GWAVA 4

Appliance Installation Guide

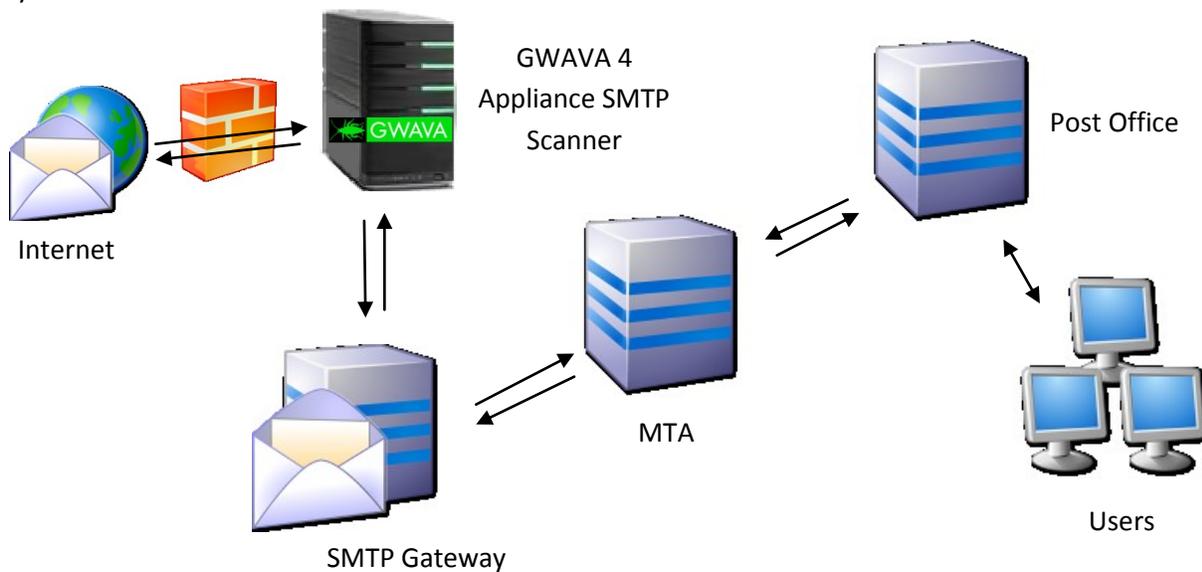## GWAVA4

Contents

Overview

The GWAVA 4 Appliance is a complete software package for implementing the GWAVA 4 system and is designed to replace an existing GWAVA 4 server with a standalone GWAVA 4 system running an SMTP scanner for any mail system. The GWAVA 4 Appliance is ideal for a virtual machine environment.

The GWAVA 4 Appliance is designed to run the SMTP scanner for any email system in the market. The SMTP scanner, and GWAVA 4 Appliance, are completely independent of any GroupWise system and can be implemented in any system. The SMTP scanner acts as a proxy for the SMTP Gateway of your mail system.

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

If the GWAVA appliance is set behind a firewall, or multiple firewalls, the following ports should be open for mail flow and GWAVA functions or services:

Inbound and general traffic
  - ➢ 53 – UDP (DNS lookups)
  - ➢ 25 – TCP Inbound (Used for Mail)

The following should be open to access the GWAVA appliance from outside the network:
  - ➢ 49285 – TCP Inbound (QMS message release service)
  - ➢ 49282 – TCP Inbound (GWAVA Management Console)
  - ➢ 22 – TCP (SSH access. This can be a security concern, but may be necessary to enable for support access.)

Outbound traffic
  - ➢ 80 – TCP Outbound (Updates services for Antivirus, Signature Engine, and GWAVA system.)
  - ➢ 21 – FTP Outbound (OS updates)
  - ➢ 25 – TCP Outbound (Only if scanning outbound mail)
  - ➢ 123 – TCP Outbound (Network Time Protocol (NTP))

Minimum System Requirements

For a system which processes ~2,000 messages per hour:

- 2.4 GHz Pentium 4 or equivalent processor
- 1 GB RAM
- 36 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

For a system which processes ~4,000 Messages per hour:

- 3.2 GHz Pentium 4 or equivalent processor
- 1.5 GB RAM
- 40 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

For a system which processes ~8,000 messages per hour:

- 3.6 GHz Pentium 4 or equivalent processor
- 2 GB RAM
- 60 GB Hard Drive (entire drive will be formatted automatically).
- 1 Network connection

Download

http://www.gwava.com/solutions/trial-downloads.html

Installation

To install the GWAVA 4 appliance, download the ISO and burn the image to a blank CD using your preferred CD burning program.

Insert the GWAVA 4 Appliance CD into the CD or DVD drive of the target system and boot from the Appliance CD.

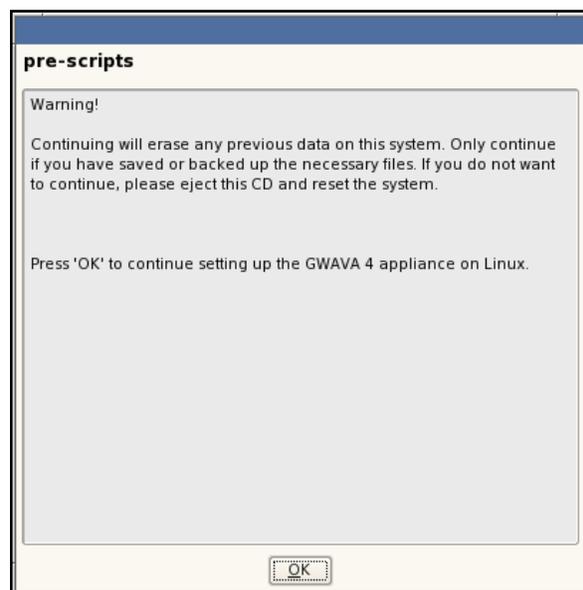On boot, you will be presented with the following menu.

To install the Appliance, choose the install option.

Allow the system to completely boot from the Appliance CD, and the installation will automatically start.

You will be warned that running the installation will delete all data currently on the system. **This is the last chance you have to avoid formatting the drive in this system.**

If you have several hard disks in the system, GWAVA4 will only install on the first one,(/dev/hda or /dev/sda), and ignore others. To ensure you install to the correct drive, physically disconnect or remove all but the destination drive from the system before you boot.

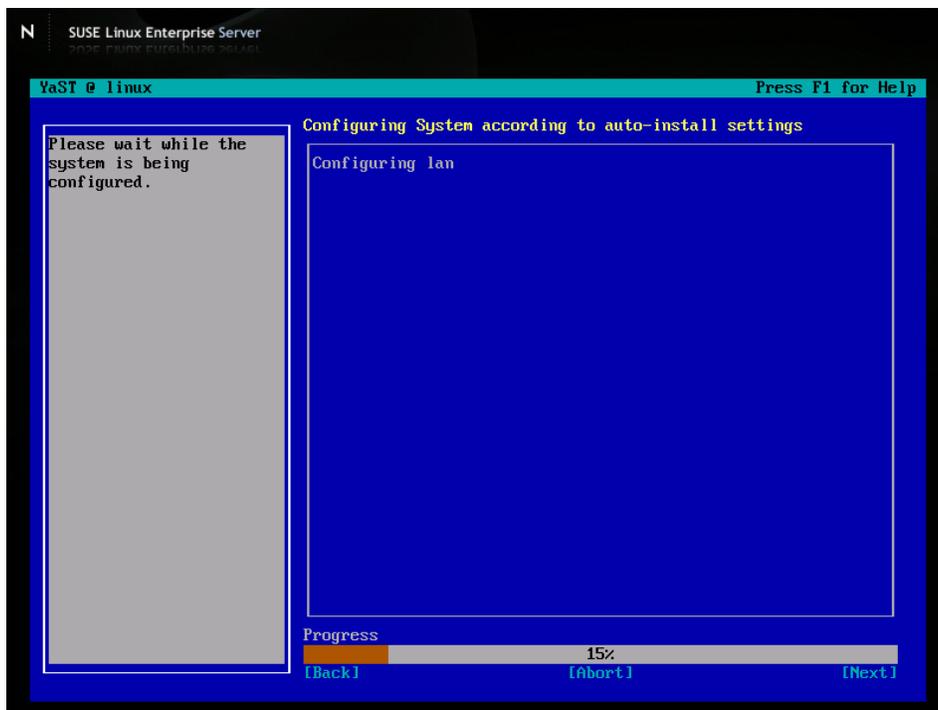As soon as you select 'OK', the installation will begin.

The setup does not require any user input until after the system reboots.

On system reboot, select boot from hard disk, and the default SLES 10.2 kernel listed.

The install will continue.
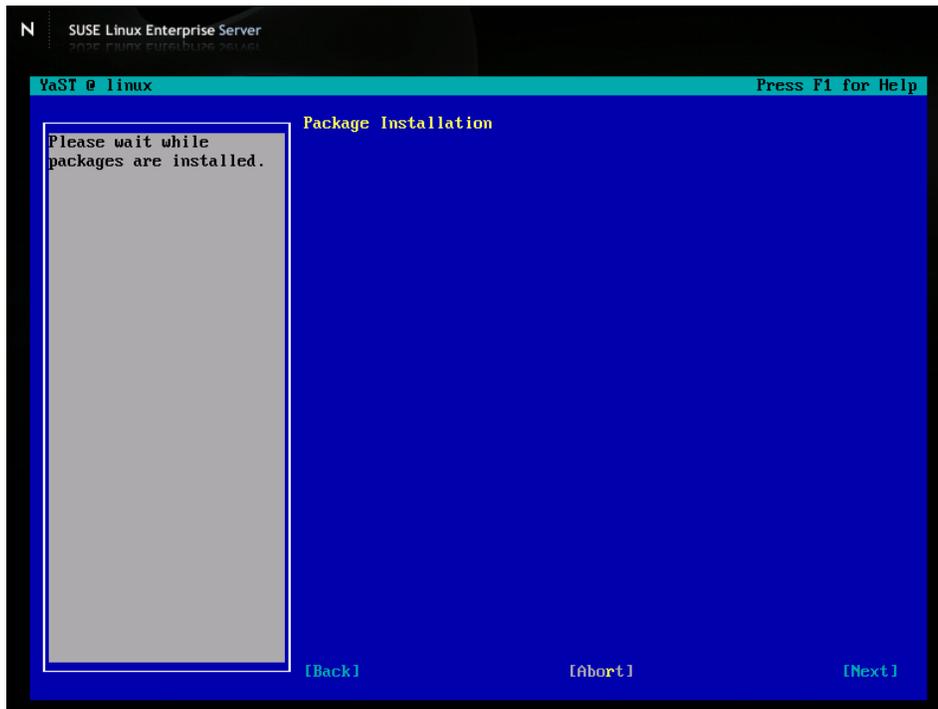
Allow the automatic configuration to continue.

Once the installation has completed, you will be asked to provide connection and security information for your new system.

To complete the setup, all pertinent network information must be provided for your system. The defaults detected in parentheses will be set if you simply hit 'enter'. To change the setting, enter the appropriate value.

Ensure that you have the ip address configured correctly, this is the only interface to set or change the network settings.

After the settings have been entered, you are asked to verify that the following information is correct. Review the information and hit 'y' or 'n' and 'enter' to either re-enter the information or to continue.

```
N   SUSE Linux Enterprise Server

########################## Final Setup Step (2/6) ##########################
############################# Test Network #############################


Your network settings will now be tested. If there is a failure, you
will be directed to resolve the problem before continuing.


Testing general connectivity using Ping
PING gwava.com (67.212.76.2) 56(84) bytes of data.
64 bytes from host.cabserver.net (67.212.76.2): icmp_seq=1 ttl=47 time=88.8 ms
64 bytes from host.cabserver.net (67.212.76.2): icmp_seq=2 ttl=47 time=90.3 ms

--- gwava.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 88.808/89.600/90.393/0.847 ms
Test port 80 inbound
--09:38:02--  http://download.gwava.com/gwava4/test/test
           => `/tmp/test'
Resolving download.gwava.com... 209.90.108.26
Connecting to download.gwava.com|209.90.108.26|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54 [text/plain]

100%[=======================================================>] 54          --.--K/s

09:38:03 (1.20 MB/s) - `/tmp/test' saved [54/54]

Test port 25 outbound
```

After you have set the network settings, they will be tested for connectivity.


```
N   SUSE Linux Enterprise Server

########################## Final Setup Step (3/6) ##########################
############################# SSH Setup #############################


SSH allows access to the server via a private key or via the root
password. It is recommended that you enable SSH permanently.

Please select an option.
1: Start SSH now and enable it permanently.
2: Stop SSH now.
3: Start SSH now.
4: Stop SSH now and disable it permanently.
5: Exit
Enter Selection: _
```

SSH allows remote console administration on port 22.   This can be turned on and off later through the GWAVA appliance control web interface. When you permanently enable or disable the service, it is removed from the runlevel and will be enabled or disabled on system startup until the setting is changed.

Next, is the time setup for the server. It is strongly recommended to setup the time on your system.

Pick your location. The wizard will narrow the terms to display a manageable list of time zones for you to select from.

Select your resident nation.

Select the appropriate time zone.

If you opt to specify a custom time zone, or do not find your time zone listed, you may choose the custom option: 'none'.

The time zone must be specified in Time Zone environment Variable. Syntax: <time zone name> <hours ahead of UTC> The time zone name does not matter, but the hour variable sets the time for the system.

for example:
MST-6

...would be accurate for the Mountain Standard Time zone, U.S. and Canada. The time zone may be any name you like, as long as it conforms to Posix Time Zone format.

```
Please enter the desired value of the TZ environment variable.
For example, GST-10 is a zone named GST that is 10 hours ahead (east) of UTC.
GST-6
awk: cmd. line:4: warning: escape sequence `\.' treated as plain `.'

The following information has been given:

        TZ='GST-6'

Therefore TZ='GST-6' will be used.
Local time is now:      Wed Jul  1 23:50:39 GST 2009.
Universal Time is now:  Wed Jul  1 17:50:39 UTC 2009.
Is the above information OK?
1) Yes
2) No
#?
```

After your custom time zone has been created, the information must be verified.

```
Setting the time using NTP

Specify custom time server? (y/n) y
Time server (example: time.nist.gov):
```

A custom Network Time server may also be specified. If a custom time server is used, provide the DNS name or IP address of the NTP server. Default, (time.nist.gov), is shown.

```
Setting the time using NTP

Specify custom time server? (y/n) y
Time server (example: time.nist.gov): time.nist.gov
Server: time.nist.gov
 1 Jul 17:51:34 ntpdate[3525]: adjust time server 192.43.244.18 offset 0.080447
sec

Time is now set to Wed Jul  1 17:51:34 UTC 2009
Try to get initial date and time via NTP from  time.nist.gov          done
Starting network time protocol daemon (NTPD)cp: cannot stat `/etc/localtime': No
 such file or directory
                                                                       done

Time and timezone setup complete
gwava-iso:/opt/beginfinite/gwava/scripts #
```

After the time server is specified, the system attempts to connect and sync the time.

Confirm the time settings for your system to continue.


```
N    SUSE Linux Enterprise Server

######################### Final Setup Step (5/6) #########################
############################# QMS Migration #############################


If you have an old GWAVA 4 installation running on NetWare you can migrate the
databases and their message data over to the new GWAVA 4 appliance.

The migration process is time consuming and may take several hours depending
on the size of your quarantine. It is highly recommended that you run this
migration during off hours.

If you plan on running the migration later you may lose some data. You are
not required to migrate your old QMS data if you do not wish to.

Migrate your old QMS data now? (y/n)_
```

If you want to migrate an existing NetWare GWAVA4 Quarantine to the GWAVA Appliance, select 'yes' here. The wizard uses ncpmount to pull the information over the network connection from the existing qms to the Appliance.

You will be required to shut down the QMS system on the NetWare machine to complete the operation. This process can take several hours and should only be performed after-hours. If you wish to migrate QMS, this is the time to do so. Thought you may invoke the command later, you will have data loss unless the migration is completed during setup.

```
N    SUSE Linux Enterprise Server

######################### Final Setup Step (6/6) #######################
############################# Password Setup ###########################


At the prompt please type a new root password. You will need this
password to log back in to the system.

After the password has been changed the server will restart and be
ready for use.

Changing password for root.
New Password:
```
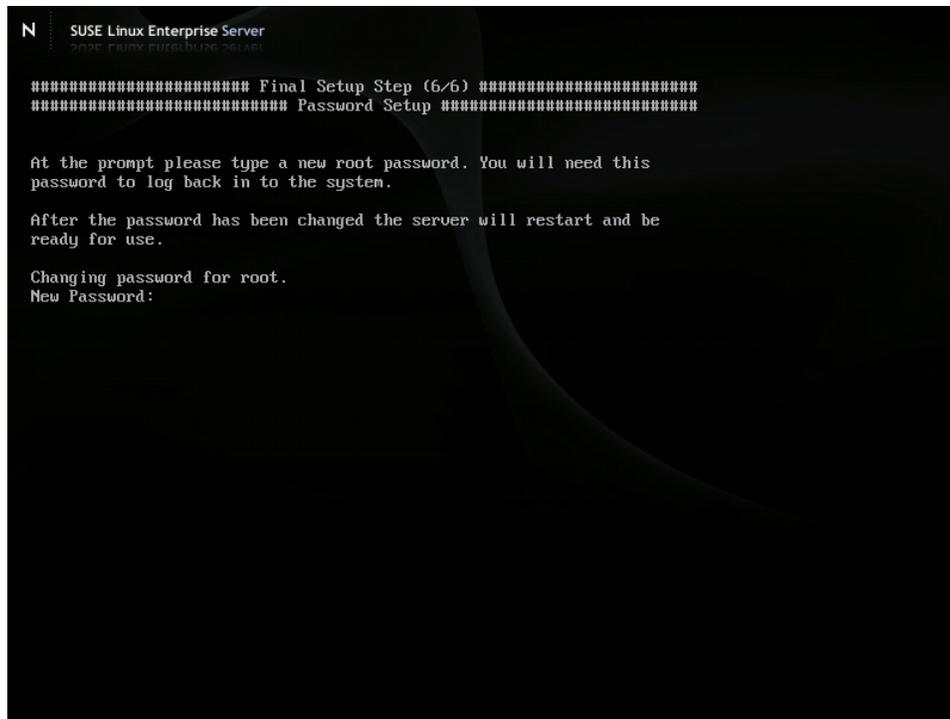
For the final step, you are asked to set the root password for the system. This is the administrator password which will be required to log in to the system via ssh or through the console. DO NOT LOSE THIS PASSWORD.

The Appliance is designed to provide all the necessary functions for GWAVA 4 inside the GWAVA 4 web administration, thereby removing all need for console level administration. While normal operation of the GWAVA 4 Appliance removes all need for console level administration, the root password may be required for support.

GWAVA 4 appliance setup is now complete. All that remains is activating the GWAVA 4 server and creating a scanner of your choice.

Server Activation

To Activate your server, open a browser and enter the ip address or DNS name of the Appliance, with port 49282.

http://<your_server_ip>:49282

This is the connection address for the GWAVA 4 management console. When you first connect to the system, you should be taken to the setup page, shown below.
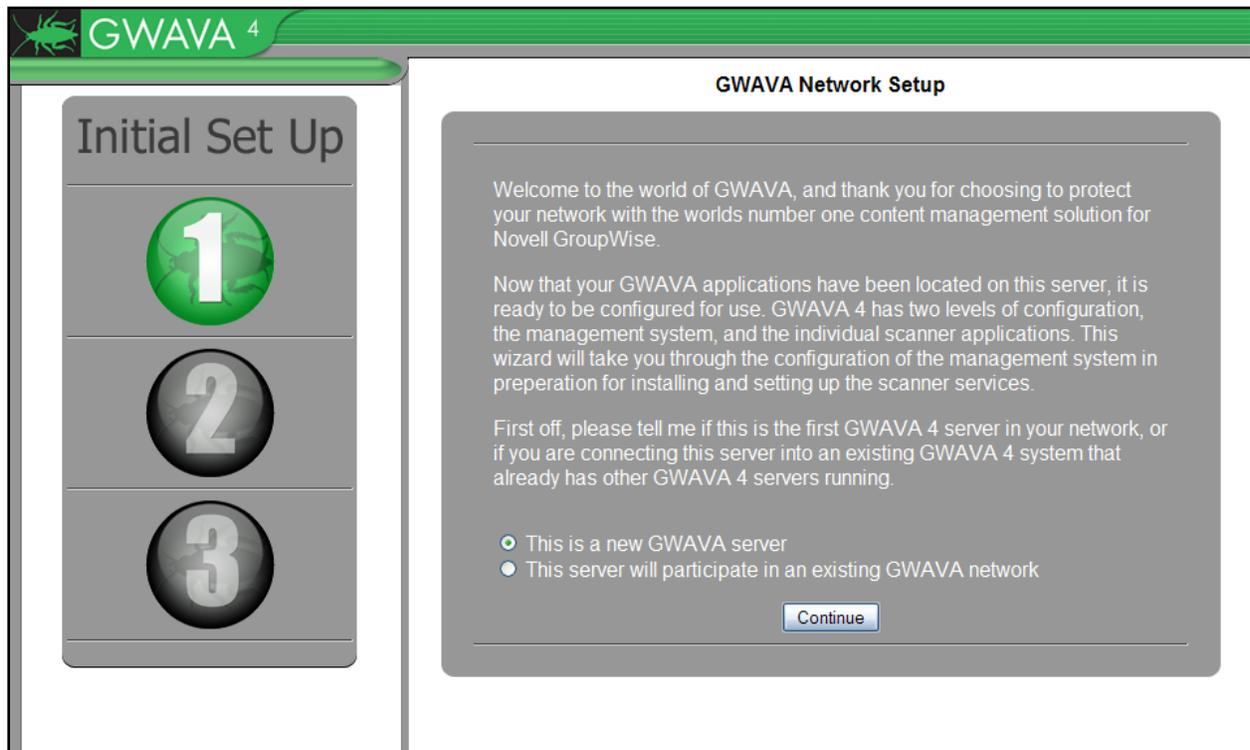
The GWAVA Appliance is designed to replace existing GWAVA 4 servers, and as such it is recommended to setup the Appliance as a new GWAVA server.

 Select '**Continue**'.

The following information is required.

The server name should match the host name you set for the server. The connection address is the address that GWAVA 4 will use to serve the management console. Both the Server parameters should be left as default.

The Administrator login name and password are required to connect to, and administer the GWAVA 4 management console. DO NOT LOSE THIS PASSWORD.

The Internet domain is the domain that the GWAVA 4 server will filter mail for. This should be your company domain. (ie. GWAVA.com)

The administrator name and email address is the name and address which will appear on GWAVA 4 notifications and digests. Any responses to these messages will be sent to the Administrator's e-mail address.

The SMTP server address should be the address of your GWIA or SMTP gateway. If you are using an SMTP scanner, this will be the address which GWAVA 4 will forward the incoming mail to. GWAVA 4 also uses this address for GroupWise authentication for QMS authentication and access.

The SMTP authorization name and password are not required for notifications, but are recommended. For GroupWise systems, this can be any username and password, and does not have to be an administrator. (ie. Username: bob   Password: c751h)

After you have provided the information, select '**Continue**'.
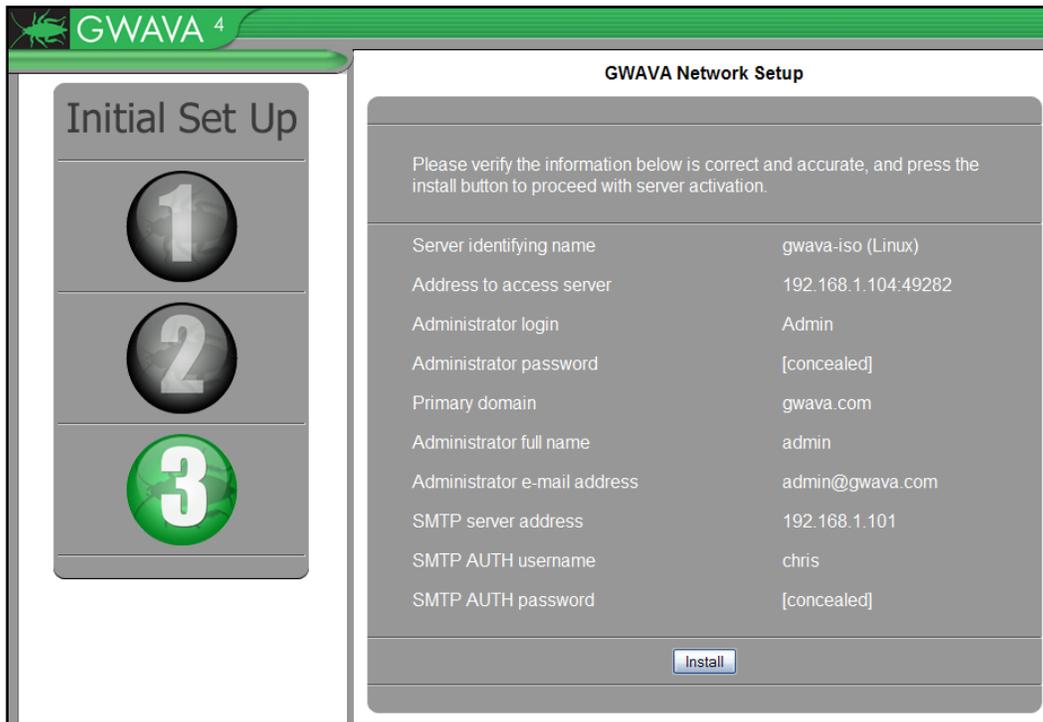
You will be asked for confirmation. Clicking '**Install**' will activate the GWAVA 4 server, and you will be required to login using the admin name and password you provided earlier. Click '**back**' on your browser if you need to make any changes.

When you click '**Install**', wait for the activation process to complete. You should be redirected to the management login screen.

Click on '**Enter Management Console'** and provide the administrator username and password to login.
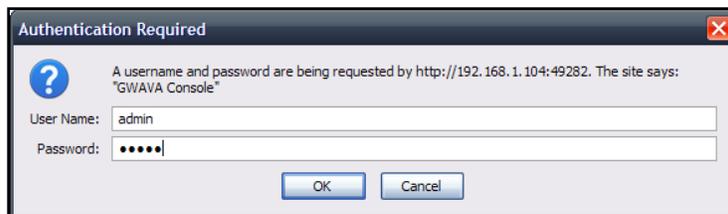
Once you log in, your new GWAVA 4 server should display the following page.
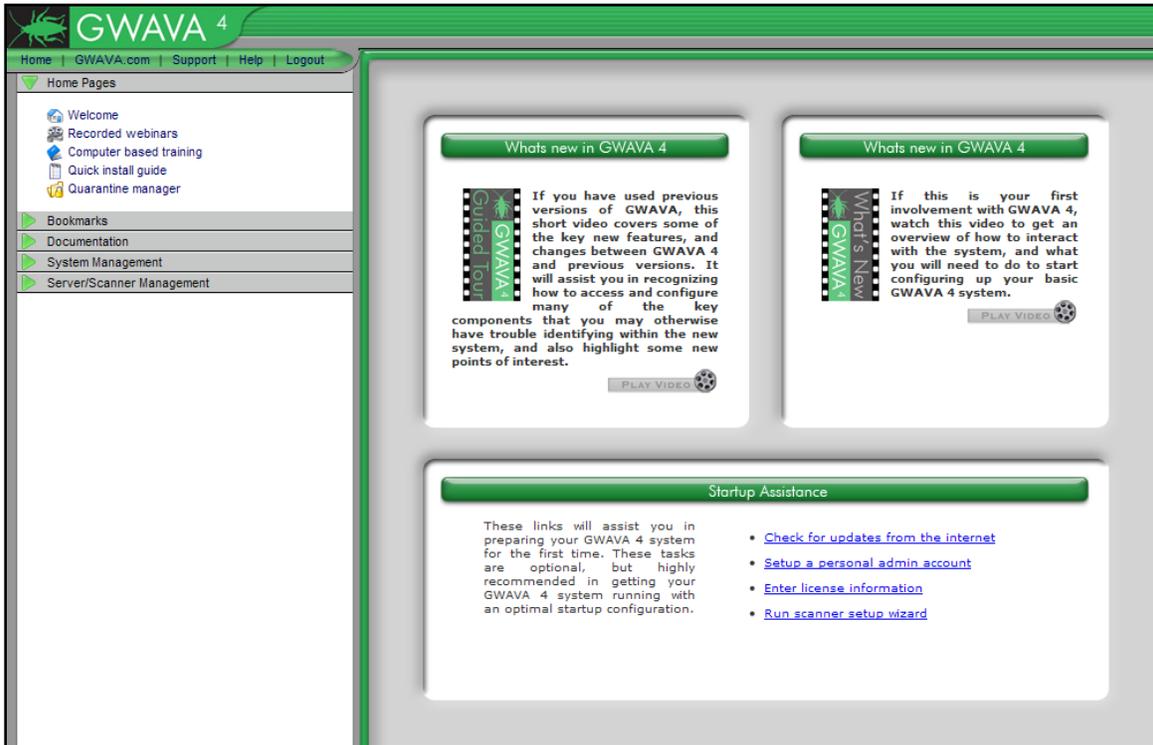
This page is the home page for the Management Console.

To administer any necessary changes to the GWAVA 4 appliance, open the **Appliance Control** page found under **Server/Scanner Management | <Server name> | Server Management**, as shown below.
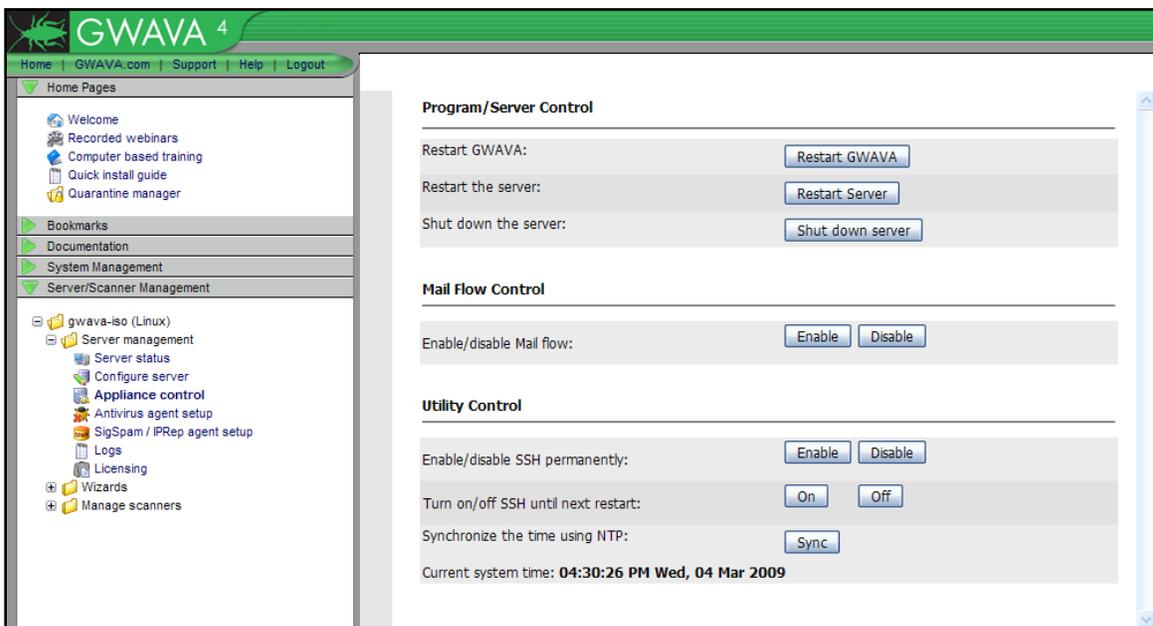
The Appliance Control page allows you to control the basic functions of the server, and open SSH access if required.

When an update is performed, GWAVA 4 must be restarted to complete the process. This can be achieved from this web console at the click of a button, as well as a full system restart or shutdown.

Suspending mail flow, enabling or disabling SSH, and synchronizing the system time can all be performed from this page.

The GWAVA 4 server is now installed and ready to be configured for your system.

SMTP Scanner, SMTP Proxy Mail Scanner

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

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

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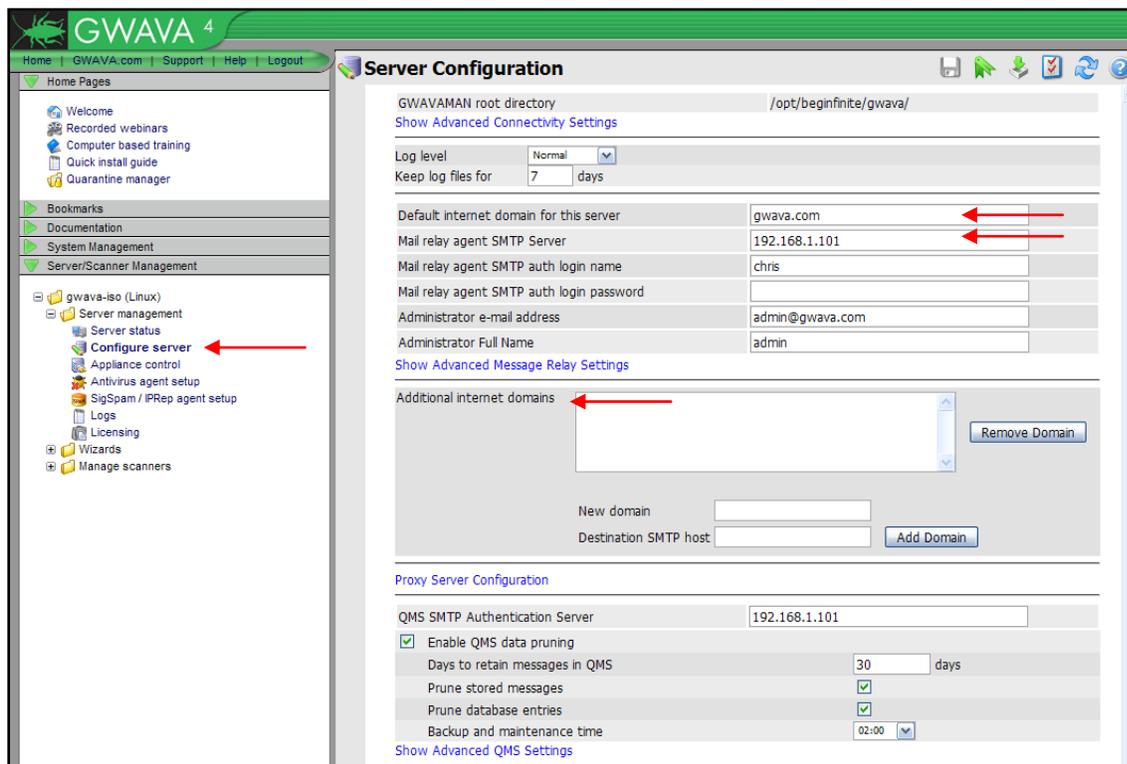
The Mail relay agent SMTP Server and Default domain MUST be Correct for your system. If you have multiple domains, list the additional domains. GWAVA will only accept mail for the listed domain(s).

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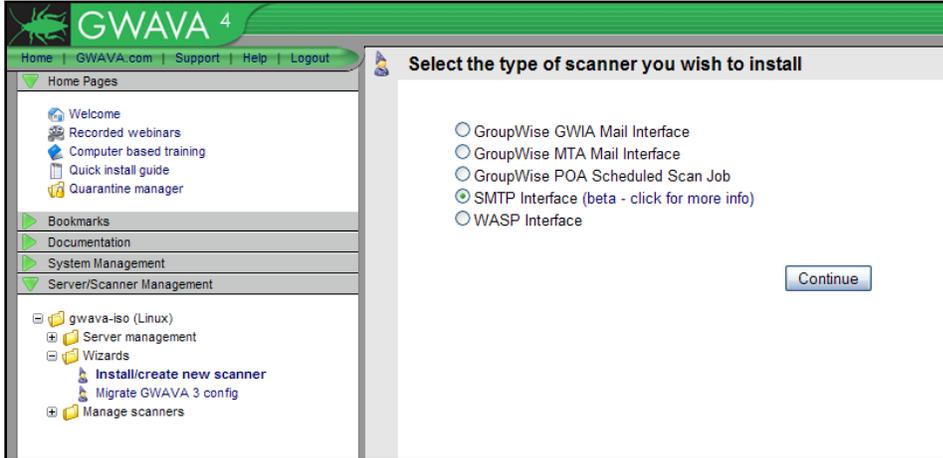
To install a SMTP scanner, select the SMTP scanner option from the wizard and click next.

The SMTP scanner creation wizard informs you of the information you must know to successfully create the scanner.
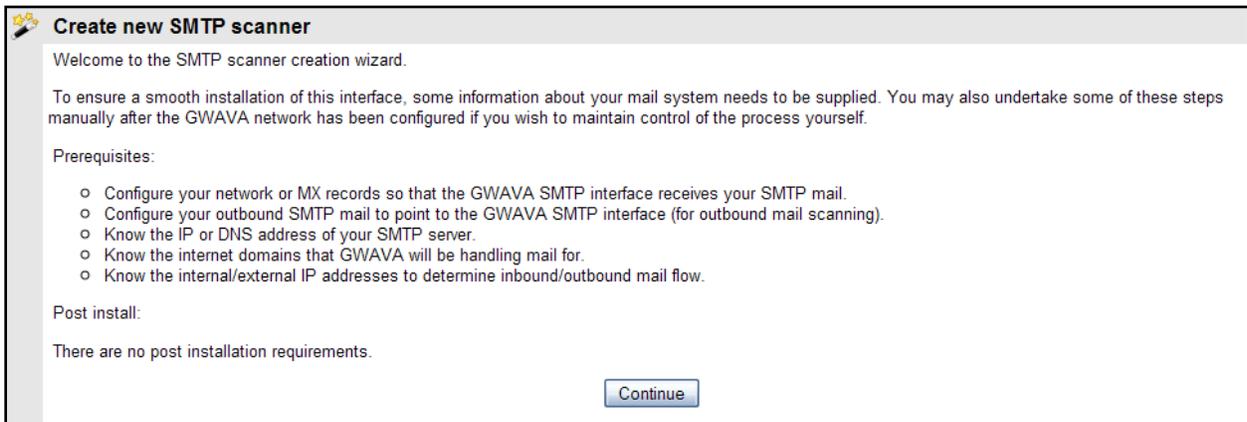
The **Scanner Name** is whatever you wish the scanner to be named in the GWAVA server.

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.
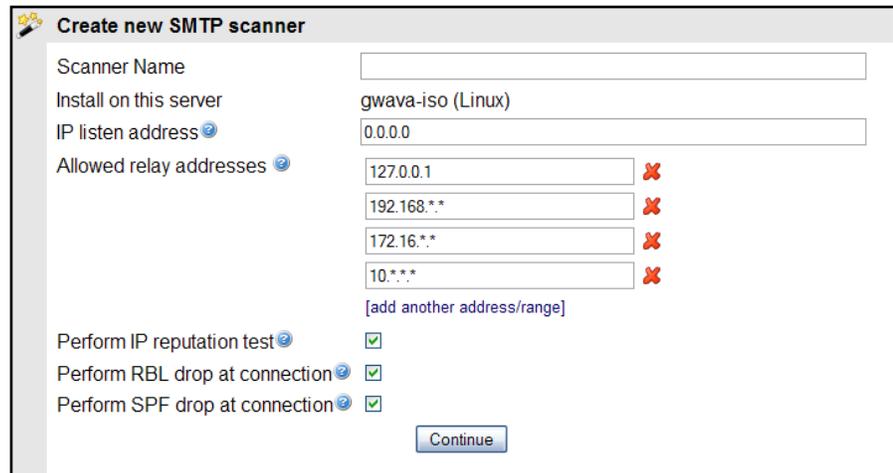
RBL
The Real-time Blackhole List scanner searches the header of incoming message files to see if their source address is listed on an RBL. When enabled to drop on connection, a positive RBL event will cause the SMTP scanner to terminate the connection to the sending server for the offending message as 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'.
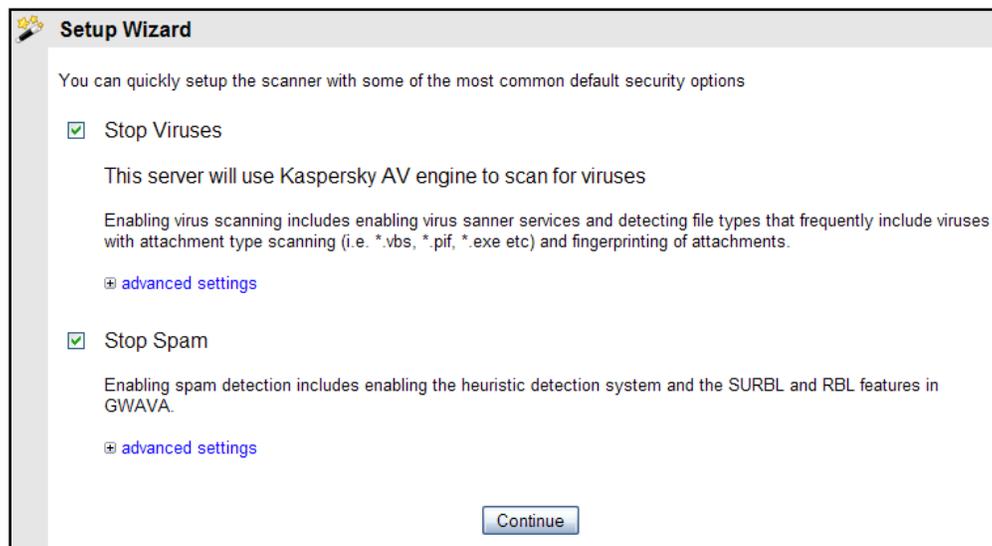
Set the default actions for viruses and spam. These settings can be changed after scanner creation.

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.

Create new SMTP scanner

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

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

Install

Click '**Install**' to continue.

Installing SMTP scanner

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

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

Wait while the installation completes.

SMTP scanner installation finished

Activating virus scanning ....

Activating Attachment Blocking ...

Setting up Fingerprinting ...

Setting up Spam System ...

Setup of Antispam system complete.

Scanner 'SMTP Scanner' was created successfully.

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

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

Your SMTP scanner is now created and ready to configure.

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