SMTP Scanner Creation

GWAVA4

SMTP Scanner

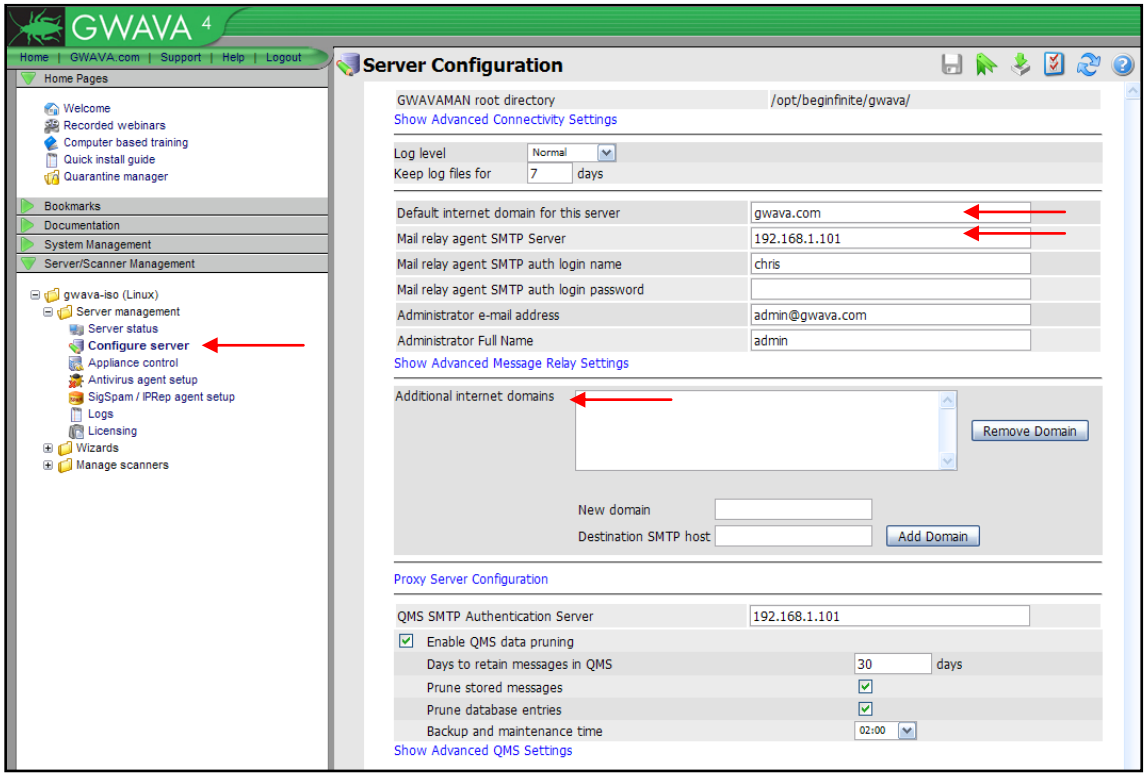
SMTP scanners allow the incoming and outgoing mail to be intercepted, scanned, and filtered completely independent of the mail system. This setup has the distinct advantage of relieving the mail system of unnecessary and unwanted traffic, leaving mail system resources open to function with greater performance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

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

Creating a SMTP Scanner

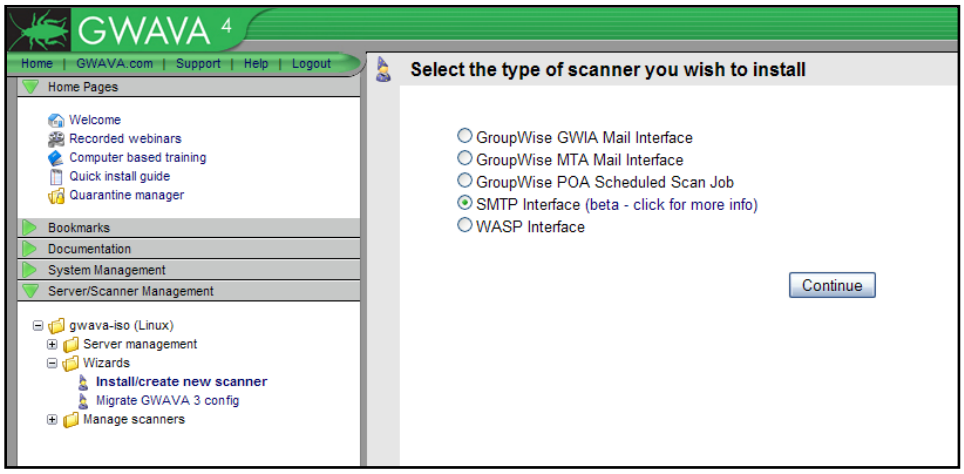
The SMTP scanner will only work if your MX record points to the GWAVA SMTP interface for mail delivery, and if your domain and mail system SMTP are listed correctly in your GWAVA system.

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



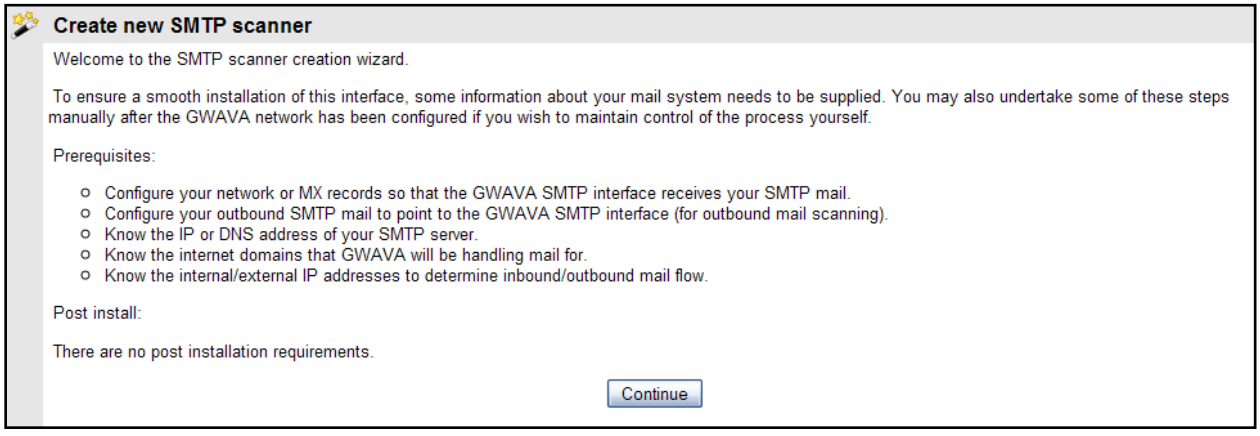
The Mail relay agent SMTP Server and Default domain MUST be Correct for your system. If you have multiple domains, list the additional domains. GWAVA will only accept mail for the listed domain(s).

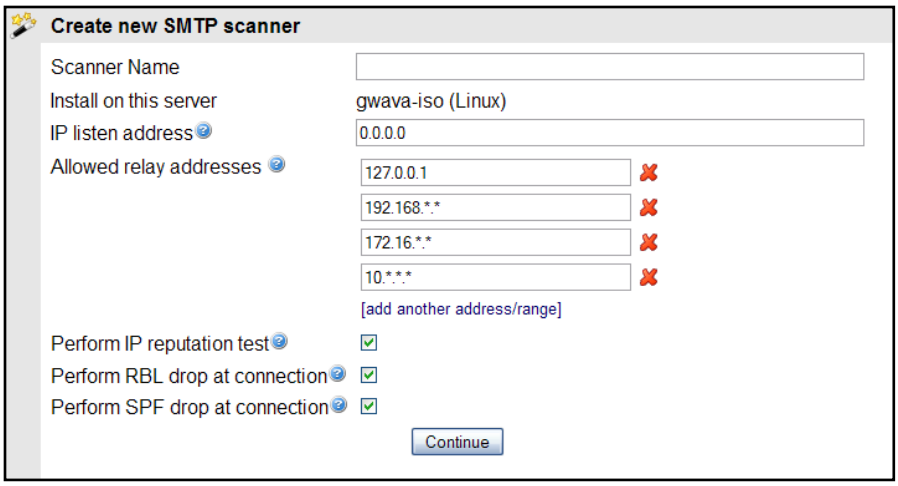
The Scanner creation wizards, (found under Server/Scanner Management | <Server name>| Wizards | Install/create new scanner), walk through the steps and information required to install the different scanners for your system. Select the SMTP Interface scanner and follow the instructions to install the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



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

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





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

The **IP listen address** is the address of the GWAVA Appliance. This should also be listed on the MX record for your domain.

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

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

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

RBL

The Real-time Blackhole List scanner searches the header of incoming message files to see if their source address is listed on an RBL. When enabled to drop on connection, a positive RBL event will cause the SMTP scanner to terminate the connection to the sending server for the offending message as soon as the event occurs. The RBL scanner utilizes real-time blackhole lists hosted on the servers listed under the RBL configuration page. RBL servers may be added or removed from the configuration. This is a strict pass or fail engine, and an offending ip address listed on the RBL will not be allowed to send mail to your system. Take time to verify that the RBL servers listed in the configuration are the desired list servers. The default list servers for RBL are, sbl-xbl.spamhaus.org and bl.spamcop.net.

IP Reputation

IP Reputation works much like the RBL scanner does, in that it uses a black list, but also has a white list for common mail sources. When used with the SMTP scanner, IP Reputation will also temporarily fail messages from sources not found on either list. The temporary fail will allow the sending SMTP gateway to retry, and it will eventually get through. This catches one-time spam bursts from sources not found on the black list, while enabling good mail to still be delivered to the system. The black and white lists are maintained and updated online, but are cached on the local machine as they are used.

SPF

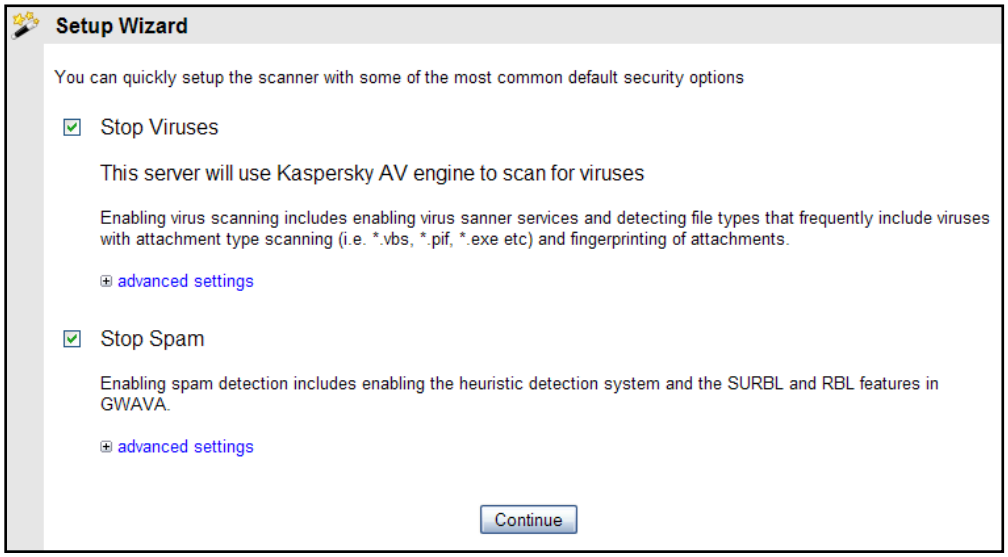
Sender Policy Framework can be used with the GWIA and SMTP scanners. Sender Policy Framework, (SPF) attempts to verify the sender of each email message, which can eliminate spoofed email and most

backscatter attacks. For SPF to work correctly, the sending domain must have an updated SPF record set up in DNS. If the sending domain does not have a SPF record set in their DNS, then their mail will not be blocked. Setting up a correct SPF record will block messages from spammers who are pretending to be you, to your system.

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

SPF is not enabled by default, but can be a powerful tool to keep spam from entering your system.

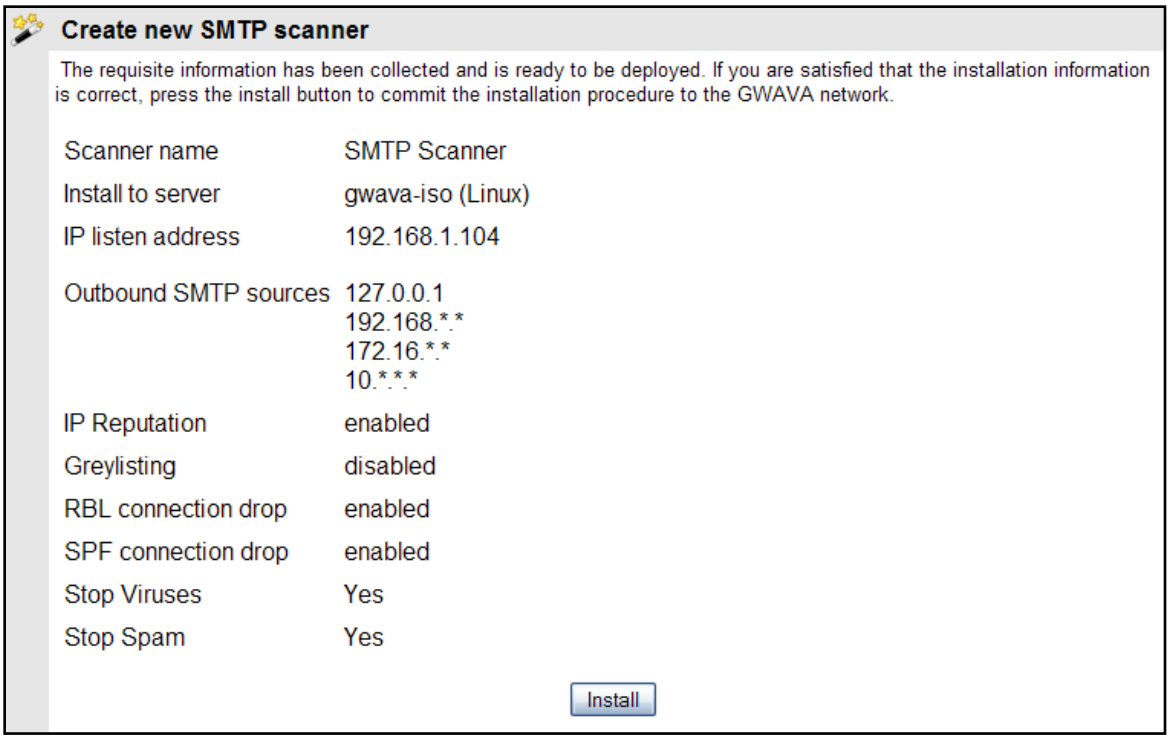
Select your preferences, and click ‘Continue’.



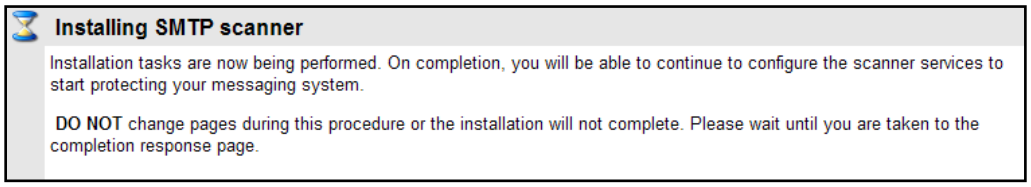
Set the default actions for viruses and spam. These settings can be changed after scanner creation.

Click ‘Continue’.

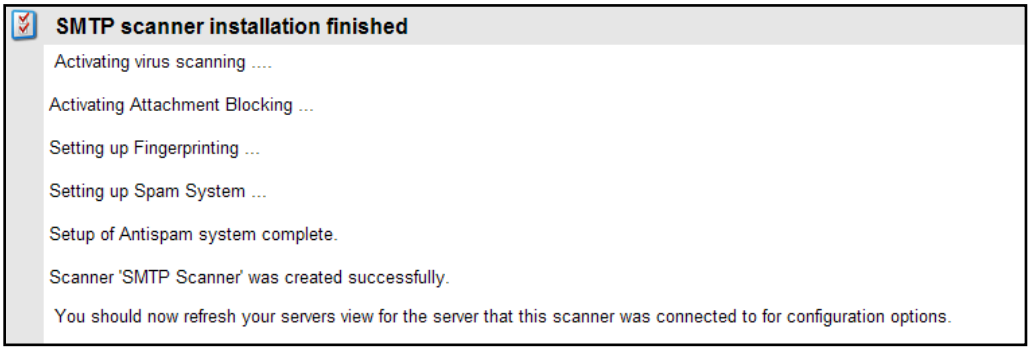
Review and confirm your settings. If you wish to make changes, use the '**back**' button on your browser, correct the information, and continue.



Click '**Install**' to continue.



Wait while the installation completes.



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

Your SMTP scanner is now created and ready to configure.

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