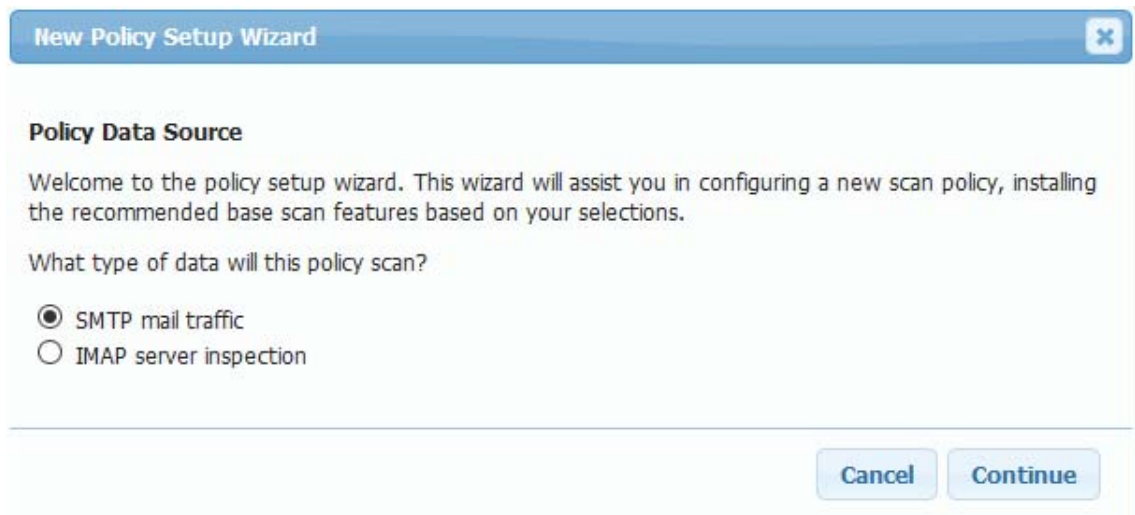
- ♦ Limit by message size
 - ♦ Minimum message size in bytes
 - ♦ Maximum message size in bytes
- ♦ Limit by interface type
 - ♦ Invert interface type list: Reverses the effect of the listed items.
 - ♦ Matched interface types: Click on [type list] to get a list of supported interfaces.
- ♦ Limit interface
 - ♦ 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.



New Policy Setup Wizard [X]

Policy Data Source

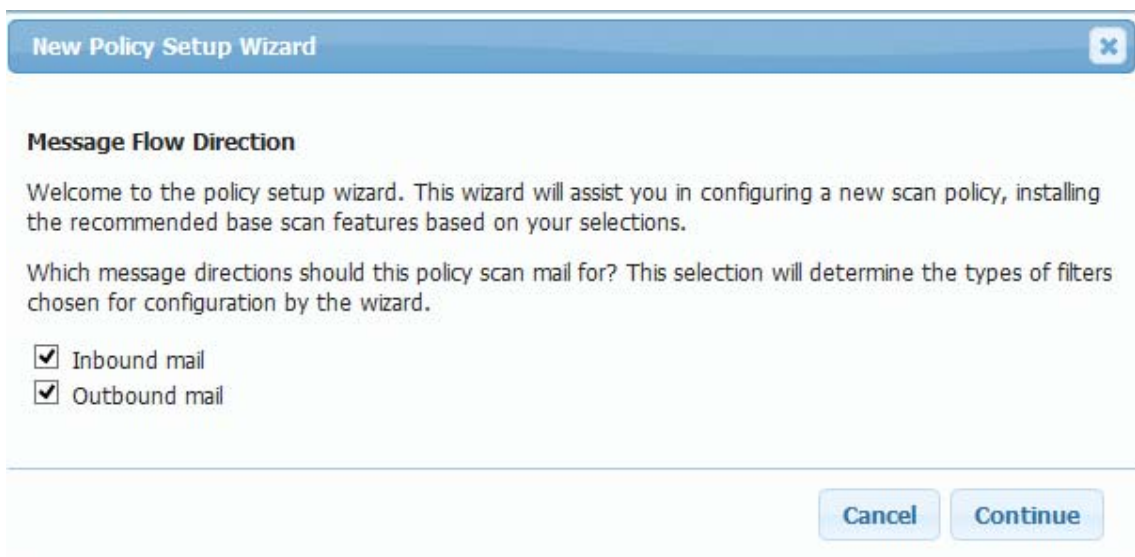
Welcome to the policy setup wizard. This wizard will assist you in configuring a new scan policy, installing the recommended base scan features based on your selections.

What type of data will this policy scan?

☒ SMTP mail traffic
☐ IMAP server inspection

Cancel Continue

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



New Policy Setup Wizard [X]

Message Flow Direction

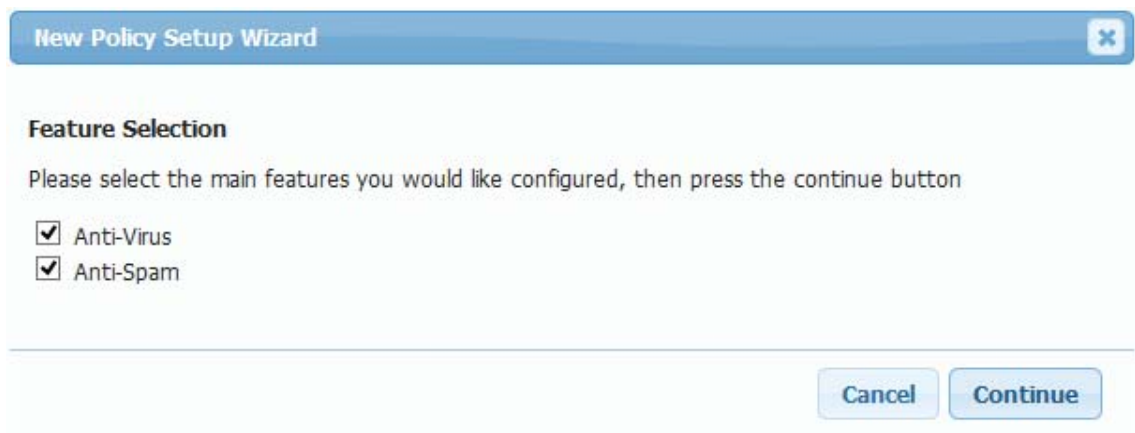
Welcome to the policy setup wizard. This wizard will assist you in configuring a new scan policy, installing the recommended base scan features based on your selections.

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

☒ Inbound mail
☒ Outbound mail

Cancel Continue

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



New Policy Setup Wizard [X]

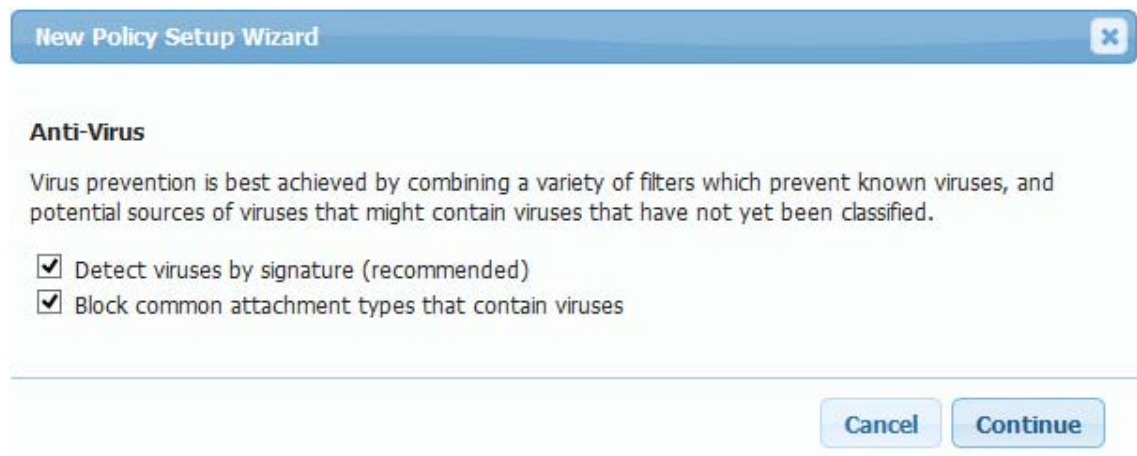
Feature Selection

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

☒ Anti-Virus
☒ Anti-Spam

Cancel Continue

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



The screenshot shows a window titled "New Policy Setup Wizard" with a close button in the top right corner. The main heading is "Anti-Virus". Below it, a paragraph states: "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." There are two checked checkboxes: "Detect viruses by signature (recommended)" and "Block common attachment types that contain viruses". At the bottom right, there are "Cancel" and "Continue" buttons.

New Policy Setup Wizard

Anti-Virus

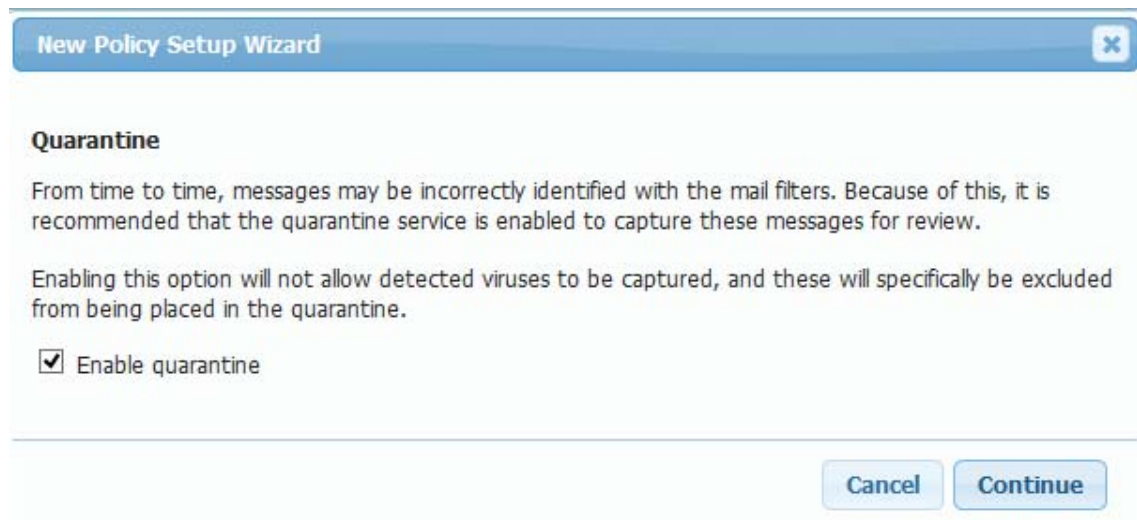
Virus prevention is best achieved by combining a variety of filters which prevent known viruses, and potential sources of viruses that might contain viruses that have not yet been classified.

☒ Detect viruses by signature (recommended)

☒ Block common attachment types that contain viruses

Cancel Continue

5. Select if you want messages quarantined.



The screenshot shows a window titled "New Policy Setup Wizard" with a close button in the top right corner. The main heading is "Quarantine". Below it, a paragraph states: "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." Another paragraph states: "Enabling this option will not allow detected viruses to be captured, and these will specifically be excluded from being placed in the quarantine." There is one checked checkbox: "Enable quarantine". At the bottom right, there are "Cancel" and "Continue" buttons.

New Policy Setup Wizard

Quarantine

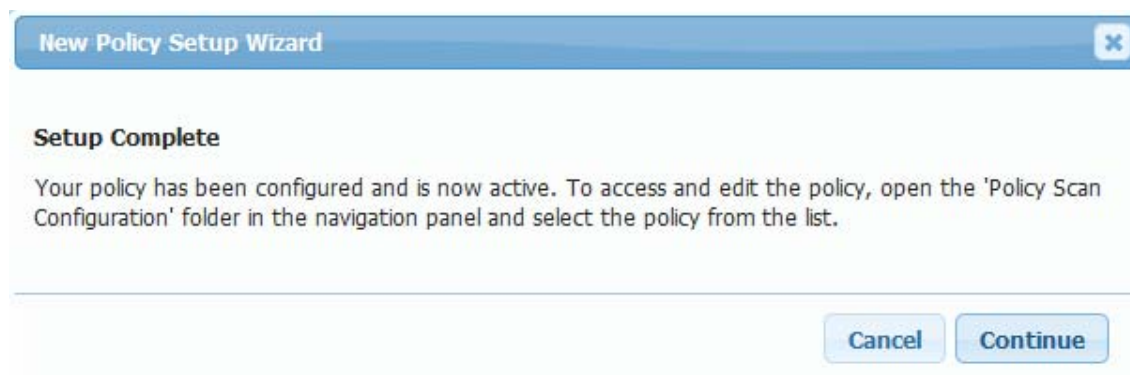
From time to time, messages may be incorrectly identified with the mail filters. Because of this, it is recommended that the quarantine service is enabled to capture these messages for review.

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

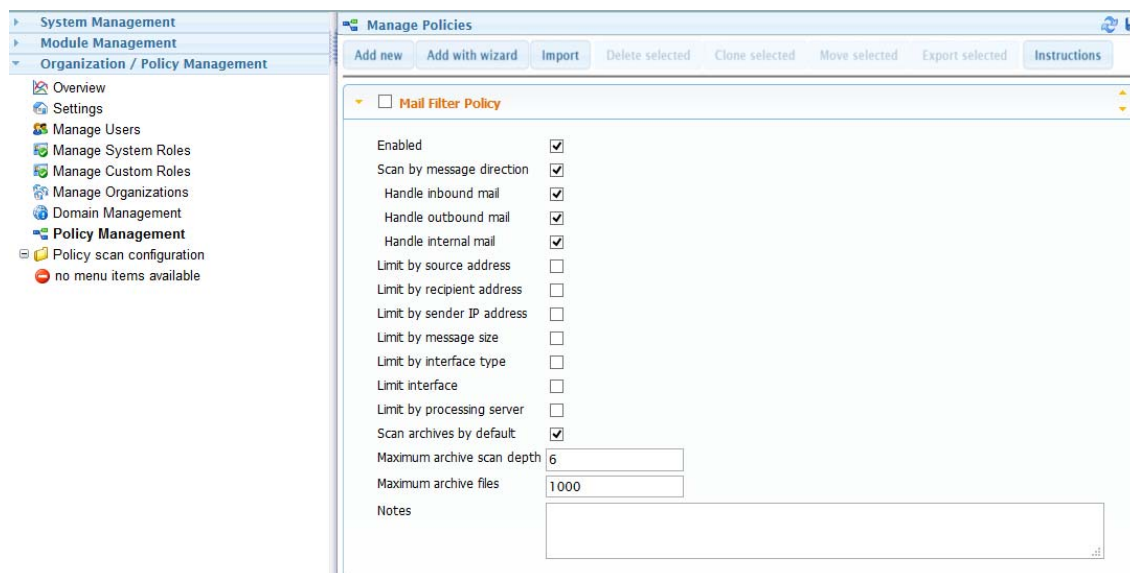
☒ Enable quarantine

Cancel Continue

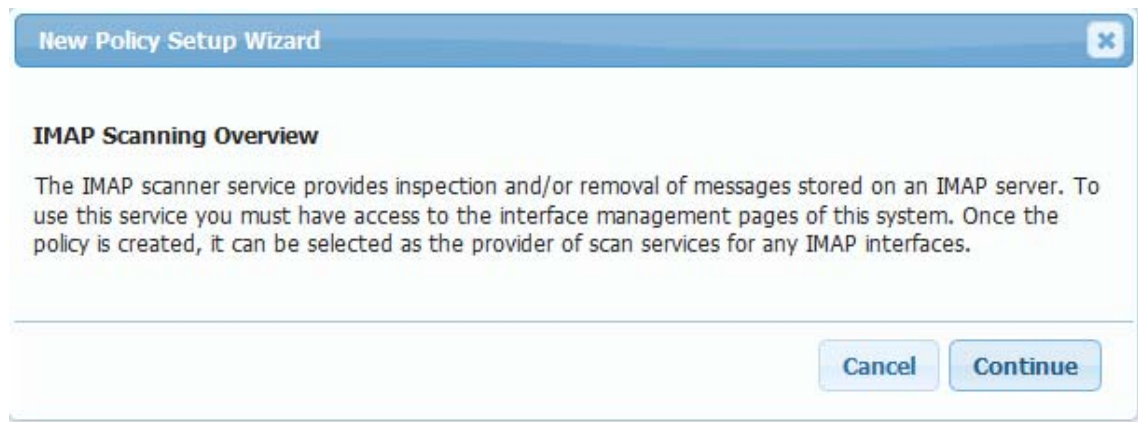
6. Select if you want messages tracked in the system.



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



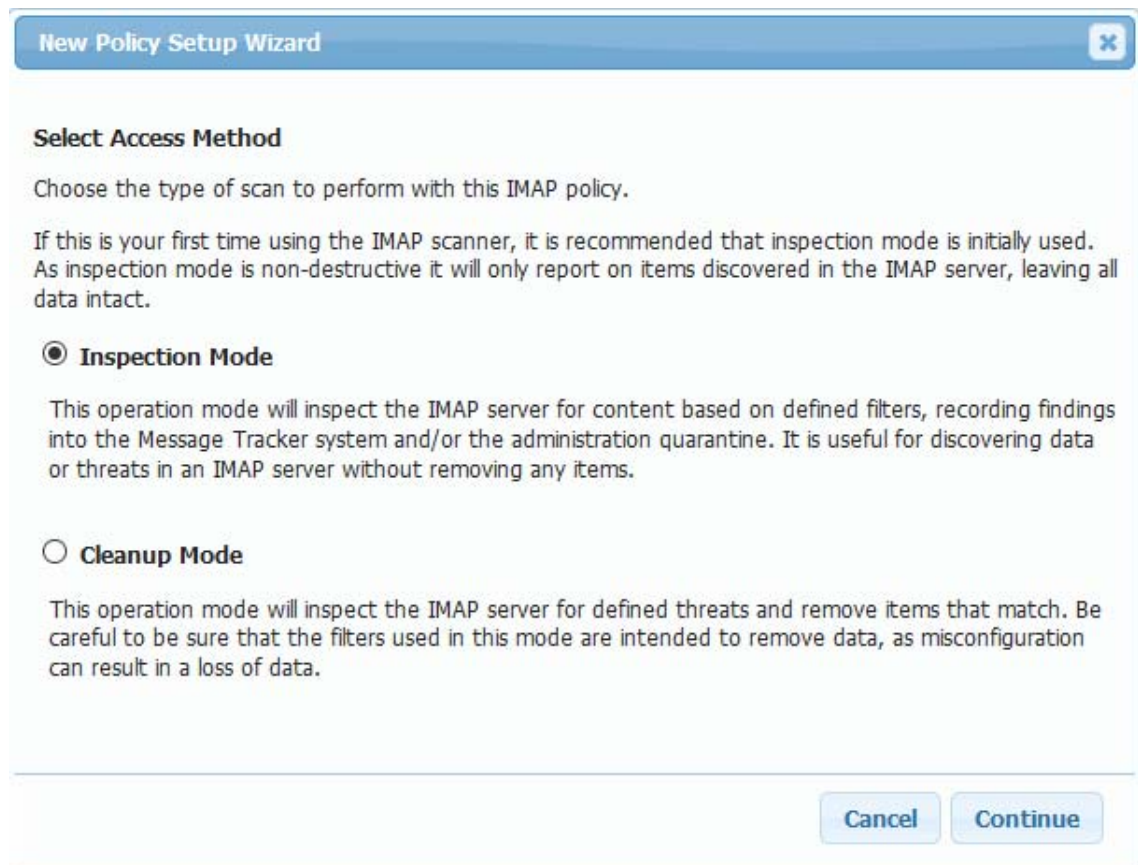
- Open the Policy scan configuration folder, or refresh to see the new policy, and click on the policy to see the workbench.



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 this 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.

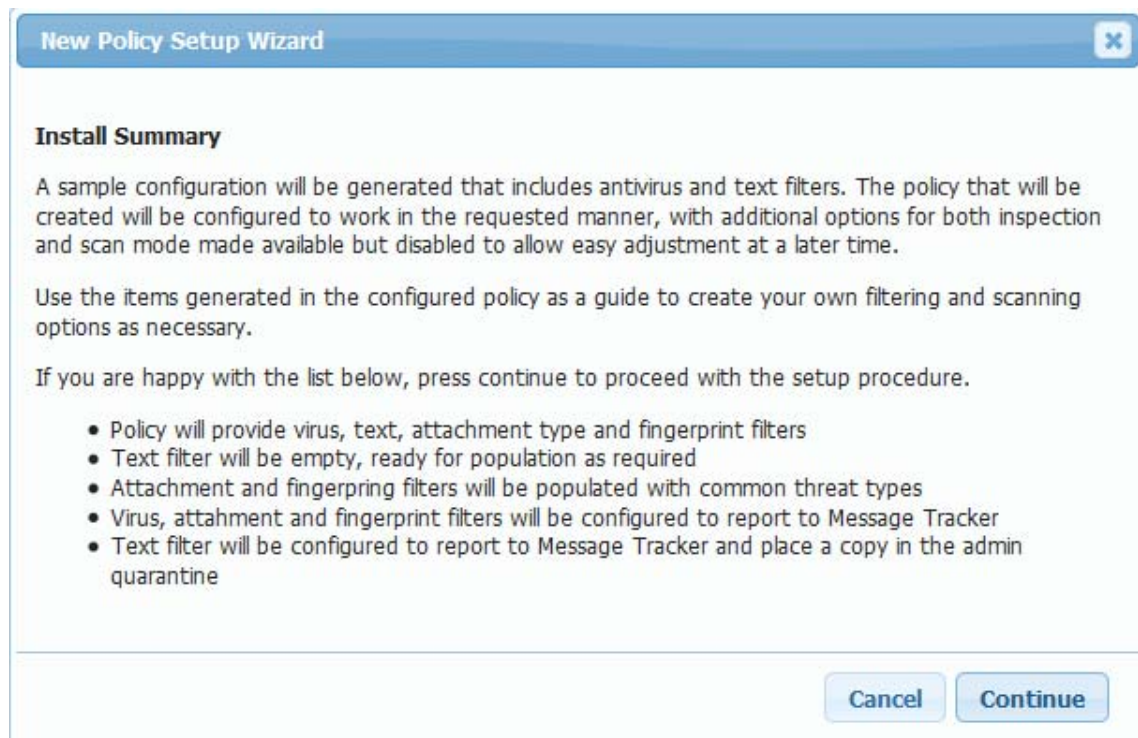
a. Inspection Mode

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.

b. 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

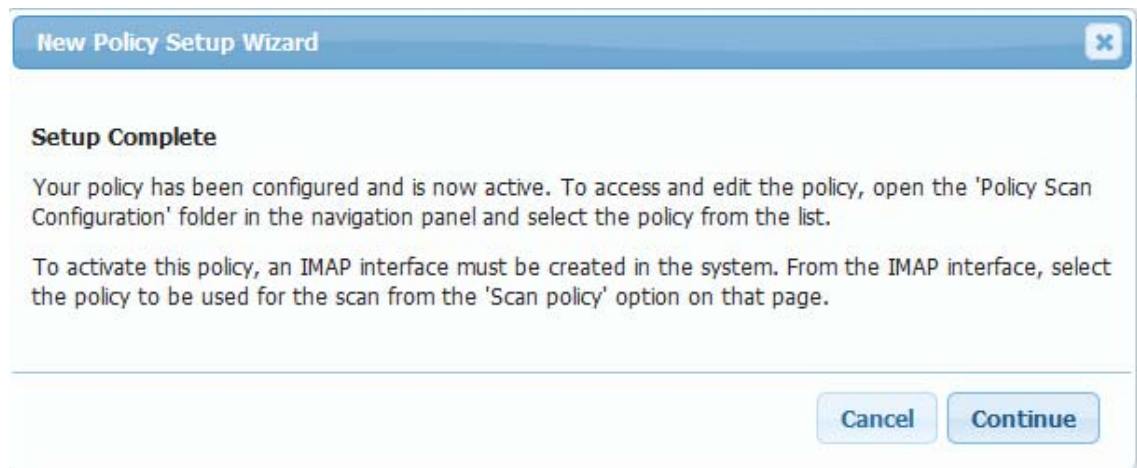
A sample configuration will be generated that includes anti-virus and text filters. The policy that will be created will be configured to work in the requested manner, with additional options for both inspection and scan mode made available but disabled to allow easy adjustment at a later time.

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

Manage Policies

Add new

Add with wizard

Delete selected

Clone selected

Move selected

Instructions

☐ IMAP Inspection Policy

Enabled

☒

Bypass scanning

☐

Scan by message direction

☒

Handle inbound mail

☐

Handle outbound mail

☐

Handle internal mail

☐

Handle collected mail

☒

Limit by source address

☐

Limit by recipient address

☐

Limit by sender IP address

☐

Limit by message size

☐

Limit by interface type

☒

Invert interface type list

☐

Matched interface types
[type list]

IMAP

Limit interface

☐

Limit by processing server

☐

Scan archives by default

☒

Maximum archive scan depth

6

Maximum archive files

1000

Notes

- ♦ 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 will allow you to chose 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 enables. 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 enabled. 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 enabled. Default, disabled (unchecked).
- ♦ Limit by message size: Allows you to set minimum and maximum message sizes for inspection. Default disabled (unchecked). Minimum message size: Default, 1000 bytes. Maximum message size: Default, 20000000 bytes.
- ♦ 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

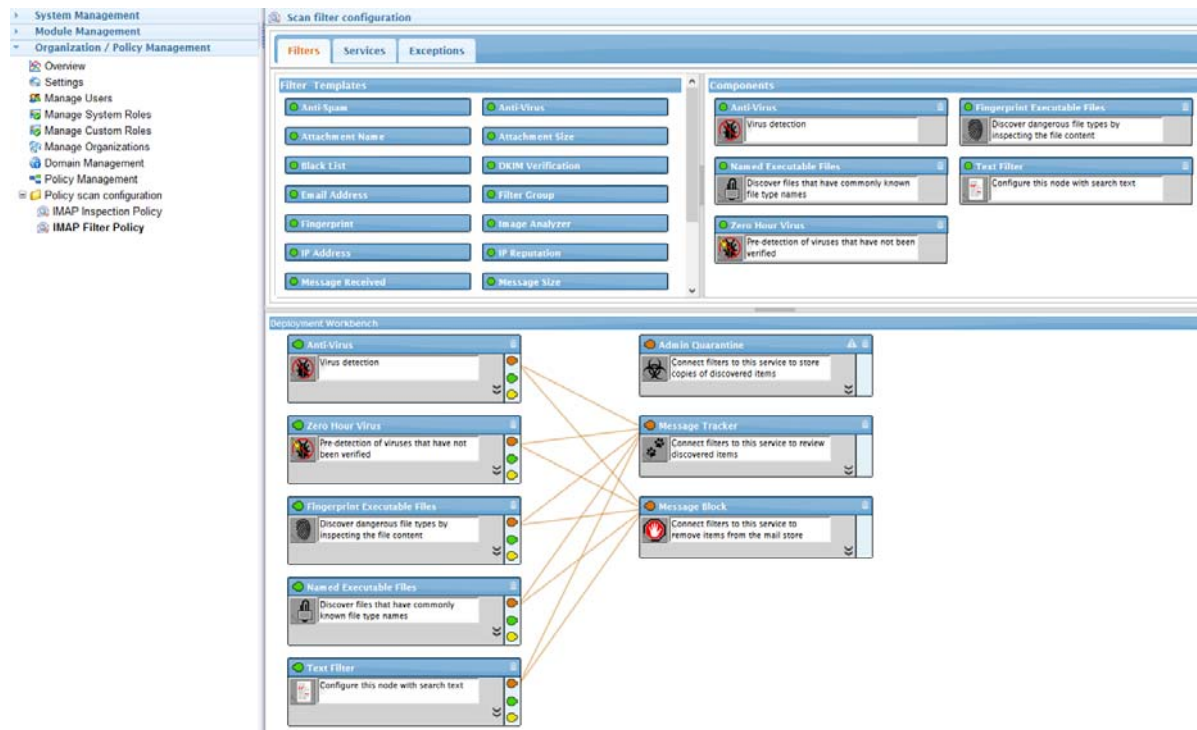
The IMAP policy wizard will create an Inspection policy with Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, Named Executable Filers, and Text filters. This will track the messages, with an Admin Quarantine for the Text Filter.

The screenshot displays the IMAP Policy Workbench interface, divided into two main sections: **Scan filter configuration** and **Deployment Workbench**.

Scan filter configuration: This section is further divided into **Filters**, **Services**, and **Exceptions** tabs. The **Filters** tab is active, showing a list of filter templates on the left and a list of components on the right. The filter templates include: Anti-Spam, Attachment Name, Black List, Email Address, Fingerprint, IP Address, Message Received, Anti-Virus, Attachment Size, DKIM Verification, Filter Group, Image Analyzer, IP Reputation, and Message Size. The components include: Anti-Virus (Virus detection), Fingerprint Executable Files (Discover dangerous file types by inspecting the file content), Named Executable Files (Discover files that have commonly known file type names), Text Filter (Configure this node with search text), and Zero Hour Virus (Pre-detection of viruses that have not been verified).

Deployment Workbench: This section shows a visual representation of the policy configuration. It features a central area with five filter nodes (Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, Named Executable Files, and Text Filter) and three service nodes (Admin Quarantine, Message Tracker, and Message Block). Lines connect the filter nodes to the service nodes, indicating the flow of data and the application of the policy. The Admin Quarantine node is connected to the Text Filter, Message Tracker, and Message Block nodes. The Message Tracker node is connected to the Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, and Named Executable Files nodes. The Message Block node is connected to the Anti-Virus, Zero Hour Virus, Fingerprint Executable Files, and Named Executable Files nodes.

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.



Importing and Exporting Policies

New in 23.4

Import and Export is a new feature that allows you to import and export policy settings, scanner filter configuration, node identities, and selected nodes. Import and export is useful to transfer policies from one SMG system to another, backup your policy configuration, track policy changes if you export the policies frequently, and get support on your SMG configuration.

Importing Policies

Importing policies lets you import a full policy as a new policy or to import the scanner configuration from an exported policy into an existing policy.

To import a policy:

- 1 In **Policy Management**, click **Import**.

or

If you are importing the scanner configuration, select a policy and then click **Import**.

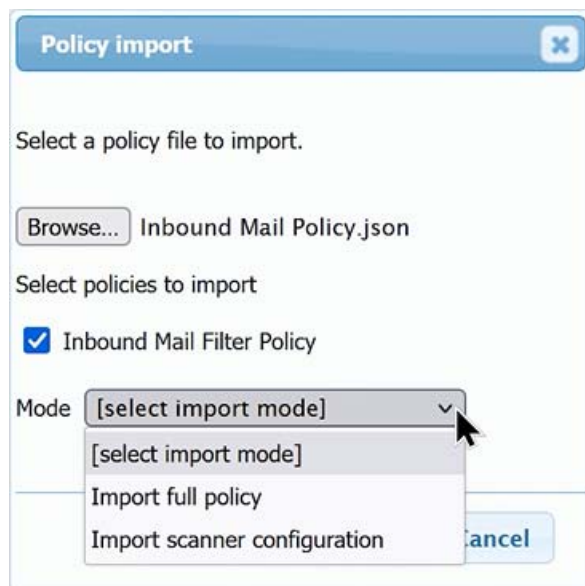


- 2 Select the file that contains the policies you want to import.



- 3 Select the policies to import and then the import mode: **Import full policy** or **Import scanner configuration**.

NOTE: **Import scanner configuration** must be imported into an existing policy. To use **Import scanner configuration**, select a policy that you want to import the scanner configuration into before selecting **Import**.



- 4 Click **Import**.

Exporting Policies

Exporting policies lets you export one or more policies in a single json file. The default name of the file export file includes the date of the export.

- 1 Select the policy/policies you want to export and click **Export**.



- 2 Select what options you want to export from the policies:
 - ♦ **Export qualifications:** Exports the policy settings from policy management.
 - ♦ **Export scanner configuration:** Exports the scanner filter configuration.
 - ♦ **Export node identities:** Exports the unique node identifiers. This allows node replacement during repeated import.
 - ♦ **Export selected nodes:** *Only available if you have a single policy selected to export.* When selected presents you with a list of individual nodes that you can export. The most common use of this is to provide a content update list a word list. Only exports the component and not the workbench instance.
- 3 Click **Ok** to save the exported policies to a file.

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.

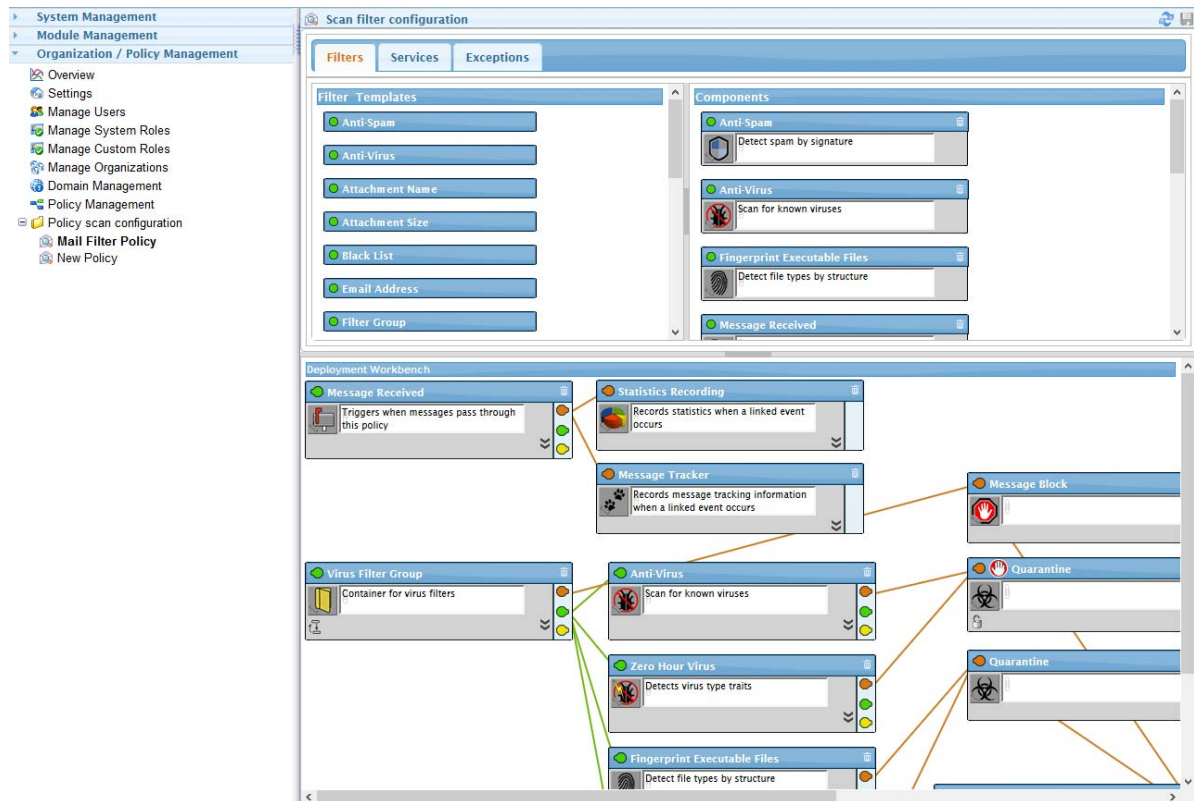
Filters scan messages passing through the system. Any message entering a policy will trigger all filters that are part of the policy.

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.

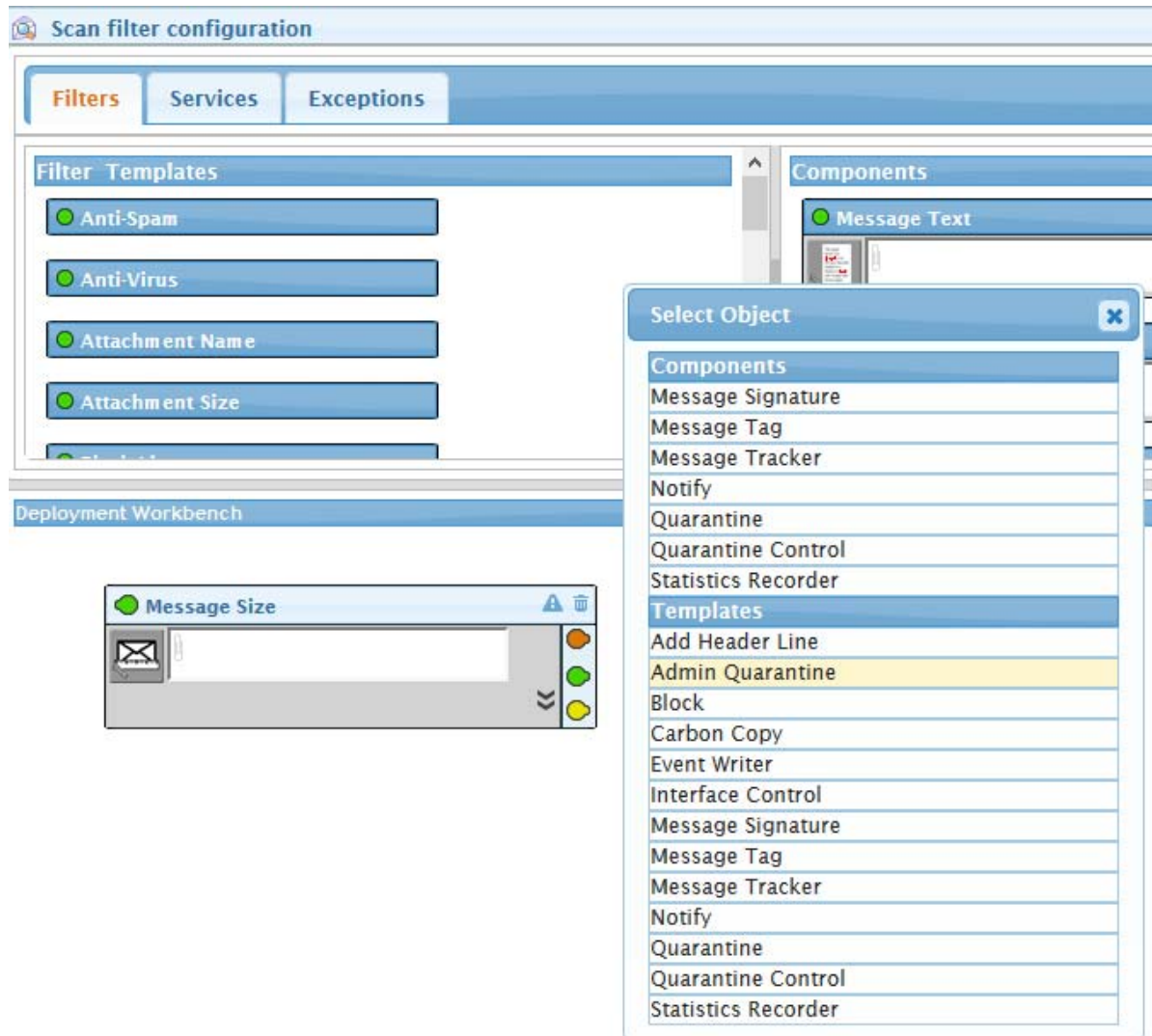


Drag items from the Template panel to the Workbench panel.

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

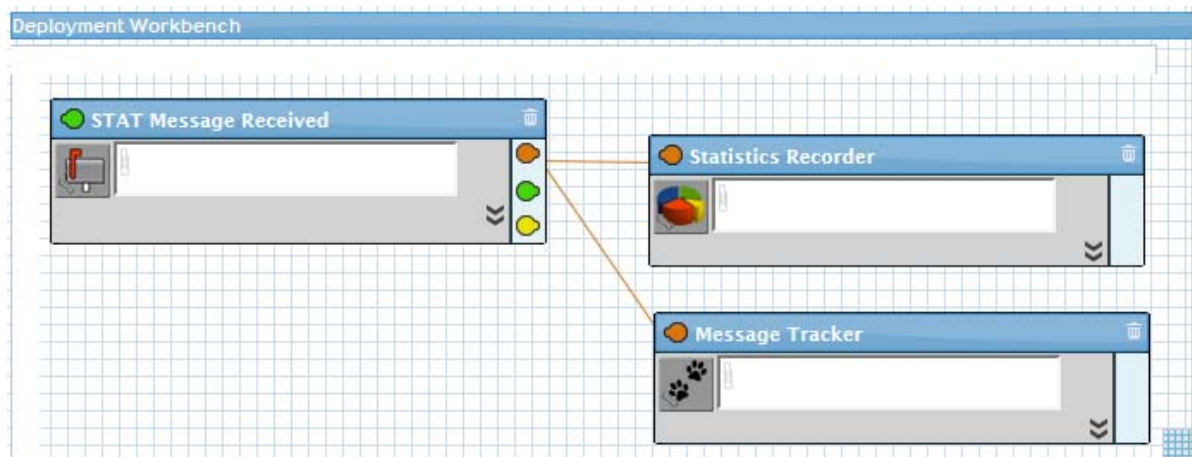
- ♦ *Red pins* on Filters go to *Red titles* on Services.
- ♦ *Green pins* on Filters go to *Green titles* on Filter Groups.
- ♦ *Yellow pins* on Filters go to *Yellow titles* on Exceptions.

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.

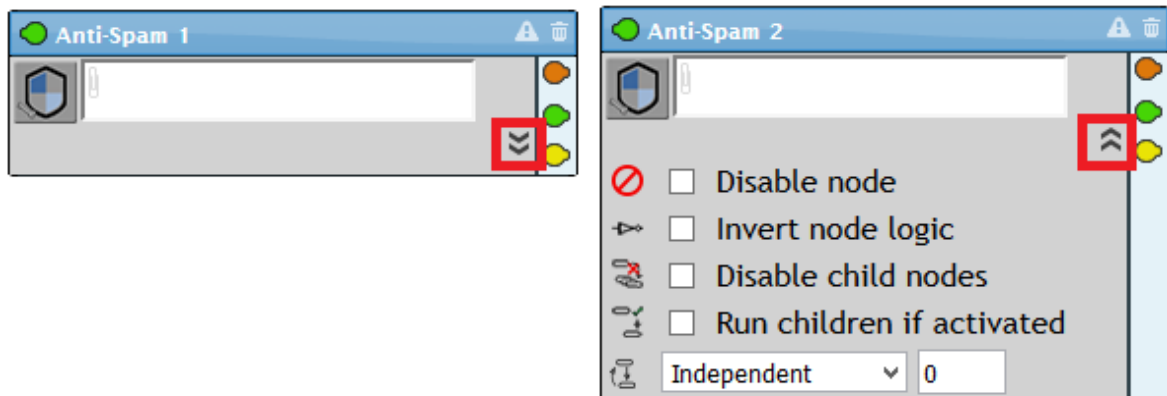
A snap-to-grid option can be toggled by clicking on the grid button at the bottom-right



Component Settings

Components can be renamed by clicking on their name.

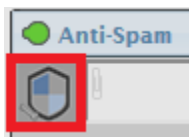
Individual component settings are accessed through the reveal chevron.



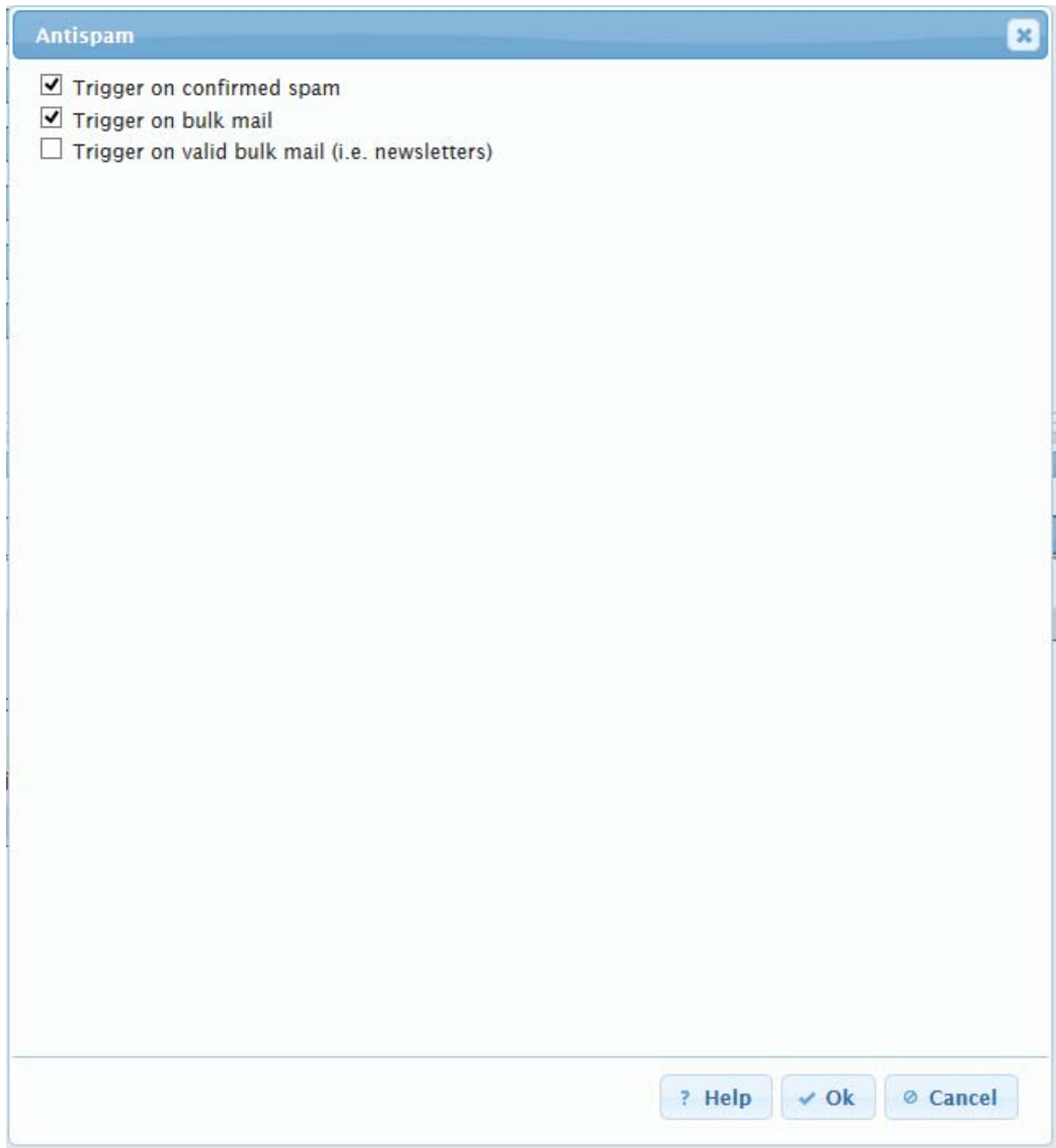
Component Configuration

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.

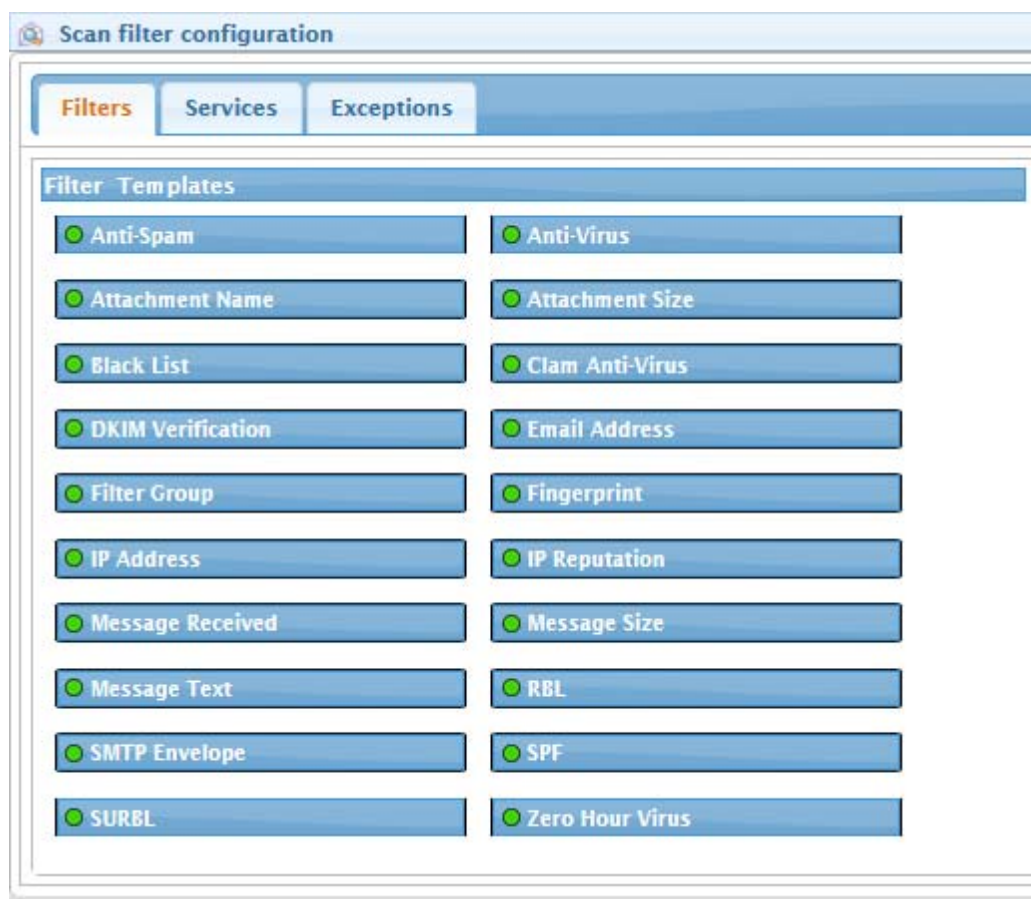


Select setting to trigger on.

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 it's own line. The attachment name differs from the fingerprint filter in that the fingerprint detects file types regardless of name, while the attachment name filter only looks at the file name.

Options

Add each criteria on its own line.

Attachment size

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

Options

Enable maximum size test.

Maximum allowable size (bytes).

Enable minimum size test.

Minimum allowable size (bytes).

Black List

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

Options

Black List Data Source

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

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

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 \(http://www.dkim.org/\)](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.

The IP reputation sensitivity slider is used to fine tune the detection level of the IP reputation service. There is a left slider and a right slider that can be changed to change the detection level. The left slider is used to ignore IP addresses that fall into the lower range of possible Spam. The right slider is used to increase or decrease the range of IP addresses that are allowed to retry and the range that are automatically rejected. The default setting of 20% delay and 80% drop provides a generally good fit to incoming connection, where 20% are offered the option of retrying and the rest is denied access.

If the engine is delaying legitimate senders, you can adjust the left slider to ignore the range of IP addresses that are legitimate.

Options

Trigger on confirmed IP.

Trigger on suspect IP.

Message Received

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

Options

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

Message direction.

Message Size

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

Options

Enable maximum size test.

Maximum allowable size (bytes).

Enable minimum size test.

Minimum allowable size (bytes).

Message Text

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

Options

Look in message body.

Look in message subject.

Look in message header.

Look in message source file.

RBL

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

Options

Include connecting IP address.

Include ip addresses located in headers.

Received headers scan range.

RBL Server.

sbl-xbl.spamhaus.org (Default).

bl.spamcop.net (Default).

Skip Local IP.

SMTP Envelope

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

Options

Client is authenticated.

Client is SSL secure.

Client switched to SSL using STARTTLS.

SPF

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

Options

Treat ~all as -all. 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

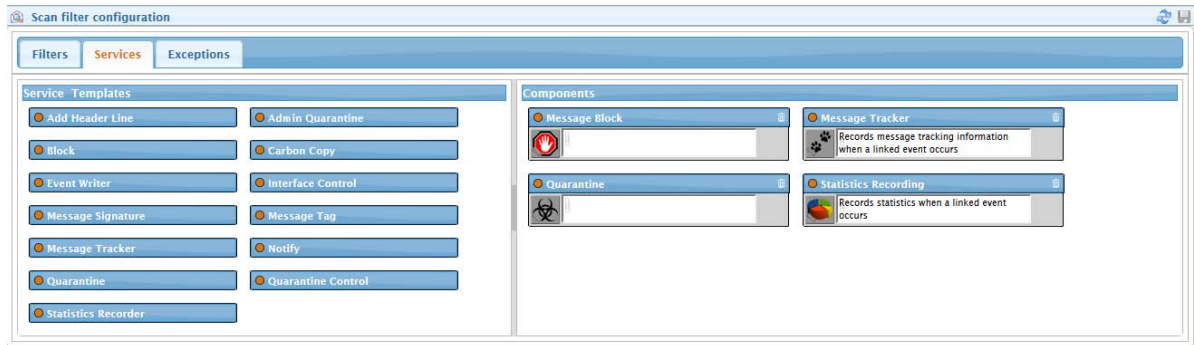
The Zero Hour Virus filter checks each message for virus-like characteristics to protect against new and unidentified viruses.

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).

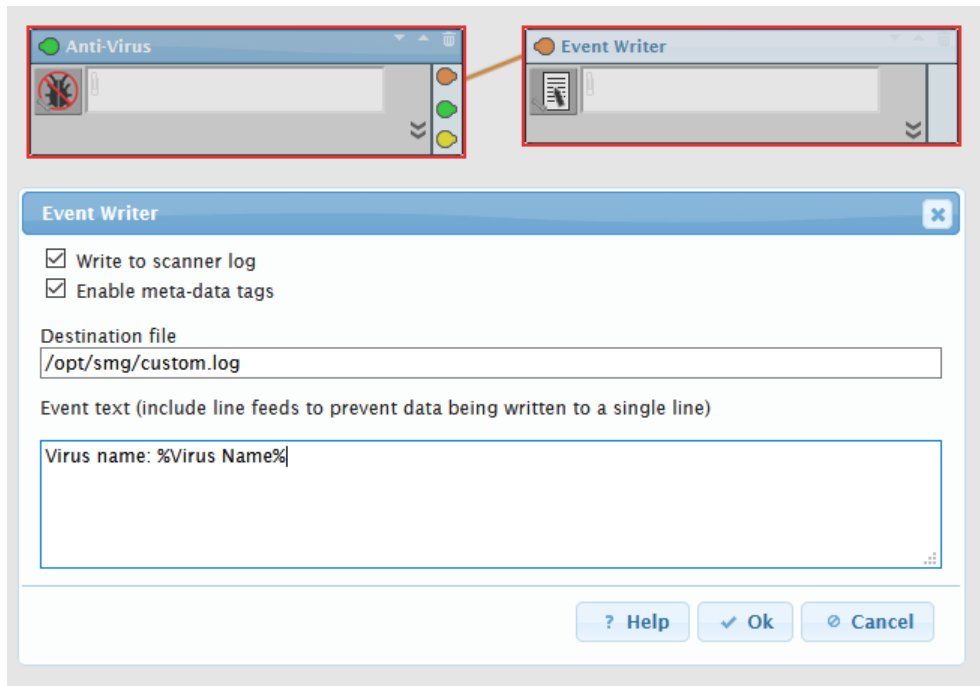
DKIM Sign

The DKIM Sign allows for the signing of outgoing messages. See Enabling DKIM Signing [“Enabling DKIM Signing” on page 174](#) 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. You can also write the event to the scanner log and enable meta-data tags in the event text.



Meta-data Tags

When using meta-data tags in the logs, there are three forms that can be used:

- **%meta-var%** - Writes the value of the meta-data to the log. If more than one item with the name exists, this will report the first one found. **Example:** %Recipient email%.
- **%meta-var[n]%** - Write the value of the meta-data at the given index *n* where *n* is a number, 0 or higher. If the index is not found, the result will be blank. **Example:** %Recipient email[3]%.
- **%meta-var[s]%** - Writes all of the values of the meta-data to the log separated by *s* where *s* is a string, but not a number. **Example:** %Recipient email[,]%.

The default meta-data that can be written is limited to the filter that triggers the event writer service. You can access all meta-data that is gathered by adding a colon to the front of the meta-data tag after the percent symbol. This is useful if you are exporting generic data to be consumed by other programs and just want a single meta-data collection node attached to the Message Received filter.

Example event text: SURBL: %:SURBL service%/:%:Site matched% RBL: %:RBL service%/:%:Client address%.

Available meta-data tags are as follow (grouped by event):

Global

- ♦ **%time%** - Time formatted as hh:mm:ss.
- ♦ **%date%** - Date formatted as yyyy-mm-dd.
- ♦ **%epoch%** - Unix epoch value (number of seconds since Jan 1, 1970).
- ♦ **%procid%** - The unique identifier of the message scan session
- ♦ Address filter:
 - ♦ **%Sender email%** - The envelope sender address.
 - ♦ **%Recipient email%** - The envelope recipient address.

Antispam Filter

- ♦ **%Spam status%** - When detected, which type of detection.
- ♦ Attachment Name filter:
 - ♦ **%Filename%** - The matching file name.
 - ♦ **%Extracted from%** - The container file that the detected file was extracted from.
- ♦ Attachment Size filter:
 - ♦ **%Filename%** - The file that did not conform to the size limits.
 - ♦ **%Attachment size%** - The size of the file.
 - ♦ **%Maximum allowable size%** - The maximum size limit.
 - ♦ **%Minimum allowable size%** - The minimum size limit.

Antivirus Filter

- ♦ **%Virus name%** - The name of the virus that was detected.

Blacklist Filter

- ♦ **%Email from/to%** - The address pair that triggered the filter.

ClamAV Filter

- ♦ **%ClamAv Virus name%** - The name of the virus that was detected.
- ♦ Fingerprint filter:
 - ♦ **%Filename%** - The matching file name.
 - ♦ **%Extracted from%** - The container file that the detected file was extracted from.
 - ♦ **%Fingerprint%** - The fingerprint that was detected.

IP Address Filter

- ♦ **%IP address%** - The IP address that matched the filter.
- ♦ IP Reputation filter:
 - ♦ **%Source address detected%** - The IP address that was marked as confirmed.
 - ♦ **%Source address temp failed%** - The IP address that was marked as suspicious.

- ♦ Message size filter:
 - ♦ **%Message size%** - The size of the message.
 - ♦ **%Maximum allowable size%** - The maximum size limit.
 - ♦ **%Minimum allowable size%** - The minimum size limit.
- ♦ RBL filter:
 - ♦ **%RBL service%** - The RBL server that detected the IP address.
 - ♦ **%Client address%** - The IP address of the connecting client used to check RBL.
 - ♦ **%Header address%** - The IP address from header used to check RBL.
- ♦ SMTP filter:
 - ♦ **%Envelope state%** - The test that activated the filter.
- ♦ SPF filter:
 - ♦ **%IP address%** - The connecting client IP address.
 - ♦ **%Email address%** - The envelope sender address.
- ♦ SURBL filter:
 - ♦ **%SURBL service%** - The SURBL server used for detection.
 - ♦ **%Site matched%** - The URI that triggered the filter.
- ♦ Text filter:
 - ♦ **%Location%** - The part of the message that matched the text filter.

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 than 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.

Force SSL in report link: Linked to the release server URL. Default disabled.

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

Options

Notification template: To customize templates, see [Templates“Templates” on page 46.](#)

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 by 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 than 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

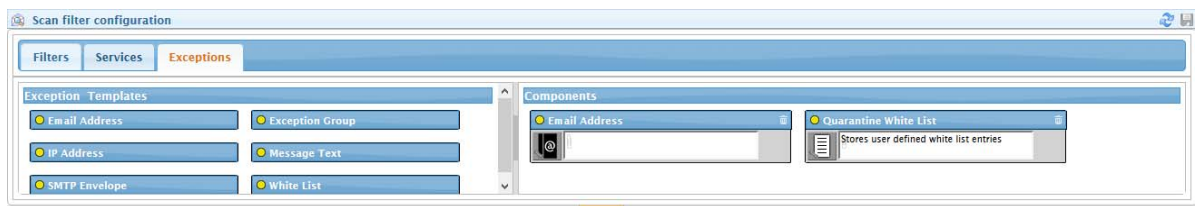
The statistics recorder records data on messages passing through the system where it is connected to events, exceptions, and filters. This is used with the Message Received filter. This Service requires no configuration. Simply set it in the correct listening spot in the system.

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.

7 Policy Configuration Tips and Tricks

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

Creating a policy manually involves:

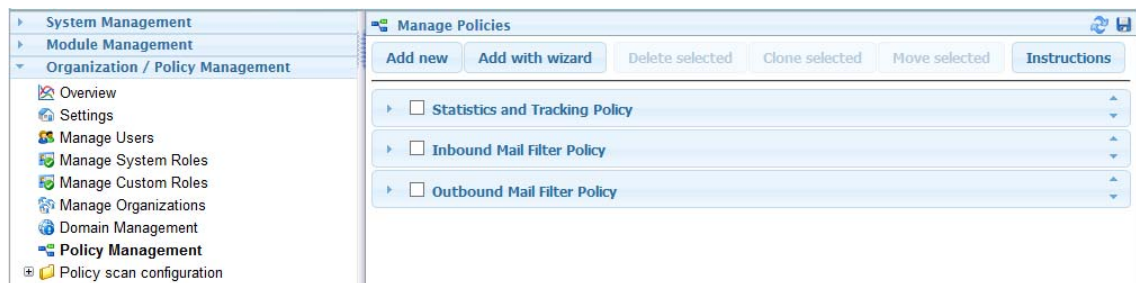
1. Creating the policy
2. Setting the policy priority, messages move through the policies from top to bottom
3. Set the policy message scan direction
4. Configuring the policy with filters, services and exceptions

The following are examples of policy implementations.

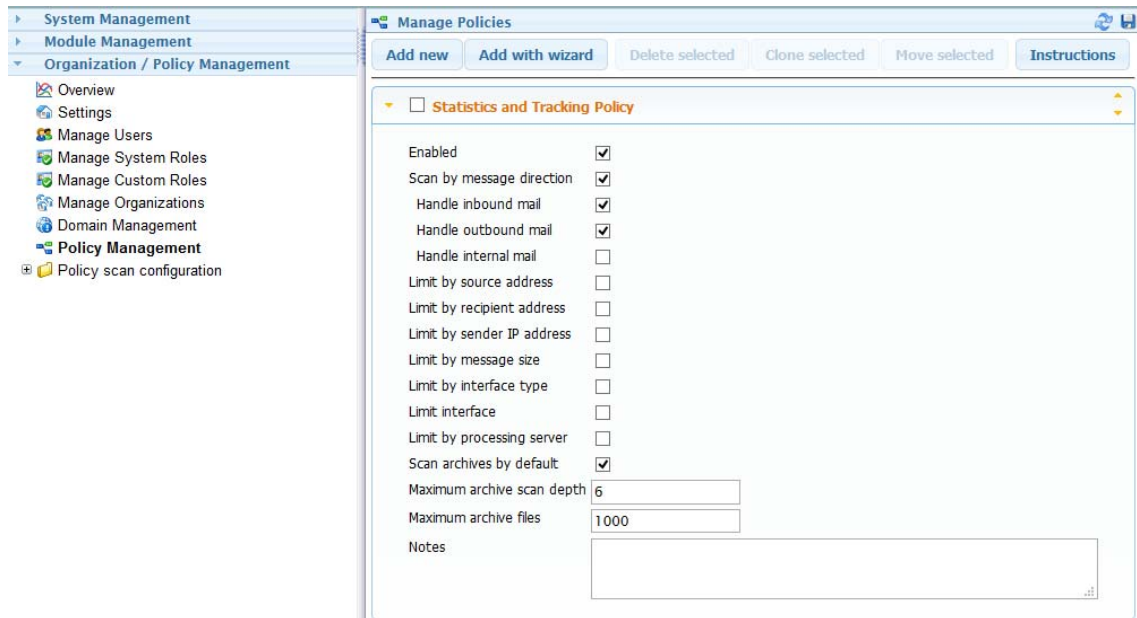
Creating a Statistics and Tracking Policy

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.

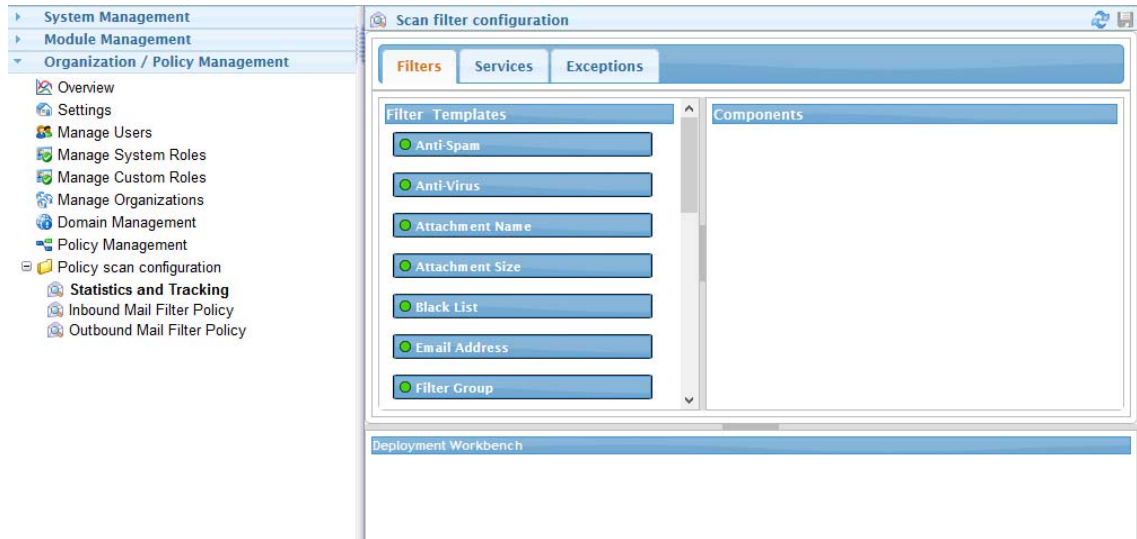


3. Set the Policy Message Direction
4. Open the panel and enable *Scan by message direction* then enable *Handle inbound mail* and *Handle outbound mail*.



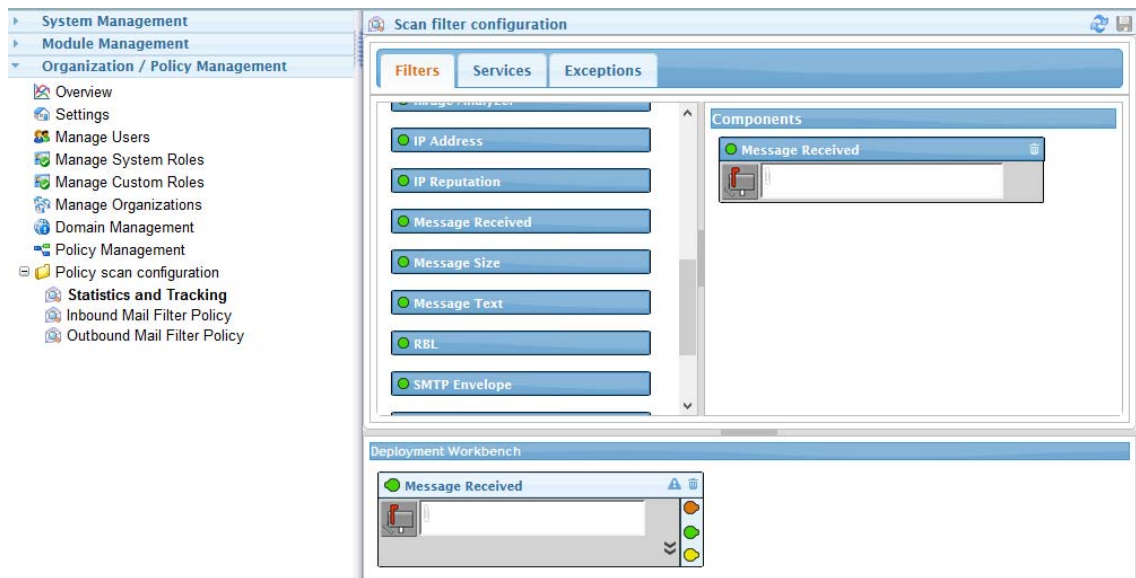
5. Configure the Scanner

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



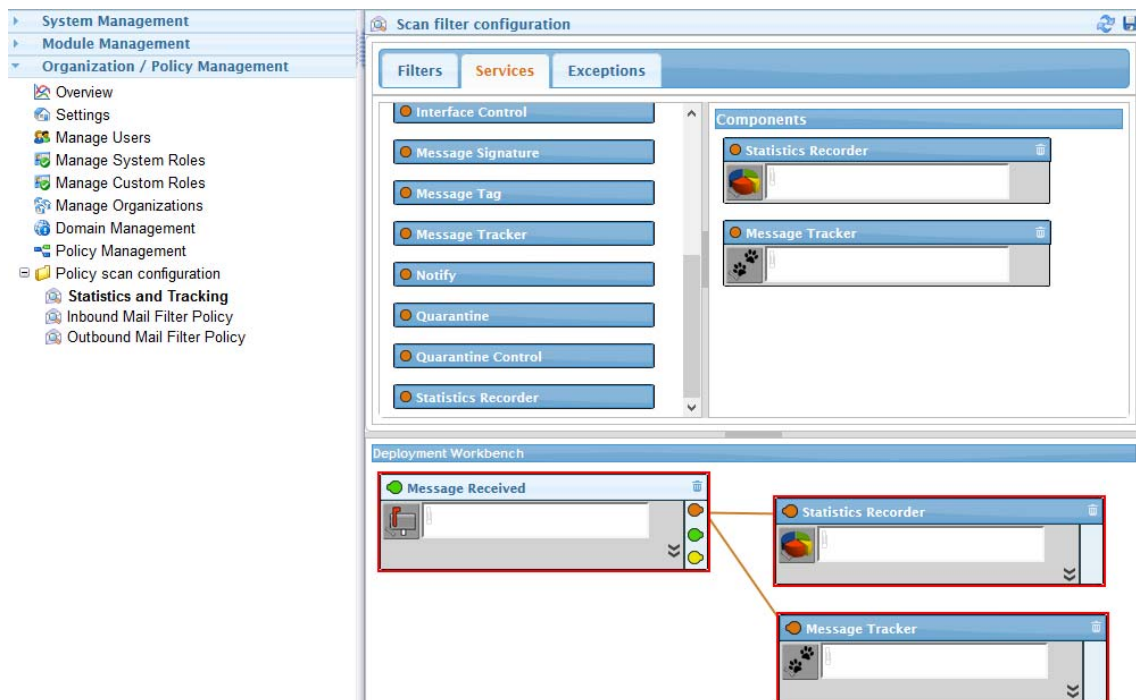
7. Add the Filter

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.

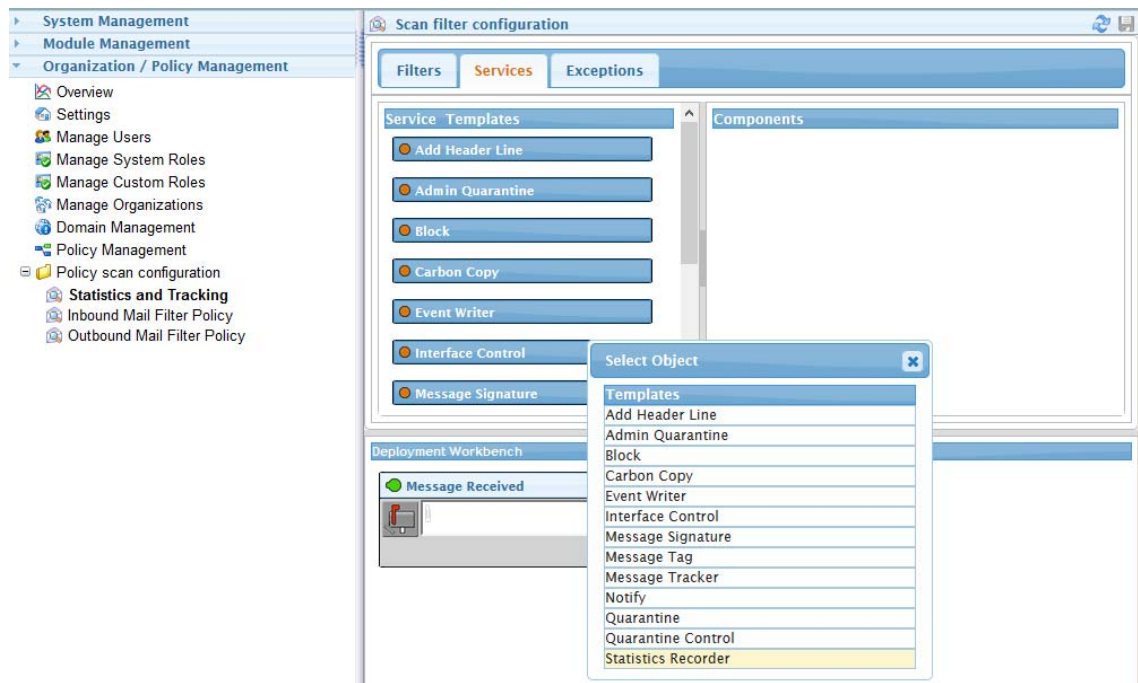


9. Add the Service

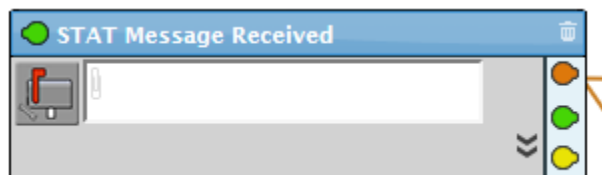
10. A service can be added by selecting the Services tab and dragging the desired service to the workbench and then clicking and dragging the red services pin on the right side of the filter to the service. Multiple services may be attached to a filter.



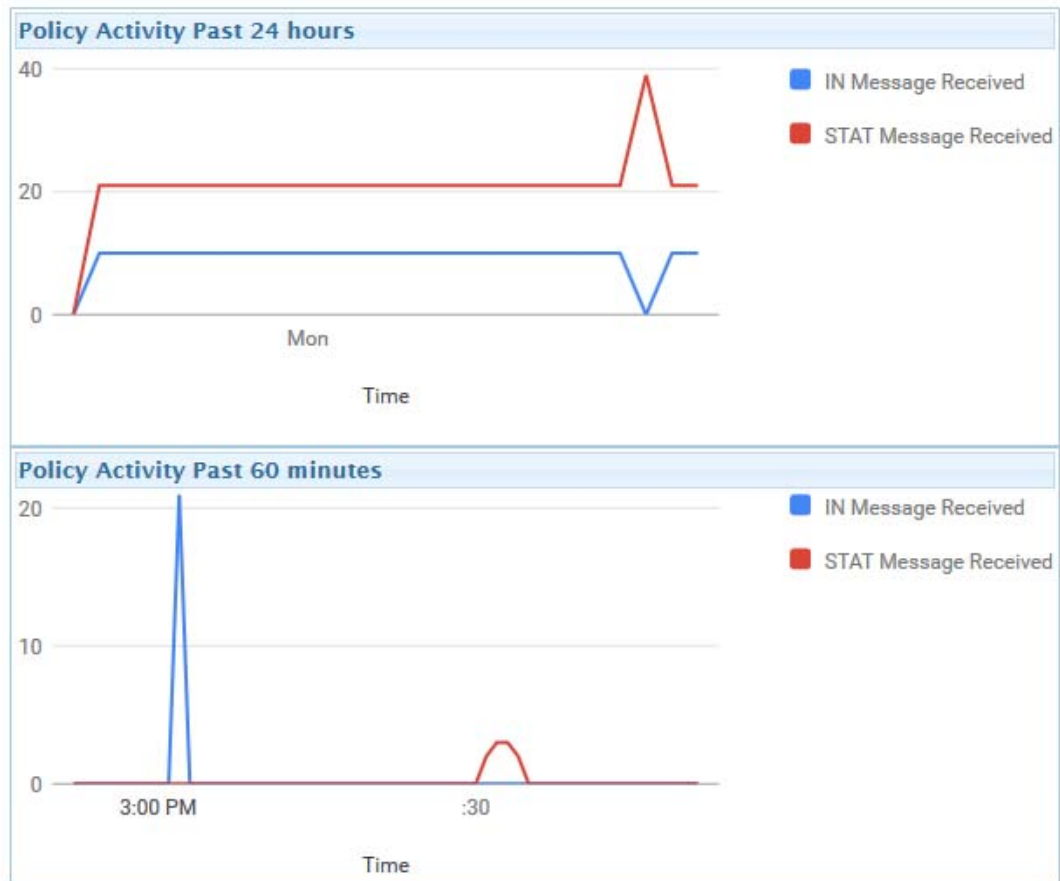
11. Alternatively, drag the red services pin on the right side of the filter and drop on any white space within the workbench and a service selection menu will appear. Select the service desired, for example, Statistics Recorder.



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*



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

Jun 8, 2017							Search
Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address	
08-Jun-2017 11:34:47 am	Fruit flavors are used in fizz drinks. 1263368060	script@sf.gwava.net	test7@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:34:25 am	The hail pattered on the burnt brown grass. 498208501	script@sf.gwava.net	test8@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:34:03 am	Whittings are small fish caught in nets. 2120411854	script@sf.gwava.net	test9@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:33:52 am	A thick coat of black paint covered all. 1128763930	script@sf.gwava.net	test5@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:33:30 am	The leaf drifts along with a slow spin. 946886760	script@sf.gwava.net	test4@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:33:08 am	A castle built from sand fails to endure. 1357637890	script@sf.gwava.net	test6@doc.mf.net	internal	none	151.155.183.142	
08-Jun-2017 11:32:46 am	The fly made its way along the wall. 826354919	script@sf.gwava.net	test3@doc.mf.net	internal	full	151.155.183.142	
08-Jun-2017 11:32:24 am	They felt gay when the ship arrived in port. 25998381	script@sf.gwava.net	test2@doc.mf.net	internal	full	151.155.183.142	

17.

18.

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.

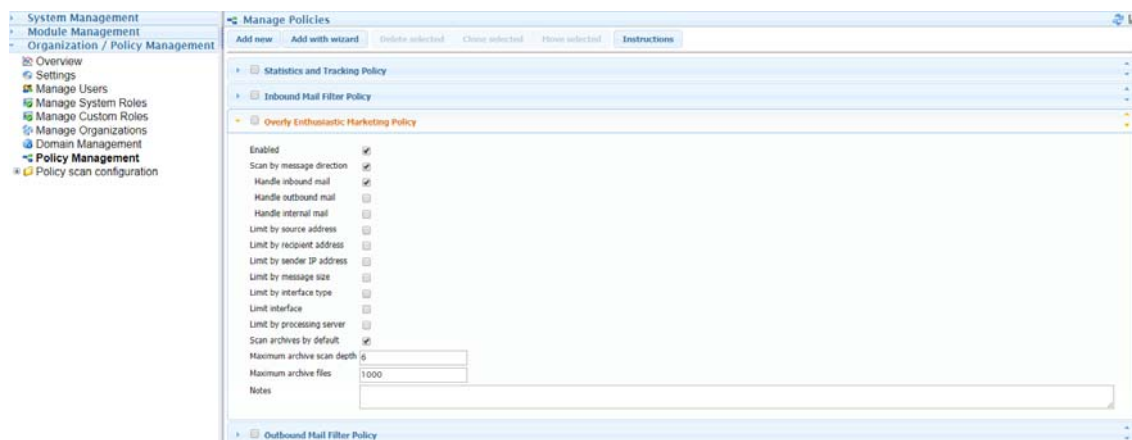
In this case, the Inbound Mail Filter Policy is a wizard created policy that deals with general spam, and malware. However, unwanted message are getting through and need to be dealt with.

Creating a policy manually involves:

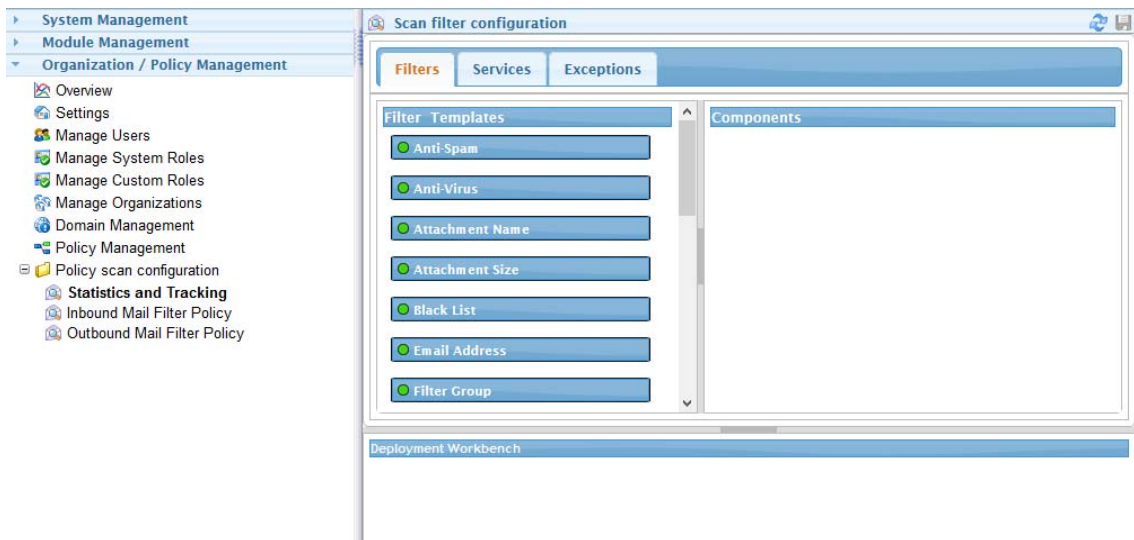
1. Creating the policy
2. Setting the policy priority, messages move through the policies from top to bottom
3. Set the policy message scan direction
4. Configuring the policy with filters, services and exceptions

Create the Policy

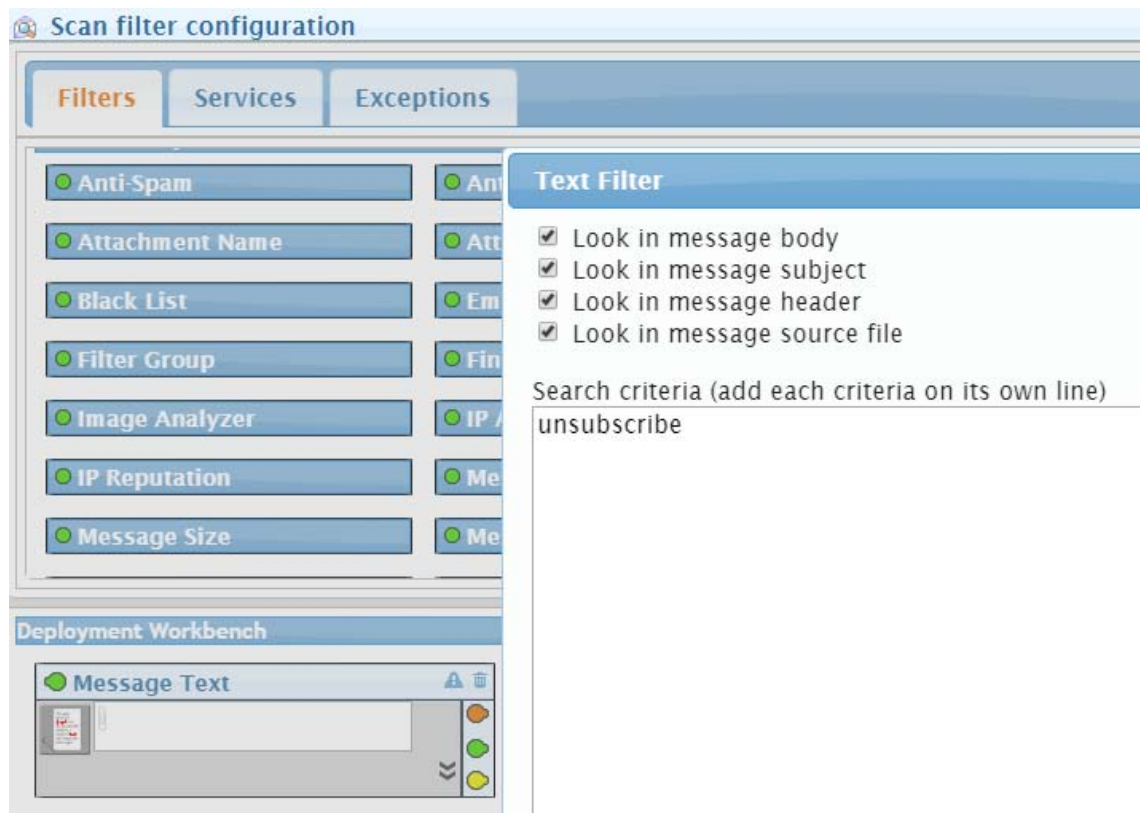
1. Under *Organization / Policy Management / Policy Management*, click *Add New* to create a new policy and name it something easy to remember like *Overly Enthusiastic Marketing Policy*.
2. Set the Policy Message Direction
3. Open the panel and enable *Scan by message direction* then enable *Handle inbound mail*.



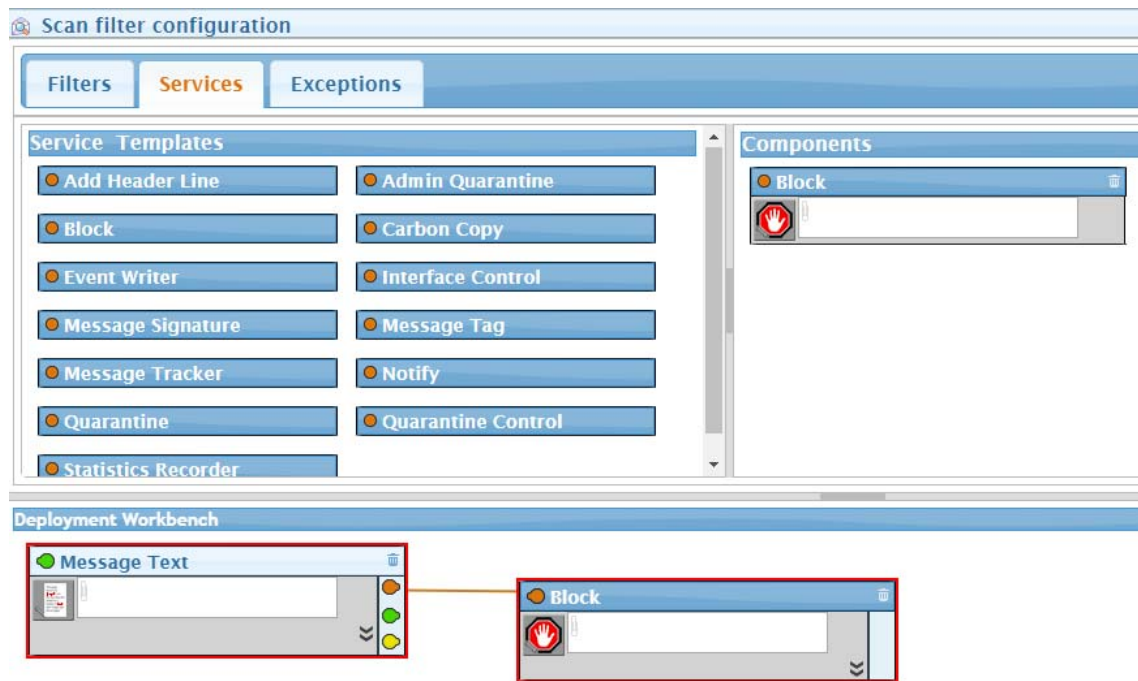
4. *Configure the Scanner*
5. Open the *Policy scan configuration* folder and select the policy. The workbench will be empty.



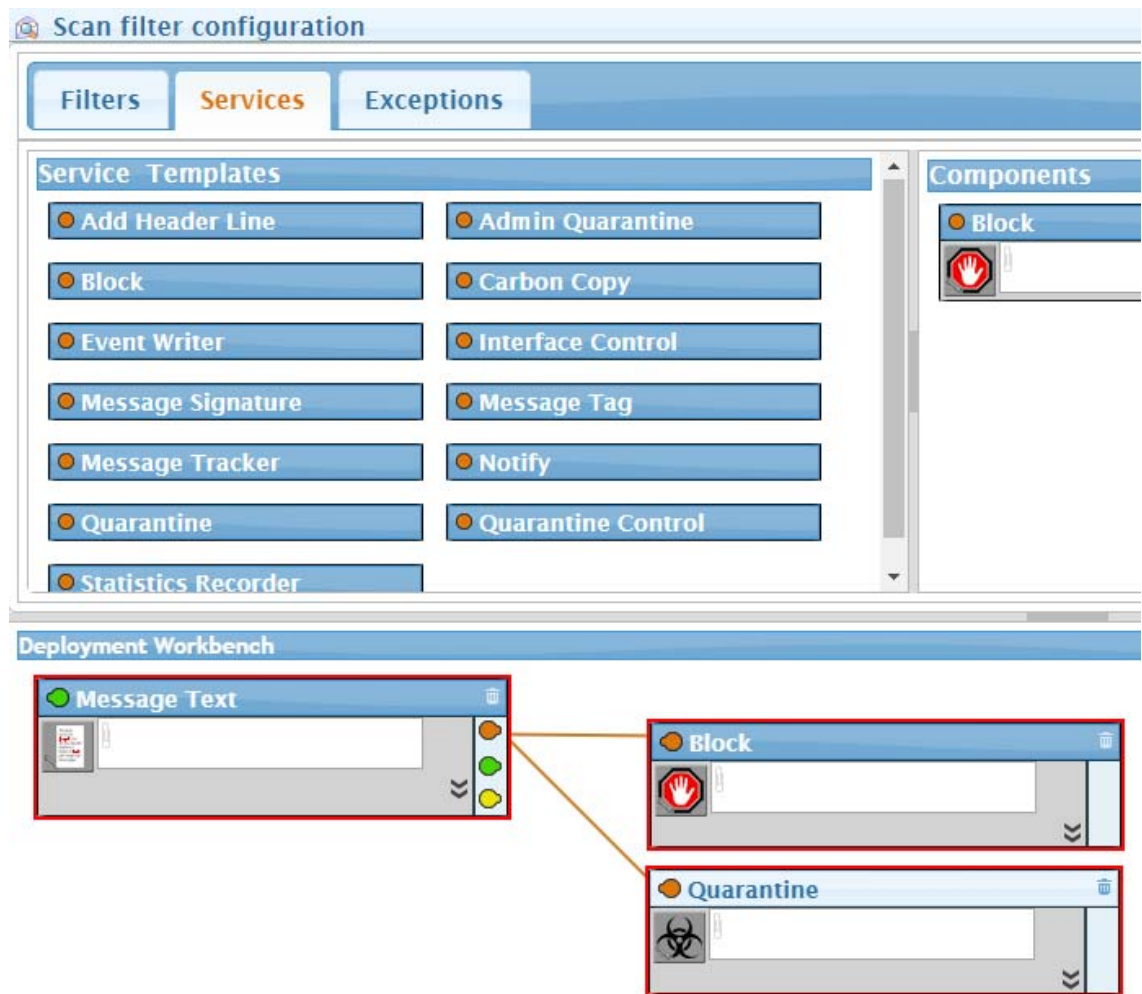
6. *Add the Filter*
7. There are a number of filters that could be used to manage the unwanted mail.
8. *Black List*: This requires a known Sender address and Recipient address. This is useful if the CEO is getting too much email from a particular marketer.
9. *Email Address*: This can filter by sender 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.



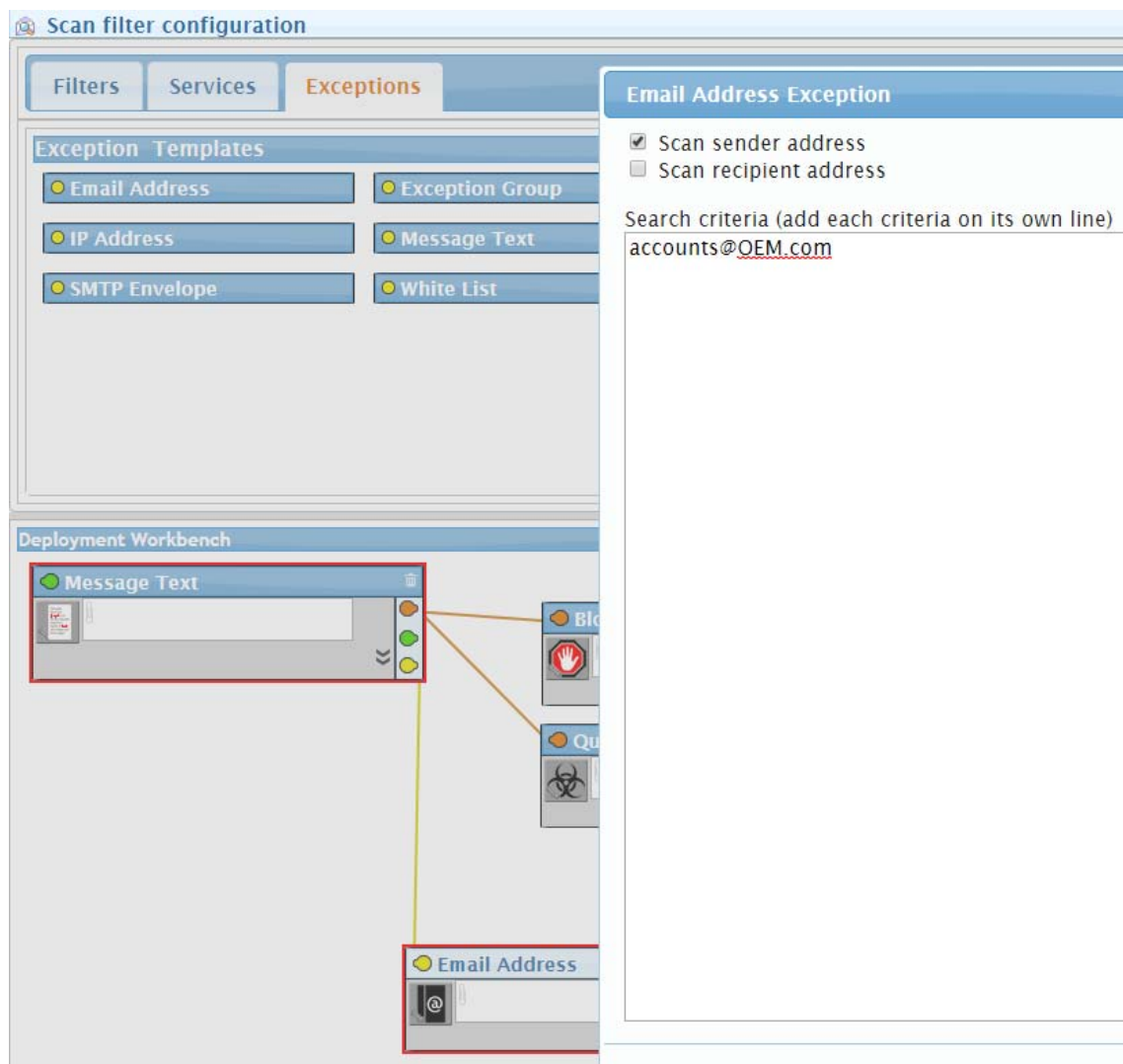
15. The filter will now scan messages for the word “unsubscribe”, but without one or more services nothing will be done with the message.
16. Add Service
17. Select the *Services* tab and drag and drop the Block service to the workbench, or drag and drop the red Services pin and select Block.



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 Enthusiatic 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.

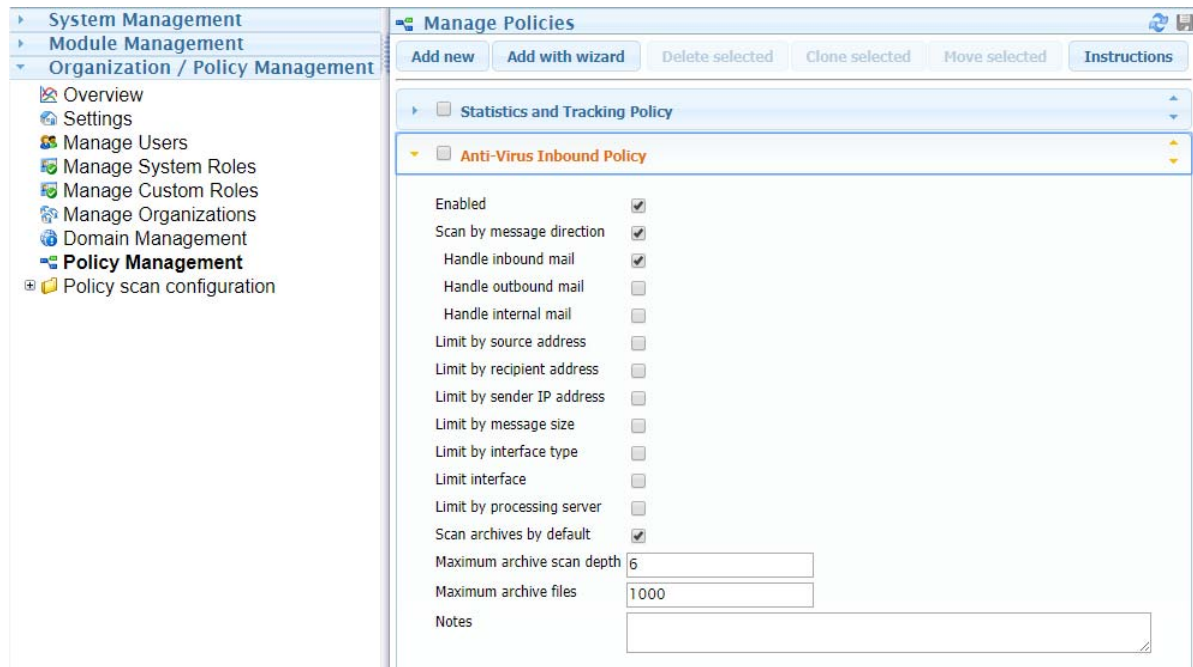
In this case, the Inbound Mail Filter Policy is a wizard created policy that deals with general spam, and malware. However, unwanted message are getting through and need to be dealt with.

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

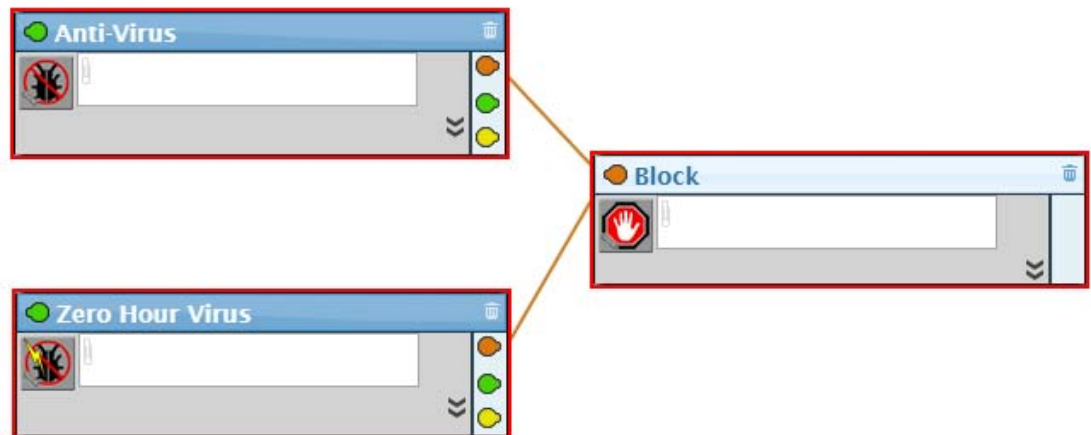
Open the panel and enable *Scan by message direction* then enable *Handle inbound mail*.



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.

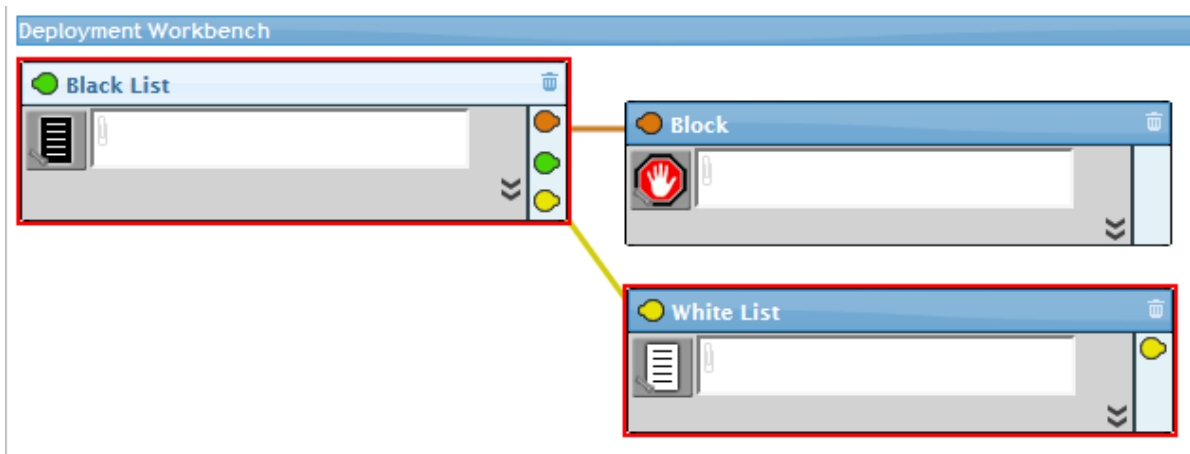
9. Connect the Red Services pin to the service with drop and drop.



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.

Black List

Black List Data Source [No data source] + 🔗

Ok Cancel

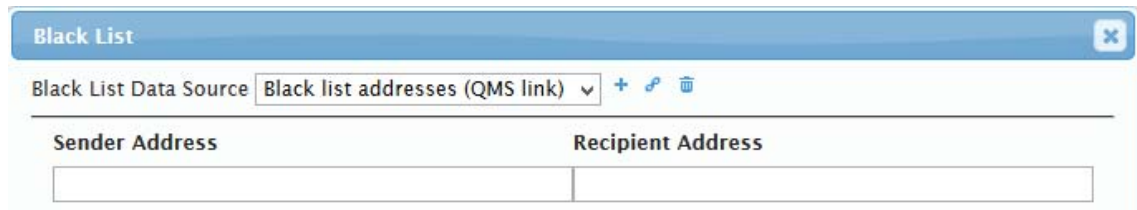
- From the Black List Data Source dropdown menu select a source or use the plus (+) button to create a data source. For example, "Black list addresses".

Black List

Black List Data Source Black list addresses + 🔗 🗑️

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

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



Black List

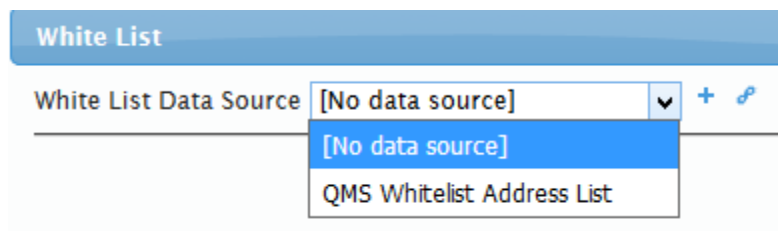
Black List Data Source: Black list addresses (QMS link) + 🔗 🗑️

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

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".

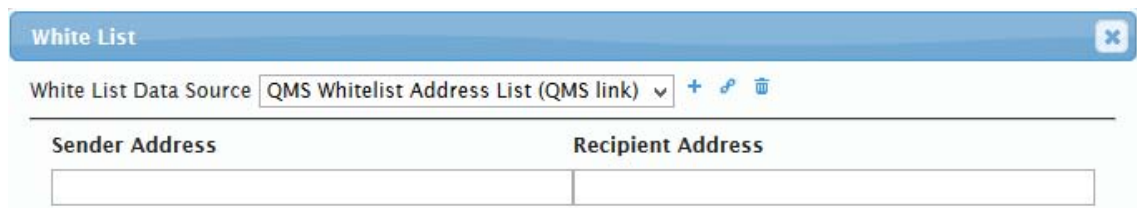


White List

White List Data Source: [No data source] + 🔗 🗑️

- [No data source]
- QMS Whitelist Address List

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.



White List

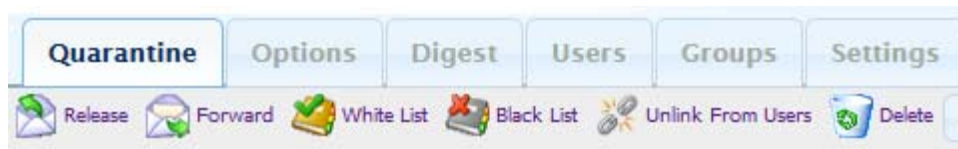
White List Data Source: QMS Whitelist Address List (QMS link) + 🔗 🗑️

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

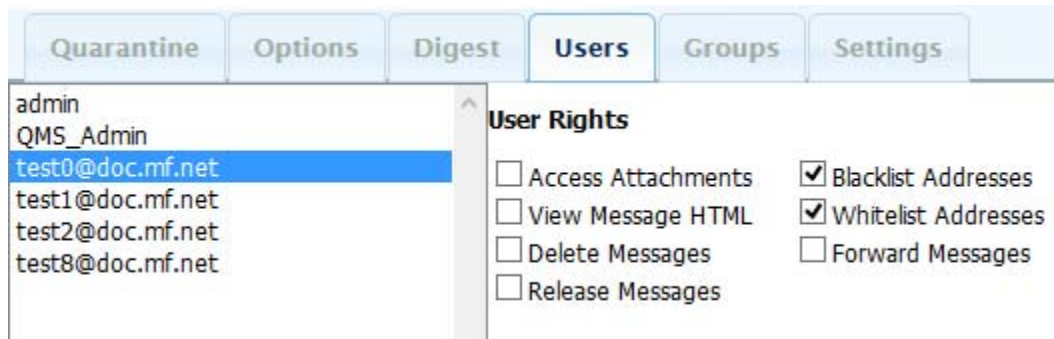
5. Sender and Recipient email addresses need to be added in pairs and can be added or removed in the configuration dialog box.
6. Press Ok.
7. Click the Save icon.

Black List and White List QMS Configuration

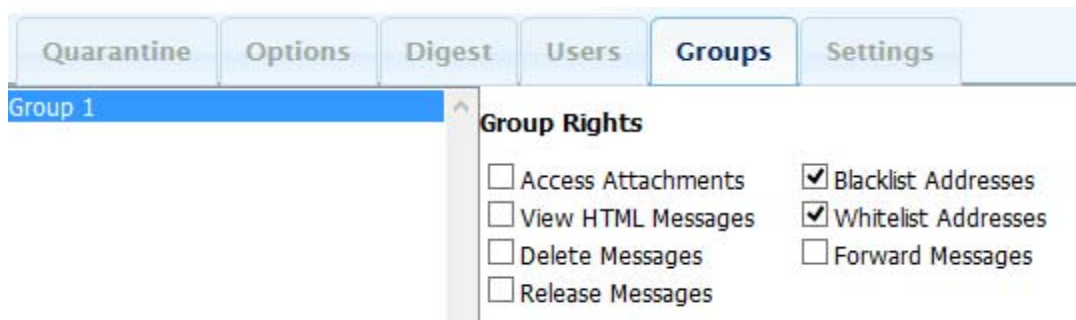
1. Log into the QMS as the System Administrator, or as a QMS Administrator with the 'Expose as QMS group' option enabled in Manage Custom Roles.
2. White list and Black list action buttons will appear in the Quarantine.



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

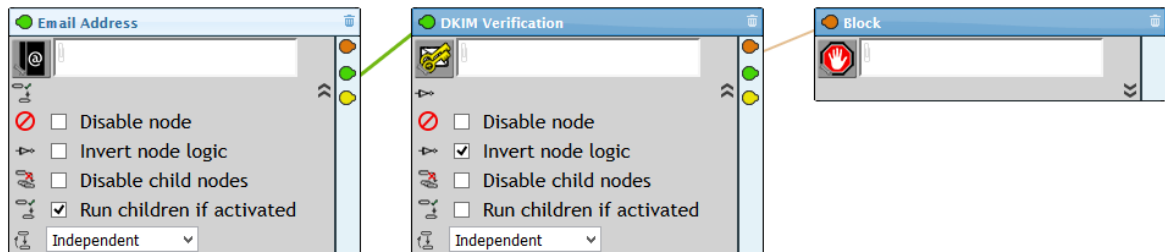
Unlike the typical filter in Secure Messaging Gateway, instead of looking for things to filter a message out by, this will filter searches for something to allow a message in. Depending on the use case the "Invert mode logic" switch may be needed. For more information on DKIM please see [OpenDKIM.org. \(http://opendkim.org/\)](http://opendkim.org/)

Blocking Messages Without a Valid DKIM Signature

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

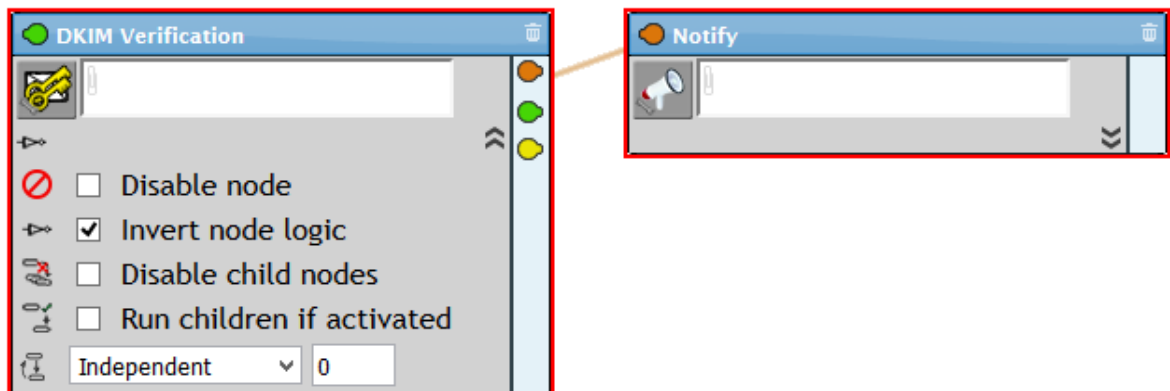
1. If you know that a sending domain applies DKIM signatures to all of their outbound email, you can define a rule chain to protect against spoofed email attempts of that domain. This setup will start with an email address filter connected to a child DKIM filter, followed by a block service connected 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 \(http://opendkim.org/\)](http://opendkim.org/).

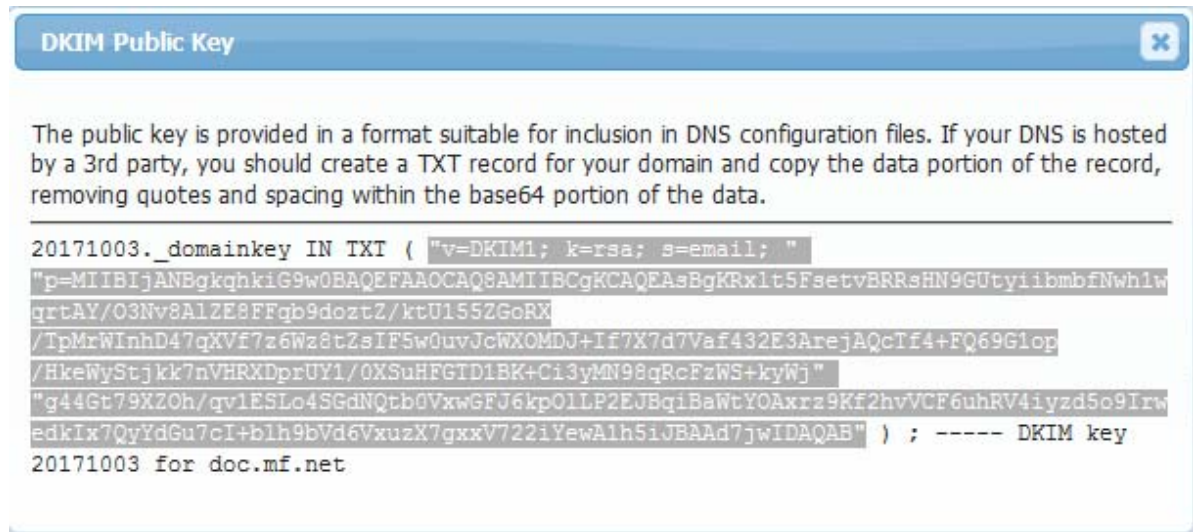
Prerequisites

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:



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:

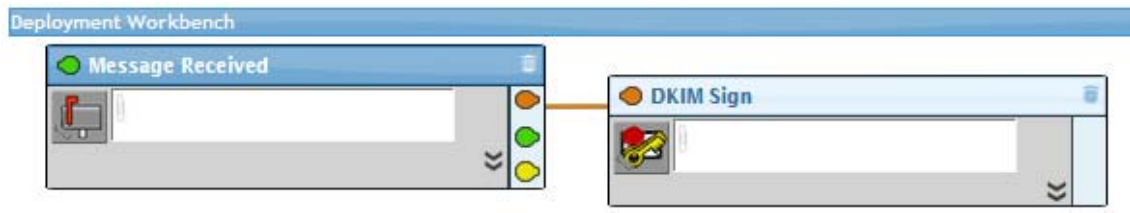
20171003._domainkey.doc.mf.net.

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=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsBgKRxlt5FsetvBRRsHN9GU
tyiibmbfNwhlwqrtAY/O3Nv8AlZE8FFqb9doztZ/ktU155ZGoRX/
TpMrWInhd47qXVf7z6Wz8tZsIF5w0uvJcWxOMDJ+If7X7d7Vaf432E3ArejAQcTf4+FQ69
Glop/HkeWyStjkk7nVHRXDprUY1/
0XSuhFGTD1BK+Ci3yMN98qRcFzWS+kyWj " "q44Gt79XZOh/
qv1ESLo4SGdNQtb0VxwGFJ6kp0lLP2EJBqiBaWtY0Axyz9Kf2hvVCF6uhRV4iyyzd5o9Irw
edkIx7QyYdGu7cI+blh9bVd6VxuzX7gxxV722iYewAlh5iJBAAAd7jwIDAQAB"

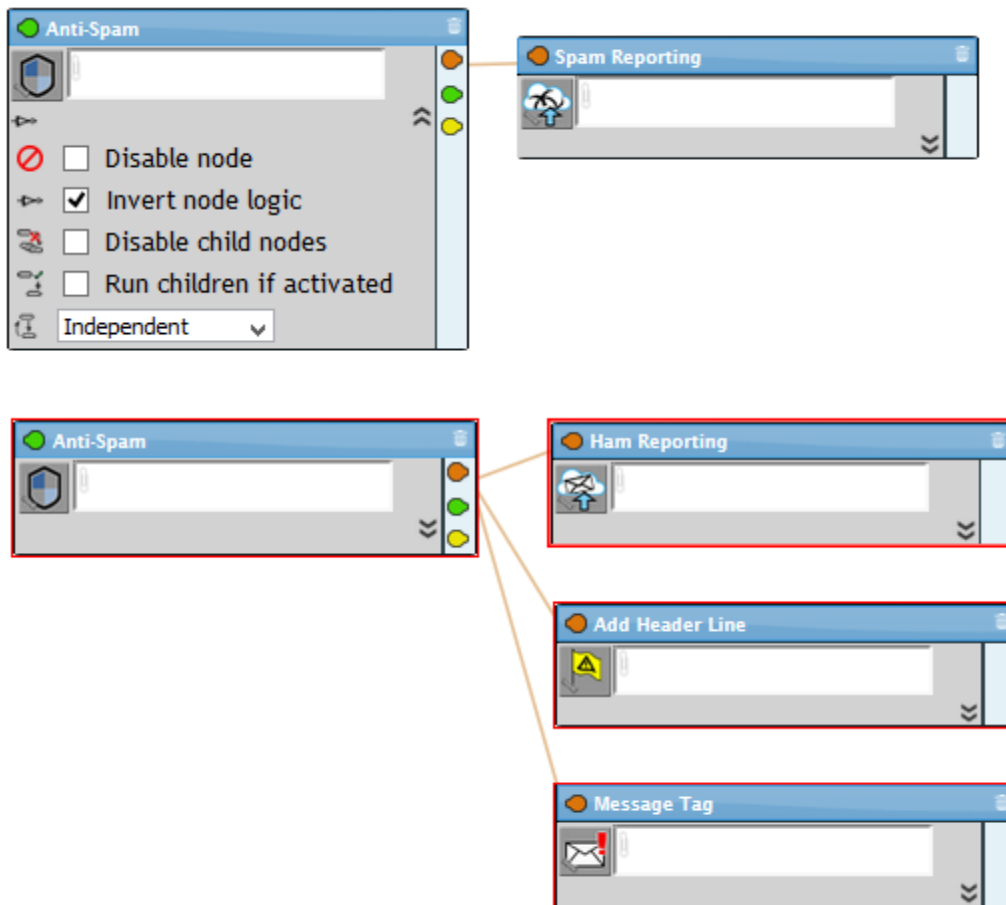
3. Finally, you need to create a DKIM signing service in Secure Messaging Gateway, either in an existing policy or in its own policy. No other configuration is necessary. In this example all mail will have DKIM signatures added. More sophisticated filters can be created if only some emails should be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

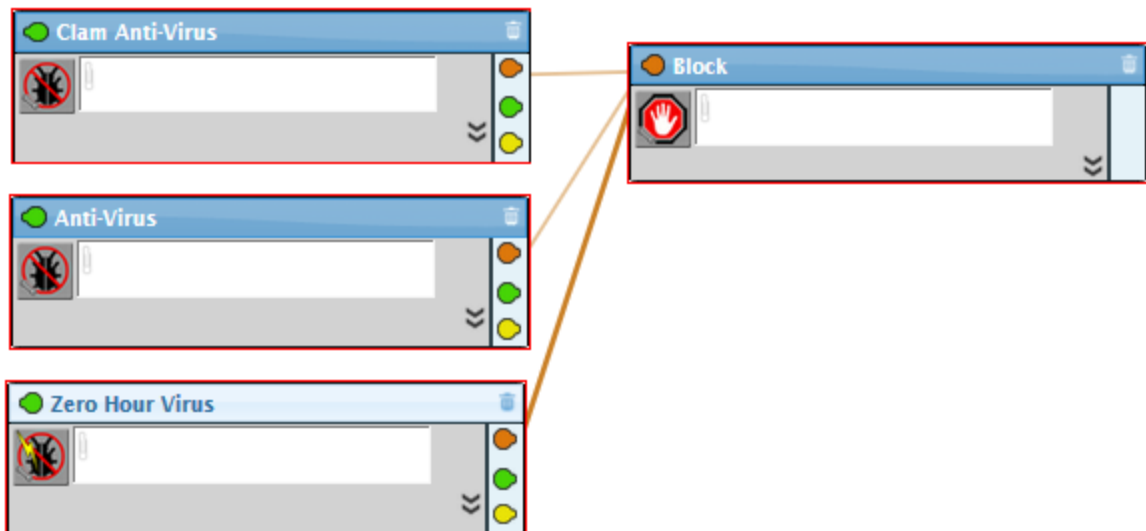
Ham Reporting

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 167](#).



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.

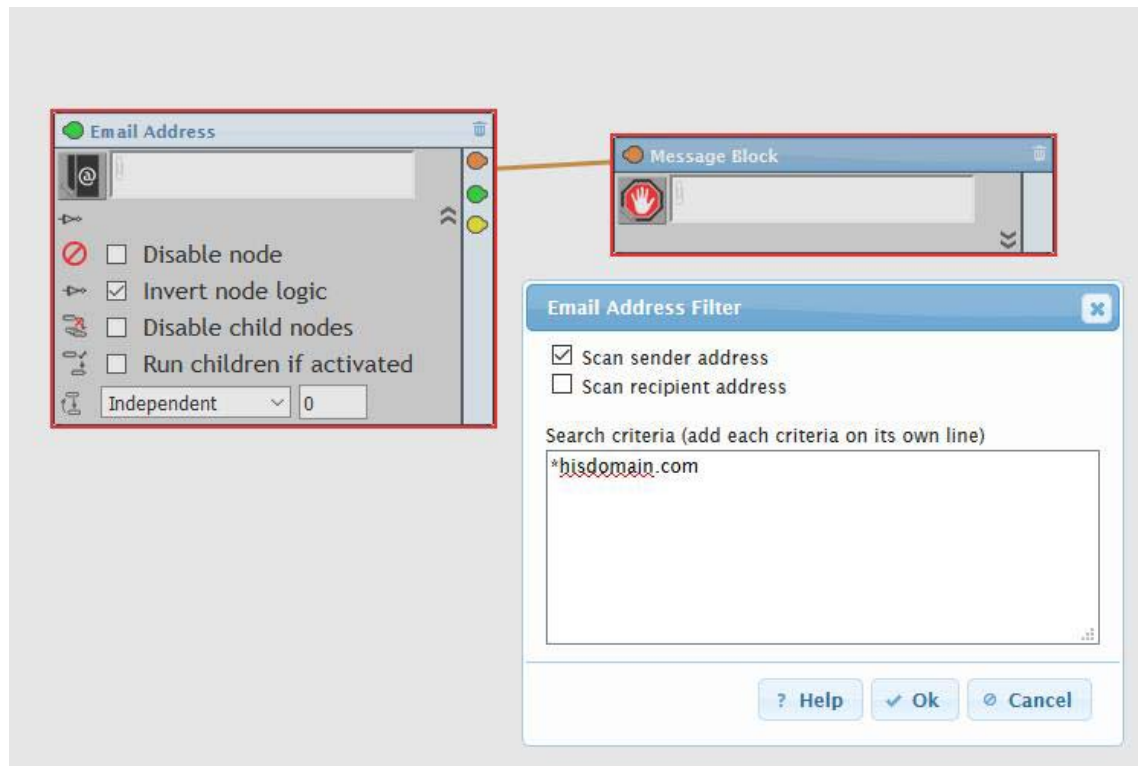
Go to the System Administration console | Organization \ Policy Management | Domain Management and set the domain to the fully qualified domain name of your email server.

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.



8 Quarantine System

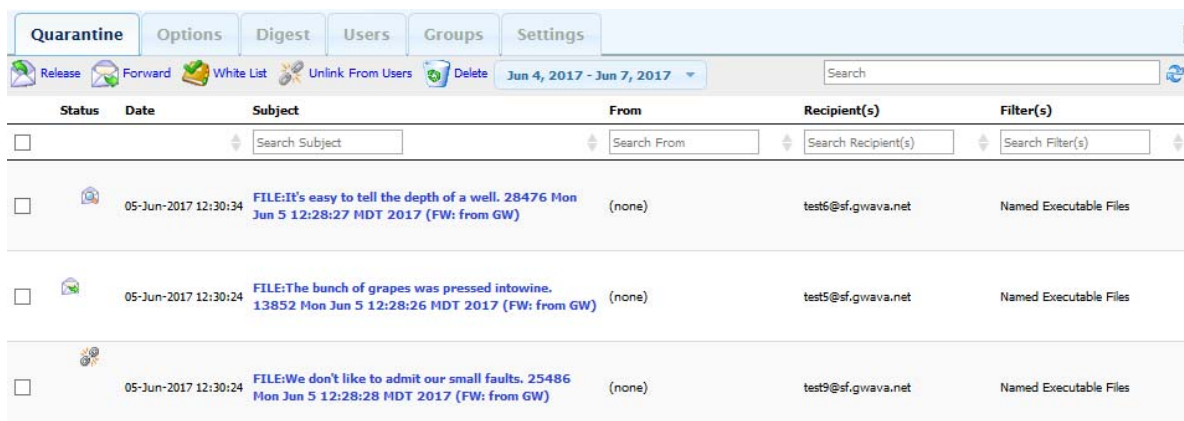
The quarantine is where suspicious messages are stored until someone can deal with them or they are removed because they have been in quarantine too long.

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.



Quarantine						
Options Digest Users Groups Settings						
Release Forward White List Unlink From Users Delete Jun 4, 2017 - Jun 7, 2017 Search						
Status	Date	Subject	From	Recipient(s)	Filter(s)	
<input type="checkbox"/>		Search Subject	Search From	Search Recipient(s)	Search Filter(s)	
<input type="checkbox"/>	05-Jun-2017 12:30:34	FILE:It's easy to tell the depth of a well. 28476 Mon Jun 5 12:28:27 MDT 2017 (FW: from GW)	(none)	test6@sf.gwava.net	Named Executable Files	
<input type="checkbox"/>	05-Jun-2017 12:30:24	FILE:The bunch of grapes was pressed intowine. 13852 Mon Jun 5 12:28:26 MDT 2017 (FW: from GW)	(none)	test5@sf.gwava.net	Named Executable Files	
<input type="checkbox"/>	05-Jun-2017 12:30:24	FILE:We don't like to admit our small faults. 25486 Mon Jun 5 12:28:28 MDT 2017 (FW: from GW)	(none)	test9@sf.gwava.net	Named Executable Files	

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



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

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

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

Show 20 messages

Showing 1 to 1 of 1 messages

First Previous 1 Next Last

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

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

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

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

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

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

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

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

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

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

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

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

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

April 2017
May 2017
June 2017

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

Apply
Clear
Cancel

Quarantine Options

The Options tab provides access to setting information.

Core Settings

Core Setting are the user definable options available.

Quarantine
Options

Core Settings
White List
Rights
Owned Addresses
Delegated Access

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

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.

The screenshot shows the 'White List' tab within the 'Options' section of the Quarantine System. The interface includes a navigation bar with tabs for 'Quarantine', 'Options', 'Digest', 'Users', 'Groups', and 'Settings'. Below this, a sub-navigation bar contains 'Core Settings', 'White List', 'Black List', 'Rights', 'Owned Addresses', and 'Delegated Access'. A message states: 'Mail from addresses that match the sender and recipient pairs in the white list will bypass all filters associated with the quarantine white list.' There are 'Delete' and 'Add' buttons. Below these are search fields for 'From' and 'To'. A message indicates 'There are no addresses in the white list'. At the bottom, there is a 'Show 10 entries' dropdown and a pagination control showing 'Showing 0 to 0 of 0 entries' with 'First', 'Previous', 'Next', and 'Last' links.

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.

The screenshot shows the 'Rights' tab within the 'Options' section of the Quarantine System. The navigation bar is the same as in the White List screenshot. The sub-navigation bar highlights 'Rights'. The main content area is titled 'RIGHTS' and contains the text 'Your rights define what you can do in the quarantine.' Below this is a list of rights: 'Release', 'Forward', 'Delete', and 'Whitelist'. A 'Rights' button is visible on the left side of the list.

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*.

The screenshot shows a web interface for managing owned addresses. At the top, there are tabs: 'Quarantine', 'Options', 'Core Settings', 'White List', 'Rights', 'Owned Addresses' (which is selected), and 'Delegated Access'. Below the tabs, the title 'Owned Addresses' is displayed. A paragraph explains that these are e-mail addresses considered part of the user's identity. Below this, there are two bullet points: 'Remove any of these email addresses' and 'Add additional addresses, if you can authenticate with the email address. (If you cannot authenticate, your quarantine administrator may add them for you)'. There are 'Delete' and 'Add' buttons. Below these is a table with a header 'Address' and one row containing a checkbox and the email 'test1@doc.mf.net'. At the bottom, there is a 'Show 10 entries' dropdown and a pagination bar showing 'Showing 1 to 1 of 1 entries' with links for 'First', 'Previous', '1', 'Next', and 'Last'.

Delegated Access

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

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

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

Grant/revoke additional rights to the delegate user:

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

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

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

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

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

Quarantine

Options

Core Settings

White List

Rights

Owned Addresses

Delegated Access

Delegated Access

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

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

Delete

Add

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

Show 10 entries

Showing 1 to 1 of 1 entries

First

Previous

1

Next

Last

Quarantine Digest

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

Settings Tab

	Quarantine	Options	Digest	Users	Groups	Settings
	Settings		Schedule	Manual Release		
Enable global digest services	<input checked="" type="checkbox"/>					
Contact email address	<input type="text" value="alpha@sf.gwava.net"/>					
Digest Template	<input type="text" value="Digest (en)"/> ▼					
Preferred digest language	<input type="text" value="English (en)"/> ▼					
Maximum digest rows	<input type="text" value="50"/>					
Custom digest action address	<input type="text"/>					
Digest recipients	<input type="text" value="Send digest to all users"/> ▼					
Custom address list	<div><div></div><div>Remove selected ✖</div><div>Add new ➕</div></div>					

Enable digest services: Default, disabled.

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

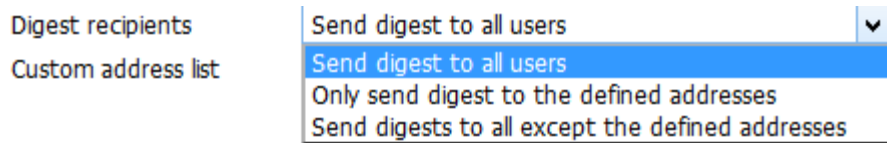
Digest Template: The default template selected in **System Administration | System Management | Templates**. Default, Digest (en).

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

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

Custom digest action address:

Digest recipients: The recipients that should receive digest emails.



- ♦ Send digest to all users (Default)
- ♦ Only send digest to the defined addresses
- ♦ Send digest to all except the defined addresses

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

Schedule Tab

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

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

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

Manual Release Tab

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


Quarantine
Options
Digest
Users
Groups
Settings

Settings
Schedule
Manual Release

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 ▾ 13 ▾ 00 ▾ [Set](#)

Custom digest release

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

Start date  22 ▾ Feb ▾ 2018 ▾ 13 ▾ 00 ▾

End date  22 ▾ Feb ▾ 2018 ▾ 13 ▾ 24 ▾

Select users:

☒

admin
QMS_Admin
test0@doc.mf.net
test1@doc.mf.net
test2@doc.mf.net
test8@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.

The screenshot displays the 'Users' tab in a web interface. On the left, a list of users is shown: 'admin', 'QMS_Admin', 'test0@doc.mf.net' (highlighted), 'test1@doc.mf.net', and 'test2@doc.mf.net'. The main area is divided into three sections: 'User Rights', 'User Options', and 'Group Membership'. The 'User Rights' section contains six checkboxes: 'Access Attachments', 'View Message HTML', 'Delete Messages', 'Release Messages', 'Blacklist Addresses', and 'Whitelist Addresses'. The 'User Options' section includes four settings: 'Maximum number of messages returned from a search' (set to 'All'), 'Number of messages per page' (set to '20'), 'Number of days to search' (set to 'Last 3 days'), and 'Inactivity Timeout' (set to '10'). The 'Group Membership' section is currently empty.

Quarantine	Options	Digest	Users	Groups	Settings
User Rights					
<input type="checkbox"/> Access Attachments					
<input type="checkbox"/> View Message HTML					
<input type="checkbox"/> Delete Messages					
<input type="checkbox"/> Release Messages					
<input type="checkbox"/> Blacklist Addresses					
<input type="checkbox"/> Whitelist Addresses					
<input type="checkbox"/> Forward Messages					
User 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					
Group Membership					

User Rights

System Administrator or QMS Administrator users can modify these rights.

Access Attachments

View Message HTML

Delete Messages

Release Messages

Blacklist Addresses

Whitelist Addresses

Forward Messages

User Options

Maximum number of messages returned from a search

100

200

500

1000

All (Default)

Number of messages per page

10

20 (Default)

50

100

All

Number of days to search

Last 24 hours

Last 2 days

Last 3 days (Default)

Last 7 days

Last 30 days

Inactivity Timeout: Default 10 minutes.

Group Membership

The list of groups the user is a member of.

Quarantine Groups

Users can be organized into Groups to make management easier.

The screenshot shows the 'Groups' tab selected in a navigation bar with tabs for Quarantine, Options, Digest, Users, Groups, and Settings. On the left, 'Group 1' is selected. The main area is divided into two sections: 'Group Rights' and 'Group Members'. 'Group Rights' includes checkboxes for 'Access Attachments', 'View HTML Messages', 'Delete Messages', 'Release Messages', 'Blacklist Addresses', 'Whitelist Addresses', and 'Forward Messages'. 'Group Members' includes checkboxes for 'admin', 'QMS_Admin', 'test0@doc.mf.net', 'test1@doc.mf.net', and 'test2@doc.mf.net'.

Groups are created by the System Administrator as a Custom Role [“Creating a Group”](#) on page 103.

Quarantine Settings

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

The screenshot shows the 'Settings' tab selected in a navigation bar with tabs for Quarantine, Options, Digest, Users, Groups, and Settings. Below the tabs are three sub-tabs: 'Default User', 'Message Retention', and 'Forward From Quarantine'. The 'User Interface Options' section contains four settings: 'Maximum number of messages returned from a search' with a dropdown set to 'All', 'Number of messages per page' with a dropdown set to '20', 'Number of days to search' with a dropdown set to 'Last 3 days', and 'Inactivity Timeout' with a text input set to '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

The screenshot shows a web interface for configuring message retention. At the top, there is a navigation bar with tabs: Quarantine, Options, Digest, Users, Groups, and Settings. Below this is a sub-navigation bar with tabs: Default User, Message Retention (which is selected), and Forward From Quarantine. The main content area is titled "Message Retention Policy" and contains four settings:

- Enable quarantine message pruning: ☒
- Days to retain messages in quarantine:
- Prune message information: ☒
- Delete stored messages: ☒

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



The screenshot shows a web interface with a top navigation bar containing tabs: Quarantine, Options, Digest, Users, Groups, and Settings. Below this is a sub-navigation bar with tabs: Default User, Message Retention, and Forward From Quarantine. The 'Forward From Quarantine' tab is selected. The main content area is titled 'Forward From Quarantine' and contains two settings:

- 'Forward as an attachment template' with a dropdown menu showing 'Forward From Quarantine (en)'.
- 'Preferred forward as an attachment language' with a dropdown menu showing '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.

Jun 19, 2017							Search
Date	Subject	Sender	Recipient(s)	Direction	Block State	Sending IP Address	
Date	Search Subject	Search Sender	Search Recipient(s)	Search Direction	Search Block State	Search Sending IP Address	
19-Jun-2017 12:34:44 pm	A blue crane is a tall wading bird. 478685461	script@sf.gwava.net	test7@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:34:22 pm	His hip struck the knee of the next player. 1988893851	script@sf.gwava.net	test9@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:34:00 pm	The goose was brought straight from the old market. 1462980723	script@sf.gwava.net	test8@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:33:38 pm	Screen the porch with woven straw mats. 1170864218	script@sf.gwava.net	test5@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:33:27 pm	The sand drifts over the sills of the old house. 376325950	script@sf.gwava.net	test6@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:33:05 pm	Go now and come here later. 423062554	script@sf.gwava.net	test4@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:32:43 pm	The marsh will freeze when cold enough. 1002658249	script@sf.gwava.net	test3@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:32:21 pm	Port is a strong wine with a smoky taste. 840402094	script@sf.gwava.net	test1@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:31:59 pm	Take shelter in this tent, but keep still. 238750082	script@sf.gwava.net	test2@doc.mf.net	internal	none	151.155.183.142	
19-Jun-2017 12:31:37 pm	A six comes up more often than a ten. 1636634308	script@sf.gwava.net	test0@doc.mf.net	internal	none	151.155.183.142	
Show 10 messages							
Showing 1 to 10 of 424							Print Copy CSV Excel PDF Column visibility
							First Previous 1 2 3 4 5 ... 43 Next Last

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

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

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

Column visibility can be selected under the button.



Search

Each column can be searched individually.

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

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

Jun 19, 2017 Tire

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

Show 10 messages

Showing 1 to 5 of 5 (filtered from 424 total messages) Print Copy CSV Excel PDF Column visibility First Previous 1 Next Last

Date Range

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

Jun 19, 2017

[Today](#)
[Yesterday](#)
[This week](#)
[Last week](#)
[This month](#)
[Last month](#)
[This year](#)

April 2017

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

May 2017

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

June 2017

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

Apply

Clear

Cancel

Message Details

Click on a message to bring up a details dialog box. The policy and filters that triggered on the message will be shown.

Message Details

Date:

19-Jun-2017 11:34:47 am

Subject:

Press the pants and sew a button on the vest. 308825513

Sender:

script@sf.gwava.net

Policy:

Inbound Mail Filter Policy

Recipients:

test8@doc.mf.net

Filters:

IN Message Received

Message Text

10 SMTP Authentication

The SMTP AUTH functionality of SMG provides the ability to elevate SMTP client privileges based on their authenticated state. This allows for tiered mail delivery options based on the knowledge of access credentials by an incoming SMTP client connection.

There are a multitude of ways, reasons and goals that SMTP authentication can be used for, depending on the needs and layout of an email system.

Without any configuration, SMTP AUTH does not provide any inherent advantages to a client that logs in to the SMG server. The privileges that are afforded to authenticated users are provided through various configuration parameters that link to the authenticated state of the SMTP session. How the authentication service is used is entirely dependent on the needs of each individual mail system. SMG does not dictate which privileges any user might receive after authenticating. Use this guide to determine what SMG can provide to authenticated users, and configure your system according to your needs.

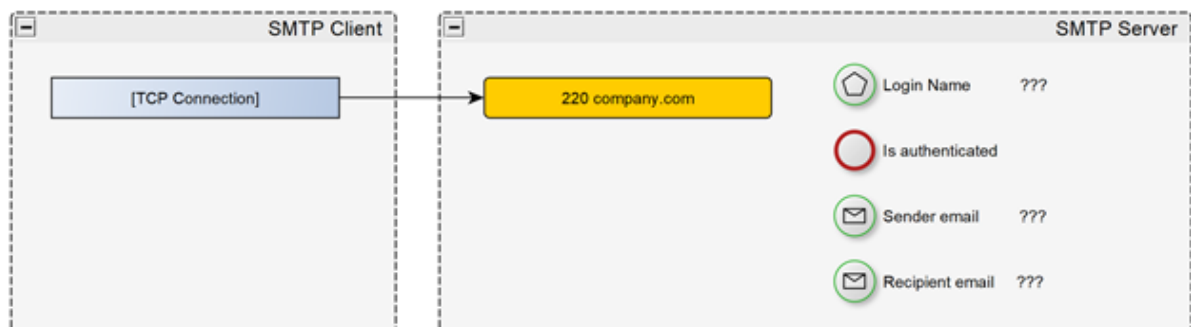
- ♦ [“Introduction” on page 201](#)
- ♦ [“SMTP Authentication Settings” on page 203](#)
- ♦ [“Configuration Scenarios” on page 214](#)

Introduction

It is helpful to understand the context of SMTP authentication in the context of an SMG server when configuring a system. It can be confusing to determine what parts of the system are interacting with authenticated privileges compared to email addresses provided in the MAIL FROM and RCPT TO commands of the SMTP protocol.

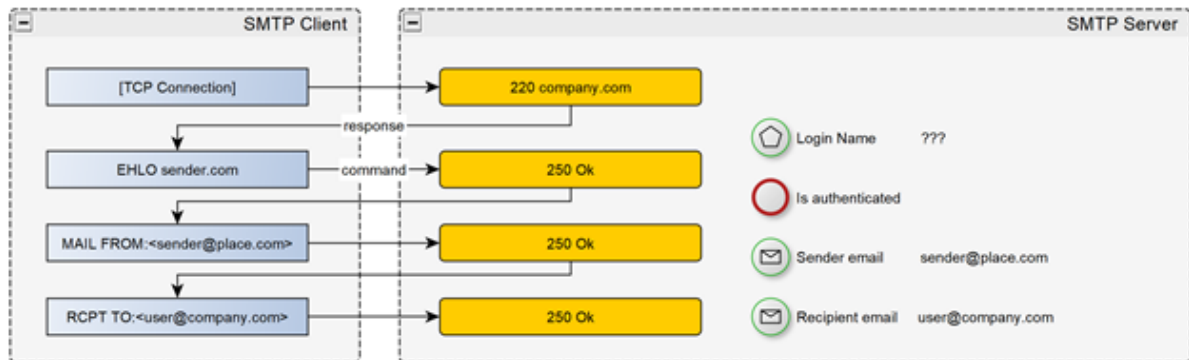
The following diagrams show the conversation between an SMTP client and server, and what pieces of information are picked up during the conversation by the server process.

When an SMTP client connects, the server knows the IP address of the incoming connection, and nothing more. In the first diagram here, the client has connected to the server, and it has no information about authentication or delivery addresses.



In the second diagram, a typical inbound message transaction is taking place. No authentication is performed, and the sender and recipient email addresses are provided. After these commands, the server has enough information to determine how to deliver the message that will be provided.

Pay attention to the server response to the EHLO command. The response does not advertise AUTH to the client. The client must not try to authenticate when AUTH is not in the initial response, and the server will not accept attempts to try it, reporting an invalid command if it is attempted.

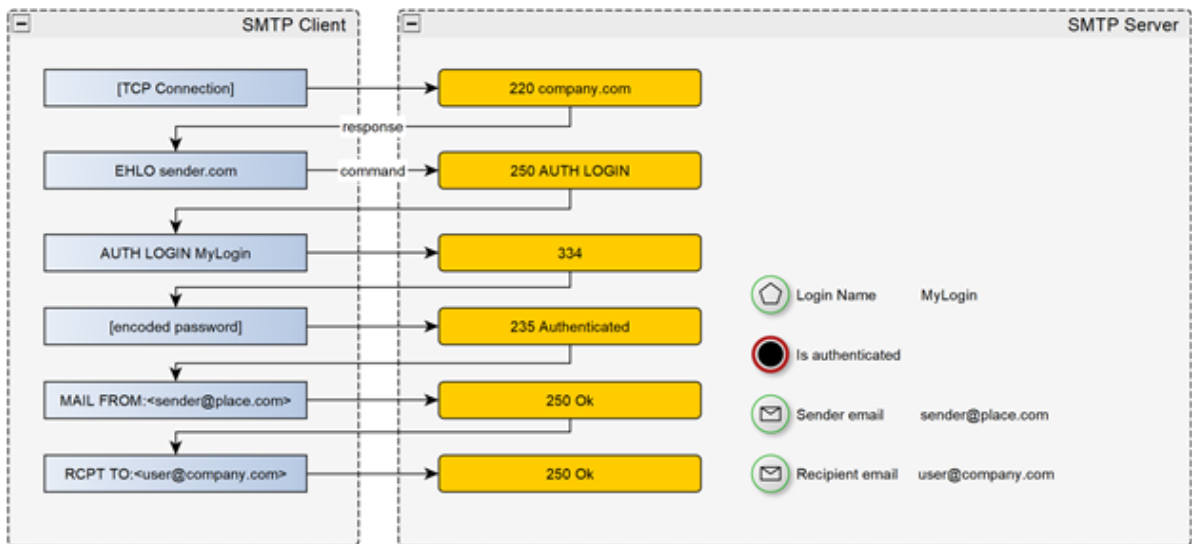


The third diagram shows the state of an authenticating SMTP client. In this case the client issues a LOGIN command along with its credentials. At the end of the addressing process, the server now has two additional pieces of information – a login name and an authenticated state.

There are some very important concepts to understand about this diagram and what it demonstrates.

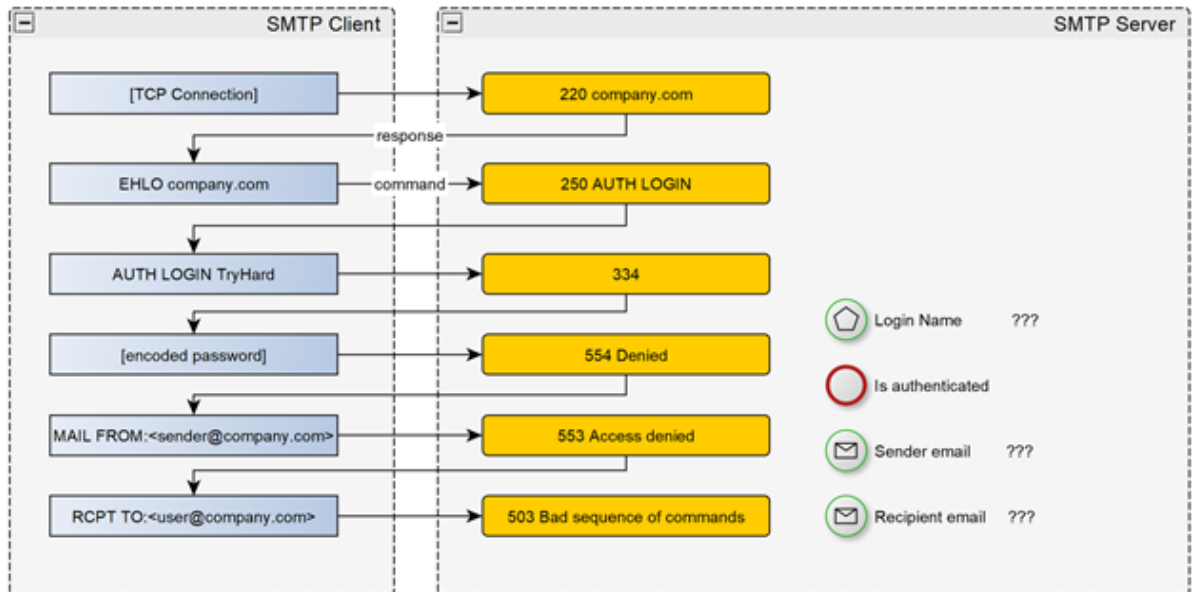
The login name may or may not match the sender email address, depending on what functionality the SMTP server provides and how it implements authentication. The privileges that are given when successfully authenticated are also not necessarily related to the sender address. They may be linked in some way, but they are not referring to the same internal information. The key point here is that when configuring rules, such as exceptions and allow/deny lists, you need to know which property you are configuring. Allowing a login name is NOT the same as allowing a sender email address, from the SMTP server perspective. Allowing AUTH names acts on the AUTH command, while allowing sender addresses acts on the MAIL FROM command.

In the authenticated state, additional privileges may be afforded to the sender, for example they may now be allowed to send messages from the mail servers internal domain name. These privileges are not automatically assumed by SMG, and must be configured based on the individual system needs.



The next image gives an insight into the state of SMG when an SMTP client fails to authenticate, but subsequently tries to brute force the sending of a message using a spoofed address (pretending to be from company.com in this example).

In this case, because the authentication fails, the internal properties remain undefined and all commands fail from this point on, preventing spoofing of the email address that is provided in the MAIL FROM command.

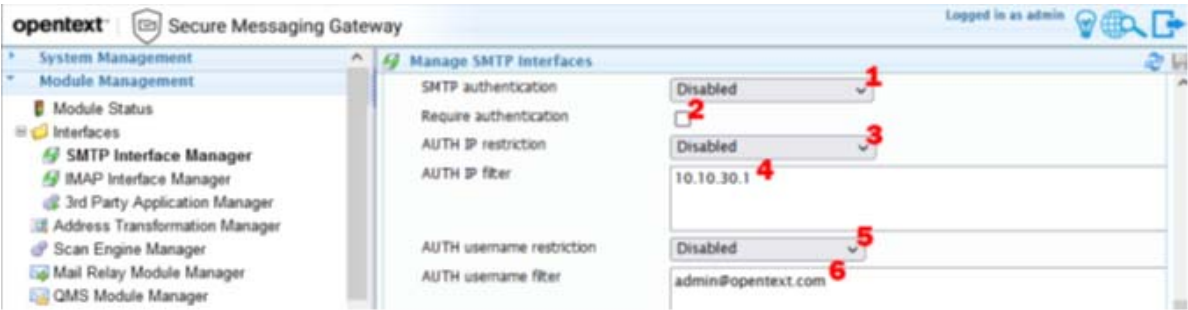


SMTP Authentication Settings

This section describes all of the individual SMTP authentication settings.

Interface Settings

These settings are applied to all SMTP connections regardless of the OU that the email addresses belong to. These settings require admin privileges to define.



Setting	Description	Value(s)
1 - SMTP authentication	Determines the availability of SMTP authentication on this SMTP interface.	<ul style="list-style-type: none">♦ Disabled: Authentication is disabled on the SMTP interface.♦ Enabled: Authentication is enabled on the SMTP interface.♦ Enabled when encrypted: Authentication is enabled for encrypted connections on the SMTP interface. Encryption is enabled by connecting to the SSL server or by switching to encrypted mode with the STARTTLS command.
2 - Require authentication	Determines if authentication is required for sending messages.	<ul style="list-style-type: none">♦ Enabled: SMTP clients must authenticate to be able to send messages. Attempting to send mail without authenticating is rejected.♦ Disabled: SMTP client do not need to be authenticated to send email.

Setting	Description	Value(s)
3 - AUTH IP restriction	Sets the enabled state for AUTH IP filter . Use this option to restrict/allow SMTP clients from accessing the AUTH command by their connecting IP address.	<ul style="list-style-type: none"> ♦ Disabled: IP address filtering is inactive. ♦ Allow IP addresses in list: Only the IP addresses listed in AUTH IP filter are able to use SMTP AUTH (Whitelist). ♦ Deny IP addresses in list: Only the IP addresses not listed in AUTH IP filter are able to use SMTP AUTH (Blacklist).
4 - AUTH IP filter	Entries in the list are give access to or denied access to SMTP authentication based on the setting in AUTH IP restriction .	Accepts IP addresses, CIDR formatted addresses, wildcards, and regexes.
5 - AUTH username restriction	Sets the enabled state for AUTH username filter . Use this option to restrict/allow specific usernames from using SMTP authentication.	<ul style="list-style-type: none"> ♦ Disabled: Username filtering is inactive. ♦ Allow usernames in list: Only the username listed in AUTH username filter are able to use SMTP AUTH (Whitelist). ♦ Deny usernames in list: Only the usernames not listed in AUTH username filter are able to use SMTP AUTH (Blacklist).
6 - AUTH username filter	Entries in the list have their credentials validated or ignored based on the setting in AUTH username restriction .	Accepts plain email addresses, wildcards, and regexes.

IMPORTANT: The following options should only be enabled if you fully understand the consequences of what you are turning on. Blindly enabling these options can lead to disastrous results to your ability to send email, possibly causing listing on blacklists. Relaying is defined as a message that is from a sender outside your system, to a user outside your system.



Setting	Description
7 - Allow relay if authenticated (global)	This settings allows any user that has authentication to relay mail via SMG.
8 - Allow authenticated OU relay	<p>This set of checkboxes enables relaying for individually selected OU's, and interacts with the authenticated state of users from those OU's. When a sender claims to be from an SMG defined domain, but has not authenticated, they are considered external for the purpose of determining relaying status.</p> <p>NOTE: Configuration of relaying is not provided within an OU itself, as this poses a risk to the entire mail system if a tenant is allowed to open up relaying, whether deliberately or by mistake.</p>

OU Level Settings

These settings are applied to SMTP connections based on the OU of the sender email address. These settings can be set by OU administrators, and as a result, are restricted in scope to affect only the addresses matching domains within the OU.

It is very important to understand how the scoping works in these settings. These rules always take the sender email address into consideration when decisions are computed. If one of these settings is not working as you expect, you should check the sender domain to see if it is 'owned' by the OU. If the sender is from a different domain than those defined for the OU, then none of the authentication settings will have any effect.

If applicable to your system, typically in single OU systems, it is normally better to define any equivalent settings at the interface. The rules at the interface can be computed earlier in the SMTP transaction. OU level rules need to receive the email addresses before rule conformance can be determined.

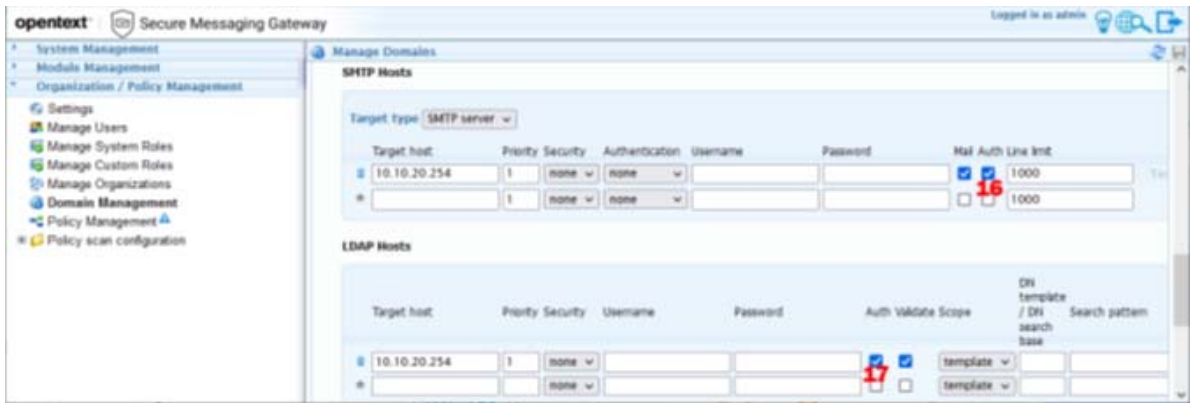


Setting	Description	Value(s)
9 - Require inbound SMTP domain authentication	<p>This setting determines the authentication requirements for SMTP clients that issue a MAIL FROM command for this domain and a RCPT TO command for this domain. For example, if the domain identity is 'opentext.com', and the SMTP client issues the commands 'MAIL FROM:<sender@opentext.com>' and 'RCPT TO:<recip@opentext.com>', this setting becomes valid. In the same case, if the SMTP client issues the command 'MAIL FROM:<user@external.com>', then the setting becomes redundant.</p> <p>The test for authentication requirement is computed when the client issues the RCPT TO command.</p>	<ul style="list-style-type: none"> ♦ Not Required: Senders from this domain do not need to be authenticated to send to this domain. ♦ Required when SMTP interface AUTH is enabled: Authentication is required according to the conditions mentioned in the description if SMTP Authentication is enabled on the SMTP interface. ♦ Required always: Authentication is required according to the conditions mentioned in the description. <p>NOTE: Depending on how your mail system is implemented, this setting can be used to require authentication even if AUTH is not enabled. This can be used to prevent address spoofing, due to the inability of a client being able to authenticate. The result of this is that all attempts to spoof mail will fail.</p>

Setting	Description	Value(s)
10 - Require SMTP Sending domain authentication	<p>Determines whether authentication is required for clients that send a MAIL FROM command for any domains defined within this OU.</p> <p>This setting is similar to Require inbound SMTP domain authentication, differing only in the scope of the restriction. This setting only tests the MAIL FROM command for conformance to the rule, which is more restrictive.</p>	<ul style="list-style-type: none"> ◆ Enabled: SMTP clients that claim to be from a domain within this OU must authenticate to be able to send messages. All attempts to send mail without authenticating will be rejected. ◆ Disabled: The setting has no effect.
11 - Match AUTH user with FROM address	<p>When enabled, the email address provided in the MAIL FROM command must match the authenticated username.</p> <p>Using this option prevents internal users from sending messages on behalf of other users.</p> <p>This setting applies to all automatically provisioned addresses for the domain, and to internal users of the domain that are configured for Enable for SMTP Auth.</p> <p>The comparison is case insensitive. I.e. ADMIN@company.com will match admin@company.com.</p>	

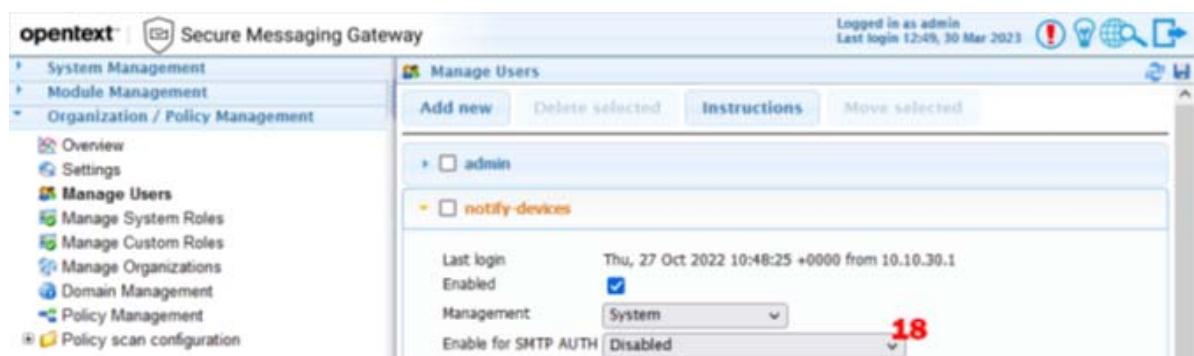
Setting	Description	Value(s)
12 - SMTP IP authentication exception mode	<p>Works in conjunction with SMTP IP authentication exceptions to define IP address exceptions to AUTH requirements. If entries exist in SMTP IP authentication exceptions, exceptions are activated. An empty list in SMTP IP authentication exceptions deactivates the exception mode.</p> <p>Where an SMTP client would have its RCPT TO command rejected due to authentication requirements, this setting overrides the rejection if the connecting IP address matches an entry in SMTP IP authentication exceptions.</p> <p>The core purpose of this setting is to allow senders from specific IP addresses to send from this domain into the SMG system, bypassing anti-spoofing measures that have been configured.</p>	<ul style="list-style-type: none"> ♦ Allow: The addresses in the SMTP IP authentication exceptions list are not subjected to authentication based addressing restrictions. ♦ Deny: Addresses that do not match the SMTP IP authentication exceptions list are not subjected to authentication based addressing restrictions.
13 - SMTP IP authentication exceptions	A list of IP address matches used by SMTP IP authentication exception mode .	The formate of addresses may be raw IP address, CIDR format, wildcards, or regexes.

Setting	Description	Value(s)
14 - SMTP AUTH username restriction	<p>Works in conjunction with SMTP AUTH username filter to restrict the names that can be used for SMTP authentication.</p> <p>During the SMTP AUTH command, the given username is compared to the entries in the SMTP AUTH username filter. If the entry matches, the authentication verification proceeds. If the entry does not match, the authentication attempt is ignored and the authentication attempt is rejected.</p> <p>It is important to understand that the username referred to in this feature is the authenticating username (AUTH command), and not the sender address (MAIL FROM). Although the authenticating username and sender email address are commonly the same, this is just coincidental. Confusing these details can lead to expectation problems in what the address restriction is applying to.</p>	<ul style="list-style-type: none"> ◆ Disabled: Authentication restrictions will not be applied. ◆ Allow usernames in list: <p>Entries that match the authenticating user that belongs to this OU will be allowed to authenticate.</p> ◆ Deny usernames in list: <p>Entries that do not match the authenticating user that belongs to this OU will be allowed to authenticate.</p>
15 - SMTP AUTH username filter	<p>A list of pattern matches used by SMTP AUTH username restriction.</p> <p>The username that is tested against this list must belong to the OU that the rule is defined, by way of address formatted usernames. If a restricted address belongs to a different OU, it will not match this list. For example, defining anybody@* in an OU that hosts the domain company.com will match anybody@company.com, but not anybody@widgets.com.</p>	<p>The format of entries in this list may be plain text, wildcards or regexes.</p>

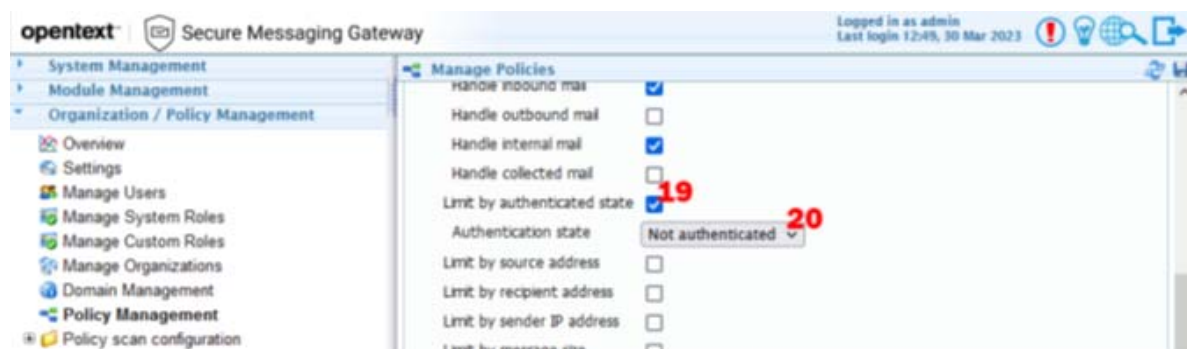


Setting	Description
16 - SMTP target host Auth passthrough	<p>To perform automated authentication for users on your email system, this checkbox tells SMG that it can use this host to perform login tests against an SMTP server.</p> <p>When an SMTP client attempts to authenticate to the SMG SMTP server, SMG will lookup the authenticating username. The internal SMG user database is looked up first, and if not found, and the authentication username is an email address, then SMG will look up the OU database for a matching domain. If the username belongs to a domain, and an SMTP target host is configured with the 'Auth' checkbox enabled, SMG will contact the SMTP server and test the credentials against the SMTP server to verify the user.</p> <p>NOTE: Authentication, username and password fields of the domain SMTP hosts are unrelated to client authentication validation. Making changes to those fields will have no effect on SMTP client authentication (They are used for sending email to the server if it requires authentication for mail delivery).</p>

Setting	Description
17 - LDAP target host Auth passthrough	<p>To perform automated authentication for users on your email system, this checkbox tells SMG that it can use this host to perform login tests against an LDAP server.</p> <p>When an SMTP client attempts to authenticate to the SMG SMTP server, SMG will lookup the authenticating username. The internal SMG user database is looked up first, and if not found, and the authentication username is an email address, then SMG will look up the OU database for a matching domain. If the username belongs to a domain, and an LDAP target host is configured with the 'Auth' checkbox enabled, SMG will contact the LDAP server and test the credentials against the LDAP server to verify the user.</p> <p>NOTE: The username and password fields of the domain LDAP hosts are unrelated to client authentication validation. Making changes to those fields will have no effect on SMTP client authentication (They are used for user validation if required to gain privileges on the LDAP server).</p>



Setting	Description	Value(s)
18 - Enable for SMTP Auth	<p>Internal SMG users can be configured to be used in the SMTP authentication process. By default, this setting is off. The setting will be unavailable if the management mode is set to 'Domain provisioning', which indicates that the user was auto-generated and will be authenticated remotely to the configured target system.</p> <p>This setting is useful to provide a single user name that can be used to grant privileges to send email within your system without needing to have the user exist in your email system.</p> <p>A typical use case for this feature is for devices such as printers that use email for notification. For convenience, a single username can be used for all devices on the network.</p>	<ul style="list-style-type: none"> ♦ Disabled: This user cannot be used for SMTP authentication. ♦ Enabled for any sender address: This user can be used for authentication, and can issue a MAIL FROM command using any email address permitted by the OU. Addressing permissions for the OU are defined by the parent OU, ensuring that permission elevation cannot be self-assigned. ♦ Enabled for matching sender address: This user can be used for authentication, and it may only issue a MAIL FROM command that matches the user name. For this functionality to work, the username must be an email address. Address matches are case insensitive.



Setting	Description
19 - Limit by authenticated state	Enable this option in a policy criteria to determine whether the policy should be used, based on the authenticated state of the connecting client.
20 - Authentication state	Select the authenticated state of the message being scanned to decide whether to use this policy.

Configuration Scenarios

Authentication can be used for a variety of purposes. This list provides some common use-cases for SMTP authentication, along with the configuration settings needed to set to enable the functionality. You may configure authentication with any combination of these settings depending on the needs of your system.

Email Address Spoofing Prevention

Address spoofing occurs when the sender of an email claims to be someone else, and particularly when the sender claims to be from the domain of the system they are sending a message into. This allows a malicious sender to pretend to be a user from your domain, gaining the trust of the target recipient who is unaware that the sender is not the same person that created the message.

There are a variety of ways to prevent address spoofing, each of which depend on the way your email system is implemented.

Proof of identity

The most obvious and common way to stop spoofing is to require proof of identity. The sender needs to know the username and password of a valid user to be able to gain sender privileges from your domain.

To enable this method, set the following configuration items:

- ♦ **Enable SMTP AUTH** (1) to turn authentication services on at the SMTP interface, preferably 'when encrypted'.
- ♦ **Require inbound SMTP domain authentication** (9) set to 'Required always'. This setting requires authentication when messages sent to your domain that are also from your domain. It does not require messages from a different domain to authenticate.
- ♦ **Match AUTH user with FROM address** (11). It's usually a good idea to enable this setting to prevent internal user masquerading or malware generated messages that have hijacked some of a user's credentials.

Interface separation

If possible, creating separate SMTP interfaces for public mail and private mail can simplify spoof prevention a lot.

SMG can run multiple SMTP interfaces, binding to different IP addresses and/or ports. With multiple interfaces, it's easy to define specific requirements for users connecting to the different interfaces. You can define a public interface to not allow authentication, and a private interface to require authentication. This both prevents attackers from using the public interface in any type of malicious authentication attempt, and also prevents users from trying to authenticate to the public interface, which can inadvertently leak credentials. The only users that can identify as being from your domain are required to authenticate on that interface.

A typical setup using this method is as follows:

- ♦ Create an SMTP interface intended for public consumption
 - ♦ Set **SMTP AUTH** (1) to disabled.
 - ♦ Enable **Require SMTP sending domain authentication** (10). This setting requires senders from your domain to authenticate, but they cannot do so due to SMTP AUTH being disabled. This combination of settings prevents any sender from claiming to be from your domain.
- ♦ Create a second SMTP interface intended for private consumption.
 - ♦ This interface may listen on the same IP address with a different port, or another IP address, depending on your internet options. It is common practice to setup this service on port 587, known as the 'message submission' port. Ensure **STARTTLS** is enabled for the interface for secure connections.
 - ♦ Set **SMTP AUTH** (1) to enabled, preferably when encrypted.
 - ♦ Enable **Require authentication** (2). This setting forces all senders coming in through this interface to be authenticated to send mail.
 - ♦ Enable **Match AUTH user with FROM address** (11). It is usually a good idea to enable this setting to prevent internal user masquerading or malware generated messages that have hijacked some of a users credentials.

VPN access

If applicable to your environment, using the interface separation method previously described, the private interface can be secured by a VPN, further reducing the possibility of any kind of identity spoofing.

Simplified Filter Control

Generally, an authenticated connection can be trusted as being a valid user of the system. As a trusted user it often makes sense to apply a different set of filtering rules to these users. A couple of good examples of this are the spam filter, which should not be relevant to messages from users of your system, and notifying the administrator of viruses sent from local users.

Using the policy system on conjunction with authentication, we can utilize the policy manager to create separate policies for authenticated users and unauthenticated users.

There are a myriad of configuration combinations that can be used to achieve this setup, with the most basic being as follows:

- ♦ Enable **SMTP AUTH** (1) to turn authentication services on at the SMTP interface, preferably **when encrypted**.
- ♦ **Require inbound SMTP domain authentication** (9) set to **Required always**. This setting requires authentication when messages sent to your domain that are also from your domain. It does not require messages from a different domain to authenticate.
- ♦ **Match AUTH user with FROM address** (11). It's usually a good idea to enable this setting to prevent internal user masquerading or malware generated messages that have hijacked some of a user's credentials.

- ♦ Create a policy, sorted at the top of your policy list, and enable the authentication criteria (settings 19/20).
- ♦ Apply appropriate filters for your users to the new policy.

External Relay

If you allow users to use email client apps that connect via SMTP into your email system, relaying off your server may be something that you allow them to do. Relaying is defined when the sender and recipient of an email routed through your server are not part of the local domain. We can consider unauthenticated users to not be part of your domain, because we don't trust they are valid, especially when the connection comes from outside the network.

Using authentication allows us to create a trust with the connecting client.

To provide relay services to your external users, configure these settings:

- ♦ Enable **SMTP AUTH** (1) to turn authentication services on at the SMTP interface, preferably **when encrypted**.
- ♦ **Require inbound SMTP domain authentication** (9) set to **Required always**. This setting requires authentication when messages sent to your domain that are also from your domain. It does not require messages from a different domain to authenticate.
- ♦ **Match AUTH user with FROM address** (11). It's usually a good idea to enable this setting to prevent internal users masquerading or malware generated messages that have hijacked some of a user's credentials.
- ♦ Enable **Allow relay if authenticated (global)** (7) on the SMTP interface (or limit it to an OU depending on your system needs).

Targeted User/Address Authentication

SMG provides a mechanism to allow specific SMTP connections the ability to authenticate. The use case for this configuration is where your email users connect directly to your email server, bypassing SMG, and SMG protects the email system by receiving messages coming from external users.

With this email topology, there can be situations where you have specific remote networks that need to send messages from the outside into your system via SMTP.

Normally to host these specific external systems, auth can be used to protect the system, however it also opens up authentication to all users that are able to login to the system.

To solve this problem, SMG provides a slew of settings for filtering the inbound connections by email and IP addresses (settings 3/4/5/6/12/13/14/15). With authentication enabled, use the settings from this list to isolate the systems that should be allowed to gain authenticated access.

Using this method provides isolation of specific user access to the system, and it also protects your target host server by only passing through authentication requests for the users or connection addresses that are granted access.

Shared Login

Where you have devices and applications in your network that require an email delivery service, it can be convenient to have a shared authentication username that all of the managed devices and applications can use.

Using an internally defined SMG user, you can provide these devices the privileges they need to send mail via SMG.

- ♦ Enable **SMTP AUTH** (1) to turn authentication services on at the SMTP interface, preferably 'when encrypted'.
- ♦ Add an SMG user and enable the appropriate AUTH method (setting 18).
- ♦ Configure the device/application with the email server and login credentials of the SMG server.

The privileges afforded to the device will be dependent on the other authentication settings defined.

11 User Guide

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 thing like black list email addresses that you know are bad and white list email addresses you know are good.

Quarantine Management System

The OpenText 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 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.

The screenshot shows the 'Micro Focus Secure Gateway' interface. At the top, a blue banner reads 'E-Mail Restriction Report' and '3 messages were quarantined from 10-Jan-2018 to 10-Jan-2018'. Below this, a message states: 'The e-mail listed below were quarantined by Secure Messaging Gateway and may be unsolicited (SPAM)'. A button labeled 'Manage my quarantine' is visible. A table lists the quarantined messages with columns: Reason, Subject, Sender, Date, and Action. The first row shows a message quarantined due to 'Attachment Size', 'Email Address', and 'Message Received' from 'NBC-Simpson Shares Her Surprising Weight Loss Details' sent by 'email@domain.com' on '10 Jan 2018 01:08:17 PM'. The 'Action' column for this message includes links for 'Release', 'Whitelist', and 'Blacklist'. At the bottom, there is a copyright notice for 2016 GWAVA, Inc., a Micro Focus Company.

Reason	Subject	Sender	Date	Action
Attachment Size Email Address Message Received	NBC-Simpson Shares Her Surprising Weight Loss Details	email@domain.com	10 Jan 2018 01:08:17 PM	Release Whitelist Blacklist

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.

Micro Focus® Secure Gateway



Login name

Password



Login

Login help





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

Micro Focus® Secure Gateway

Logged in as test0@doc.mf.net
Last login 15:40, 29 Jun 2017





QuarantineOptions



Aug 8, 2017 - Aug 11, 2017

Search



Status	Date	Subject	From	Filter(s)
<input type="checkbox"/>		<div>Search Subject</div>	<div>Search From</div>	<div>Search Filter(s)</div>
<input type="checkbox"/>	11-Aug-2017 15:37:58	A list of names is carved around the base. 1767499012	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:37:37	Two plus seven is less than ten. 1026605505	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:37:16	The hitch between the horse and cart broke. 1917350973	script142@sf.gwava.net	Message Text
<input type="checkbox"/>	11-Aug-2017 15:36:54	A pod is what peas always grow in. 2119304128	script142@sf.gwava.net	Message Text

Quarantine Actions

From here you may take action on one or more of the quarantined emails. Select one or more messages using the checkbox on the right.



- ♦ *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.

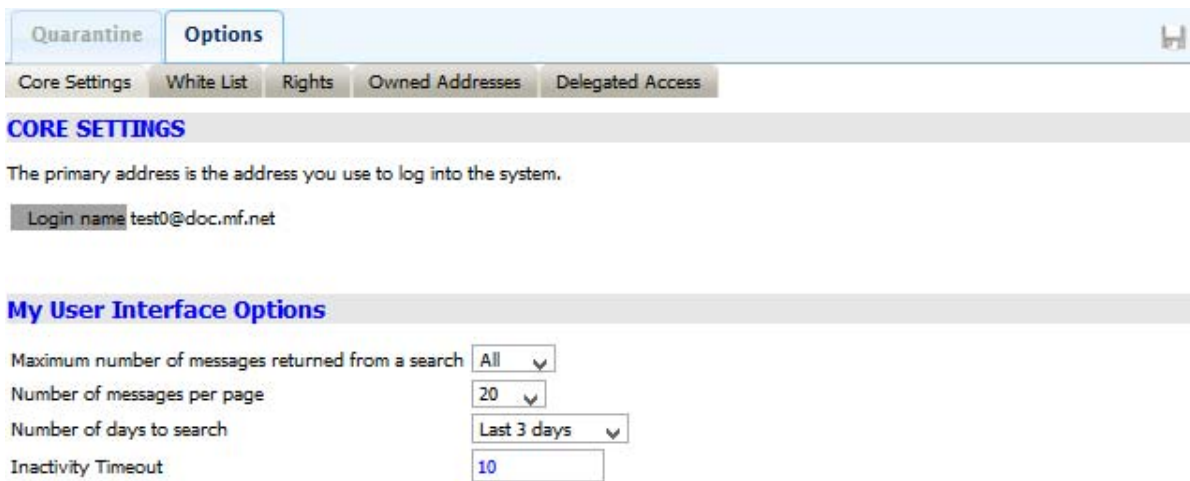
You can sort by the Date, Subject, From or Filter(s) column by clicking on the arrows

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.



Quarantine Options

Core Settings White List Rights Owned Addresses Delegated Access

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

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

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

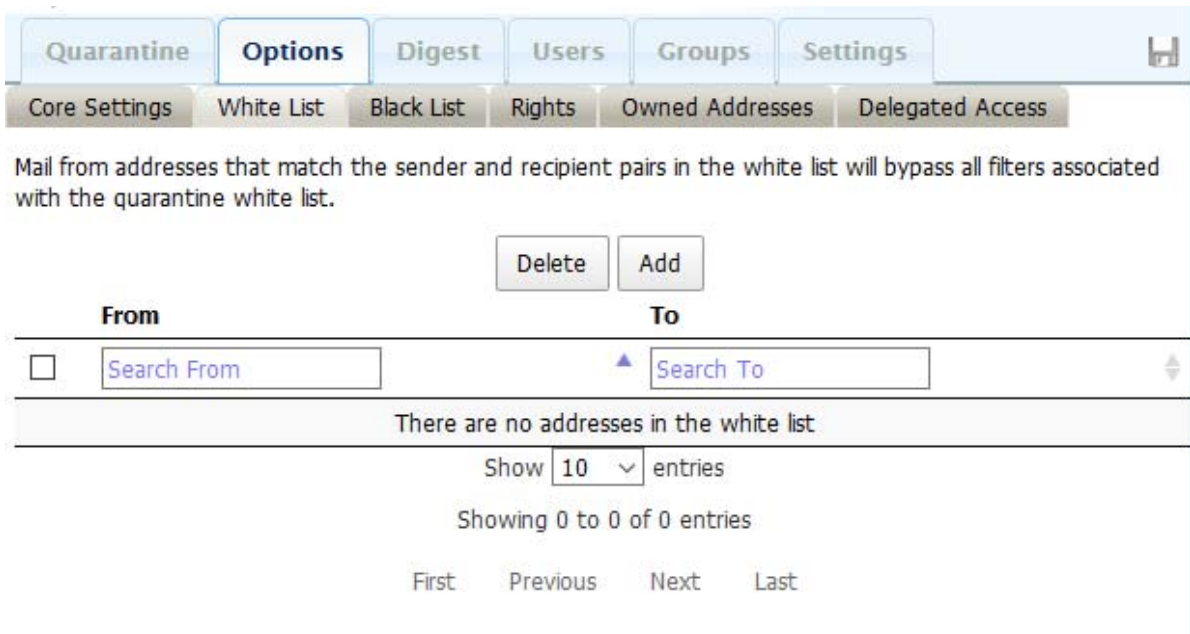
Number of messages per page. Default, 20.

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.



Quarantine Options Digest Users Groups Settings

Core Settings White List Black List Rights Owned Addresses Delegated Access

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

Delete Add

	From	To
<input type="checkbox"/>	<input type="text" value="Search From"/>	<input type="text" value="Search To"/>

There are no addresses in the white list

Show 10 entries

Showing 0 to 0 of 0 entries

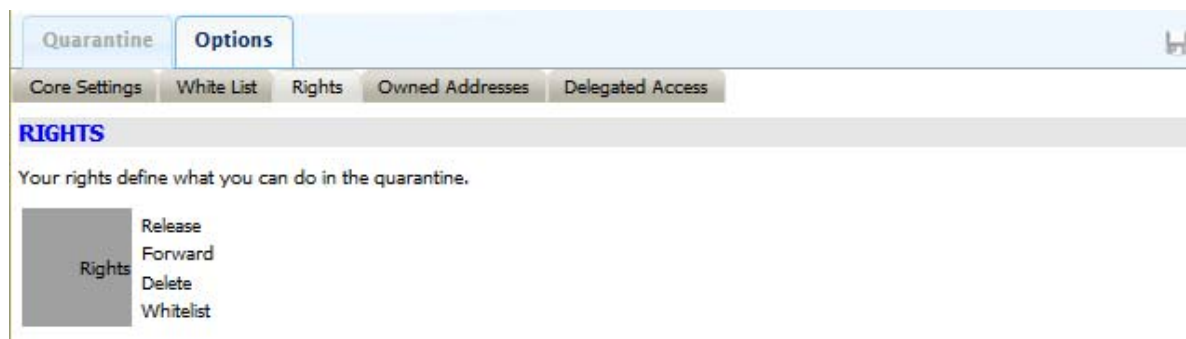
First Previous Next Last

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.



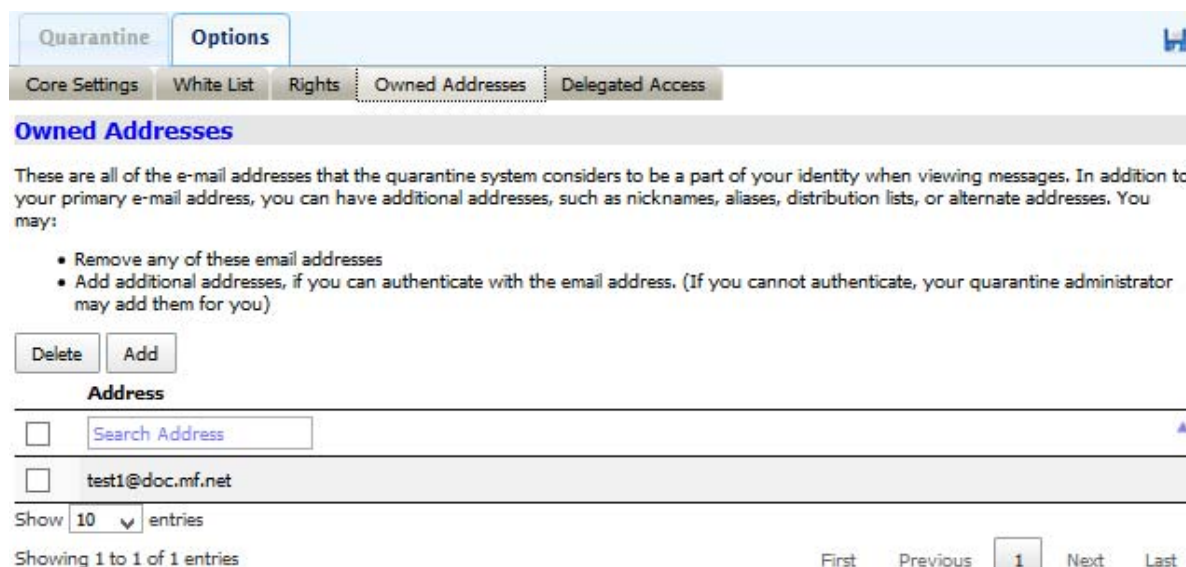
An Administrator user can change the rights granted in the *System Administration / Organization / Policy Management / Manage Users* page.

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 whilelist.

QuarantineOptions

Core SettingsWhite ListRightsOwned AddressesDelegated Access

Delegated Access

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

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

DeleteAdd

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

Show 10 entries

Showing 1 to 1 of 1 entries

First

Previous

1

Next

Last

12 Migrating Secure Messaging Gateway

- ♦ [“Migrating SMG from the Appliance to a New Server” on page 225](#)
- ♦ [“Migrating to SMG from Another Message Processing Product” on page 229](#)

Migrating SMG from the Appliance to a New Server

This section describes how to transfer your SMG system from the SMG appliance to a new server. The process may be used for a single server system or a node of a multi-server system.

Prerequisites and Considerations

- ♦ [“Prerequisites” on page 225](#)
- ♦ [“Time Requirements” on page 225](#)
- ♦ [“Assumptions” on page 225](#)
- ♦ [“Important Notes” on page 226](#)

Prerequisites

- ♦ A new SMG server. See [“Installing a New SMG Server” on page 226](#) for more information.

IMPORTANT: You must have the same (or more) CPU, RAM, and disk space on your new server as you do on your old server in order to run the migration.

- ♦ Shell access to the old and new SMG systems
- ♦ Root privileges on the old and new SMG servers
- ♦ Basic linux terminal commands knowledge such as listing files and setting file permissions

Time Requirements

Due to the nature of data stored in SMG, it is not possible to provide and estimate of how long the process will take. You can safely estimate this for your system while it is actively running by following the entire migration process without completing the final step of reassigning IP addresses. This will complete the migration, but the data will most likely not be synchronized, and the migration should not be considered valid. The time taken will be approximately the same as completing the entire process.

Assumptions

The source SMG system has no system level alterations that change the locations of files or the names of databases. Where changes exist, please ensure to adjust the process steps accordingly to conform to your system configuration.

Important Notes

- ♦ Older SMG systems that are not up to date may have different base paths than those specified.
- ♦ If the folder `/opt/opentext` does not exist on your system, replace this with `/vastorage` for the purpose of this document.
- ♦ You must have the same (or more) CPU, RAM, and disk space on your new server as you do on your old server in order to run the migration.

Migrating to a New Server

The migration process is completed by following these steps:

- ♦ [“Installing a New SMG Server” on page 226](#)
- ♦ [“Disabling SMG on Both Servers” on page 226](#)
- ♦ [“Transferring Internal Configuration Files” on page 227](#)
- ♦ [“Backing up Databases” on page 227](#)
- ♦ [“Backing Up Quarantine Data” on page 227](#)
- ♦ [“Transferring Backups and Restoring the Data” on page 228](#)
- ♦ [“Switching the IP Address” on page 228](#)

Installing a New SMG Server

Prepare and install a new SMG server. The server need to be configured to the point that you are able to login to the SMG administrations. Follow the steps in [“Installing SMG” on page 16](#) to install a new SMG server.

If you want to use the same DNS name for your new server, the new server should be given a temporary IP address and while you can migrate the data from the old system to the new system. The IP address on the new system will be changed at the end of the migration process to match the old system.

IMPORTANT: Passwords for the new system, including the database login, need to match the old server.

Disabling SMG on Both Servers

You need to disable the SMG on both the old and new servers to prevent data synchronization problems and corruption problems.

- 1 Shutdown the SMG application by running the following command on both servers:

```
service smg stop
```

- 2 Check that the services have stopped by running the following command:

```
service smg status
```

- 3 Once the system shows that the SMG services has stopped running, continue with [Transferring Internal Configuration Files](#).

Transferring Internal Configuration Files

- 1 Copy the following files/folders from the old server and set the permissions on the new server to be the same as the old server:

```
/opt/opentext/config/system.xml
/opt/opentext/msg/msg-supervisor/http_local (all files and folders in
this directory)
```

- 2 (Optional) If you have configured DKIM services, copy the following files as well:

```
/etc/opendkim/key.table
/etc/opendkim/signing./table
/etc/opendkim/keys (all files and folder in this directory)
```

- 3 (Optional) If you are using custom server certificates, copy them to the following location on the new server:

```
/opt/opentext/msg/conf/certs/
```

- 4 Continue with [Backing up Databases](#).

Backing up Databases

IMPORTANT: This steps is not required if the postgres database is hosted on a different server. Multi-node SMG systems only have a single master database server, so this step is not required on servers that do not host the database.

- 1 Run the following commands to backup all of the SMG databases to a temporary folder. You will move the dump files later.

```
pg_dump --format=p -U postgres SecureGateway > SecureGateway.dump
pg_dump --format=p -U postgres SecureGatewayStats >
SecureGatewayStats.dump
pg_dump --format=p -U postgres SecureGatewayTracker >
SecureGatewayTracker.dump
pg_dump --format=p -U postgres SecureGatewayQuarantine >
SecureGatewayQuarantine.dump
```

- 2 Continue with [Backing Up Quarantine Data](#).

Backing Up Quarantine Data

This is the majority of the data that is transferred to the new system. The recommended method of backing up this data is to zip up the files so they can be easily moved to the new server.

- 1 Run the following commands to zip up the files:

```
cd /opt/opentext/msg/msg-quarantine/data_store
zip -r qms-backup.zip *
```

- 2 Continue with [Transferring Backups and Restoring the Data](#).

Transferring Backups and Restoring the Data

- 1 Copy the database dump files and the `qms.backup.zip` file to the new server.
- 2 Move the `qms-backup.zip` file into the `/opt/opentext/smg/smg-quarantine/data_store` folder, and run the following commands:

```
cd /opt/opentext/smg/smg-quarantine/data_store
unzip -o qms-backup.zip
chown -R smg:smg *
```

- 3 Use the following commands to restore the databases:

NOTE: If an error occurs referencing the non-existence of a database, repeat the command without the `--clean` option, and then repeat the command again with the `--clean` option until no errors occur.

The `-h` and `-p` options assume the Postgres server is located locally and listening on the default port. If you receive error about connecting to the database, try removing both of these parameters, or adjust them to accomodate your server configuration.

```
pg_restore -h 127.0.0.1 -p 5432 --clean --create -U postgres -d
postgres SecureGateway.dump
pg_restore -h 127.0.0.1 -p 5432 --clean --create -U postgres -d
postgres SecureGatewayQuarantine.dump
pg_restore -h 127.0.0.1 -p 5432 --clean --create -U postgres -d
postgres SecureGatewayStats.dump
pg_restore -h 127.0.0.1 -p 5432 --clean --create -U postgres -d
postgres SecureGatewayTracker.dump
```

- 4 Continue with [Switching the IP Address](#).

Switching the IP Address

IMPORTANT: This step should be skipped if you are only evaluating how long the migration would take. Restart the services on your old SMG server to bring it back online until you are ready to perform the migration.

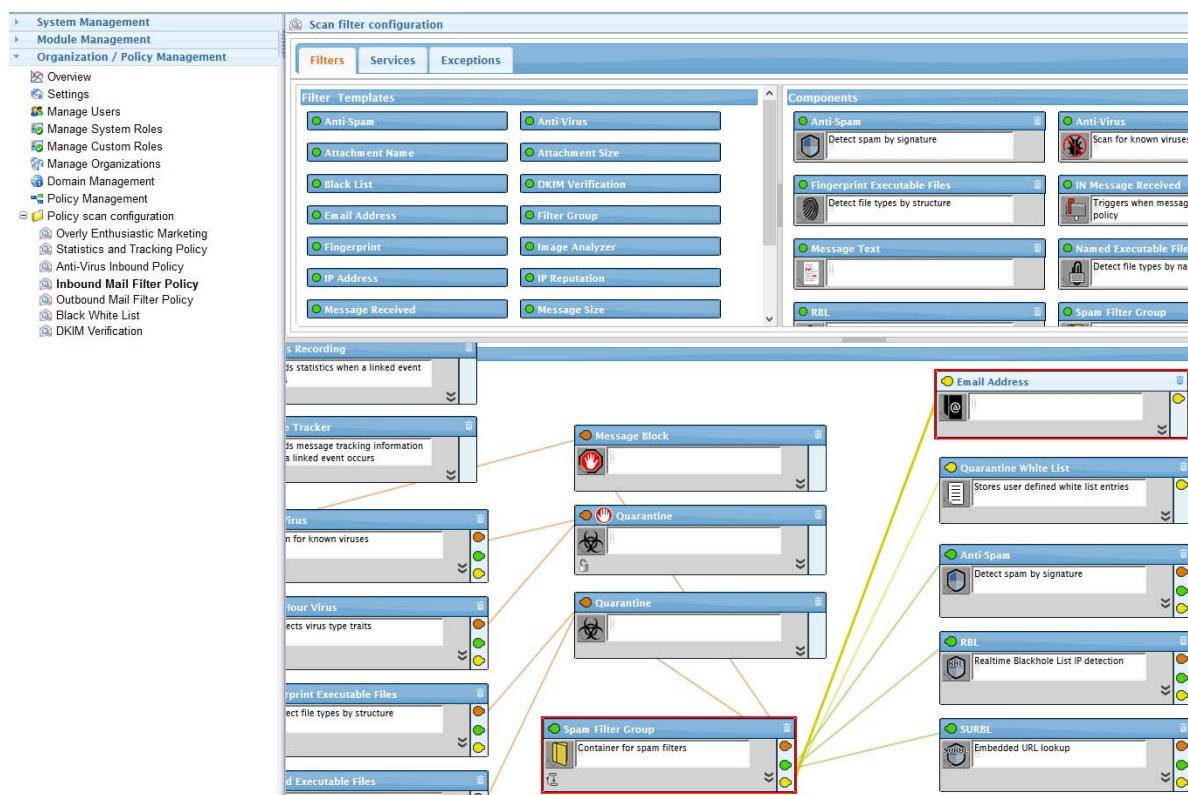
- 1 Change the IP address of the old server to a temporary IP address.
This allows access to content on that server in case anything was missed and needs to be brought over after the migration is complete.
- 2 Change the IP address of the new server to the original SMG IP address.
- 3 Restart the new SMG server to bring it online.
Your migration is complete and everything should be running as it was previously.
- 4 (Optional) If you are using custom certificates, on the new server, open the Management Interface and navigate to **Interface > SMTP** Interface Manager and change the path to the SSL certificates to `/opt/opentext/smg/conf/certs/`.

Migrating to SMG from Another Message Processing Product

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 117 or a Block and Quarantine with Exceptions policy “Creating a Block and Quarantine with Exceptions Policy” on page 162.

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



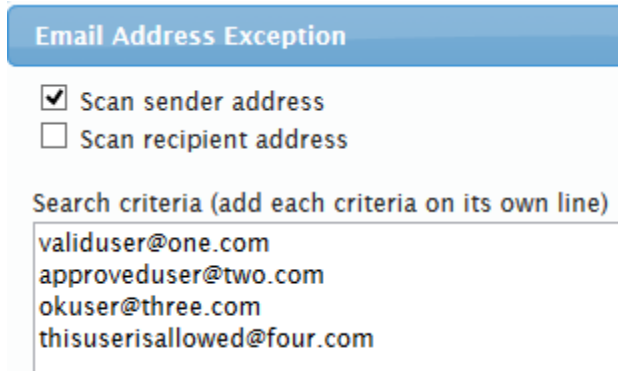
In this example, you will use an inbound mail filter policy and modify it to act as a system whitelist, which is different from a user’s personal whitelist.

1. Begin by creating a list of whitelist exceptions for this filter. Go to your old filter program and gather the list of system-wide allowed emails. Copy them to a text file, one email address on each line with no leading or trailing spaces, and no blank lines.
2. Create an inbound mail filter policy using the wizard, under System Administration | Policy Management.

3. Add an exception by going to the Exception tab and dragging down the Email Address exception to the workbench. Connect the exception to the filter by clicking and dragging the yellow pin. In this example, to the Spam Filter Group.

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

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



Email Address Exception

☒ Scan sender address
☐ Scan recipient address

Search criteria (add each criteria on its own line)

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

5. Press Ok to save the search criteria.

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

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