

---

# **Baruwa Enterprise Edition Documentation**

*Release 2.0.7*

**Andrew Colin Kissa**

July 08, 2015



<b>1</b>	<b>What is Baruwa Enterprise Edition</b>	<b>3</b>
1.1	How does it work . . . . .	3
1.2	Features . . . . .	3
1.3	System Requirements . . . . .	5
1.4	Topologies . . . . .	5
<b>2</b>	<b>Feature List</b>	<b>11</b>
2.1	System Features . . . . .	11
2.2	Management and Reporting . . . . .	11
2.3	High Availability . . . . .	12
2.4	Antispam, AntiSpam, Malware Protection . . . . .	12
2.5	Customer Support . . . . .	13
<b>3</b>	<b>Obtaining Baruwa Enterprise Edition</b>	<b>15</b>
3.1	Download ISO image . . . . .	15
3.2	Making an Installation CD/DVD . . . . .	15
<b>4</b>	<b>Planning for Installation</b>	<b>17</b>
4.1	Hardware Compatibility . . . . .	17
4.2	Supported Installation Hardware . . . . .	17
4.3	RAID and Other Disk Devices . . . . .	18
4.4	Network Firewall . . . . .	19
4.5	DNS . . . . .	19
4.6	Clustering . . . . .	19
4.7	System Profiles . . . . .	20
<b>5</b>	<b>Installation</b>	<b>23</b>
5.1	Overview . . . . .	23
5.2	Boot Menu . . . . .	23
5.3	Network Configuration . . . . .	26
5.4	Graphical Mode Installation . . . . .	28
5.5	Text Mode Installation . . . . .	32
<b>6</b>	<b>Configuration</b>	<b>37</b>
6.1	StandAlone System . . . . .	37
6.2	Automated Configuration . . . . .	37
6.3	Post Configuration . . . . .	57
<b>7</b>	<b>Cluster Configuration</b>	<b>59</b>
7.1	Backend System . . . . .	59
7.2	Database System . . . . .	68

7.3	Search Index System . . . . .	75
7.4	Message Queue System . . . . .	80
7.5	Cache System . . . . .	84
7.6	Web and Mail System . . . . .	87
7.7	Mail System . . . . .	107
7.8	Web Interface System . . . . .	127
<b>8</b>	<b>Advanced configuration</b>	<b>141</b>
8.1	Content Protection . . . . .	141
8.2	External Authentication . . . . .	142
8.3	Clustering . . . . .	143
8.4	Themes . . . . .	145
8.5	Baruwa API . . . . .	147
8.6	Addons . . . . .	149
<b>9</b>	<b>Administrators guide</b>	<b>151</b>
9.1	Managing Organizations . . . . .	151
9.2	Managing Domains . . . . .	154
9.3	Managing Accounts . . . . .	161
9.4	Managing API Applications . . . . .	164
9.5	Managing Settings . . . . .	165
9.6	System Status . . . . .	180
9.7	Command line Reference . . . . .	181
9.8	Scheduled commands . . . . .	185
9.9	Baruwa Backups . . . . .	186
9.10	Monitoring . . . . .	187
9.11	Baruwa log files . . . . .	188
9.12	Languages supported . . . . .	189
9.13	FAQ's . . . . .	190
9.14	Upgrading . . . . .	191
9.15	Changelog . . . . .	202
<b>10</b>	<b>User guide</b>	<b>209</b>
10.1	Signing In and Signing Out . . . . .	209
10.2	Changing Your Password . . . . .	209
10.3	Personalizing Your Account . . . . .	210
10.4	Messages . . . . .	211
10.5	Approved and Banned Sender Lists . . . . .	215
10.6	Reports . . . . .	215
10.7	Mail queues . . . . .	218
10.8	Baruwa Search Tips and Tricks . . . . .	219
<b>11</b>	<b>Support</b>	<b>221</b>
11.1	Free support . . . . .	221
11.2	Paid for support . . . . .	221
<b>12</b>	<b>Previous Documentation</b>	<b>223</b>

Baruwa Enterprise Edition is a fully fledged Mail Security solution, based on best of breed open source software packages. It provides protection from spam, viruses, phishing attempts and malware.

Baruwa Enterprise Edition is a proven email security platform for organizations of any size from small to medium businesses to large service providers, carriers and enterprises.

Baruwa Enterprise Edition works with any standard SMTP server, is highly accurate, scalable, easy to integrate as well as manage.

Automated installation, configuration management tools and an API are provided to ensure the efficient and easy management of the System.



## WHAT IS BARUWA ENTERPRISE EDITION

**Baruwa Enterprise Edition** is a fully fledged Mail Security solution, based on best of breed open source software packages. It provides protection from spam, viruses, phishing attempts and malware.

**Baruwa Enterprise Edition** is a proven email security platform for organizations of any size from small to medium businesses to large service providers, carriers and enterprises.

**Baruwa Enterprise Edition** works with any standard SMTP server, is highly accurate, scalable, easy to integrate as well as manage.

Automated installation, configuration management tools and an **API** are provided to ensure the efficient and easy management of the System.

The management interface is implemented using web 2.0 features (AJAX) where deemed fit. It has full support for i18n, enabling you to translate it into any language of your choosing. It has already been translated into to over 25 languages. Current *Languages supported*

Also included is reporting functionality with an easy to use query builder, whose results can be displayed as message lists or graphed as colorful and pretty interactive graphs.

Built in Full text search functionality allows you to find information very fast and easily. Advanced searching options available in leading web search engines are supported.

**Baruwa Enterprise Edition** is built on an open source core.

### 1.1 How does it work

It operates as an Email security gateway accepting mail from untrusted sources, running extensive checks on it and then passing the clean mail to the destination. It does not support the hosting of user mailboxes.

For incoming messages, it is configured to accept mail on behalf of your internal mail server run extensive checks on it then forward the clean mail to your internal mail server.

For outgoing messages, your internal mail server can be configured to pass all outbound messages to it for processing before being sent on to the destination. From the internal servers point of view the system is its smart host.

It can operate as a standalone all in one solution or as a cluster of servers sharing database, indexing, storage and message queue servers. The traditional concept of a cluster master is not supported, all the nodes in the cluster have equal status and can be brought into and taken out of the cluster without any special changes.

### 1.2 Features

- Spam, Virus, Phishing, Malware protection

- Extensive Spam Detection checks
- AJAX support for most operations
- Ultra fast full text search
- Reporting with AJAX enabled query builder
- I18n support, allows use of multiple languages
- Themes/Skins for rebranding
- Signature management / Branding
- Mail queue management and reporting
- Message delivery/relay information
- DKIM management
- Reporting graphs
- Emailed PDF reports
- Audit trails
- Archiving of old message logs
- Local DB prevents data loss when DB is unavailable
- Multi Tenancy
- User profile aware approved/banned sender management
- IP / network addresses supported in approved/banned list manager
- System status information
- IPv6 Support
- Asynchronous logging
- Import and Export of User accounts and Domains
- AD/Exchange integration to auto populate account and group information
- Easy plug-in authentication to external authentication systems
- AD/LDAP, POP3, IMAP, SMTP, RADIUS Authentication support
- REST OAUTH based API
- Tools for housekeeping tasks
- Easy clustering of multiple servers
- Works both with and without Javascript enabled
- No limits on domains and users add as many as your hardware can support.
- Email Address tagging support

A full feature list is available at [Feature List](#)



## 1.3 System Requirements

- Intel/AMD 2.0 GHZ+ 64-bit CPU
- Minimum - 2 GB RAM
- 5 GB free disk space for OS
- Additional disk space for Mail and Data storage

---

**Note: NOTE:** The amount of resources allocated to system is directly related to the amount of email the system will be processing as well as the number of users connected to the web interface.

---

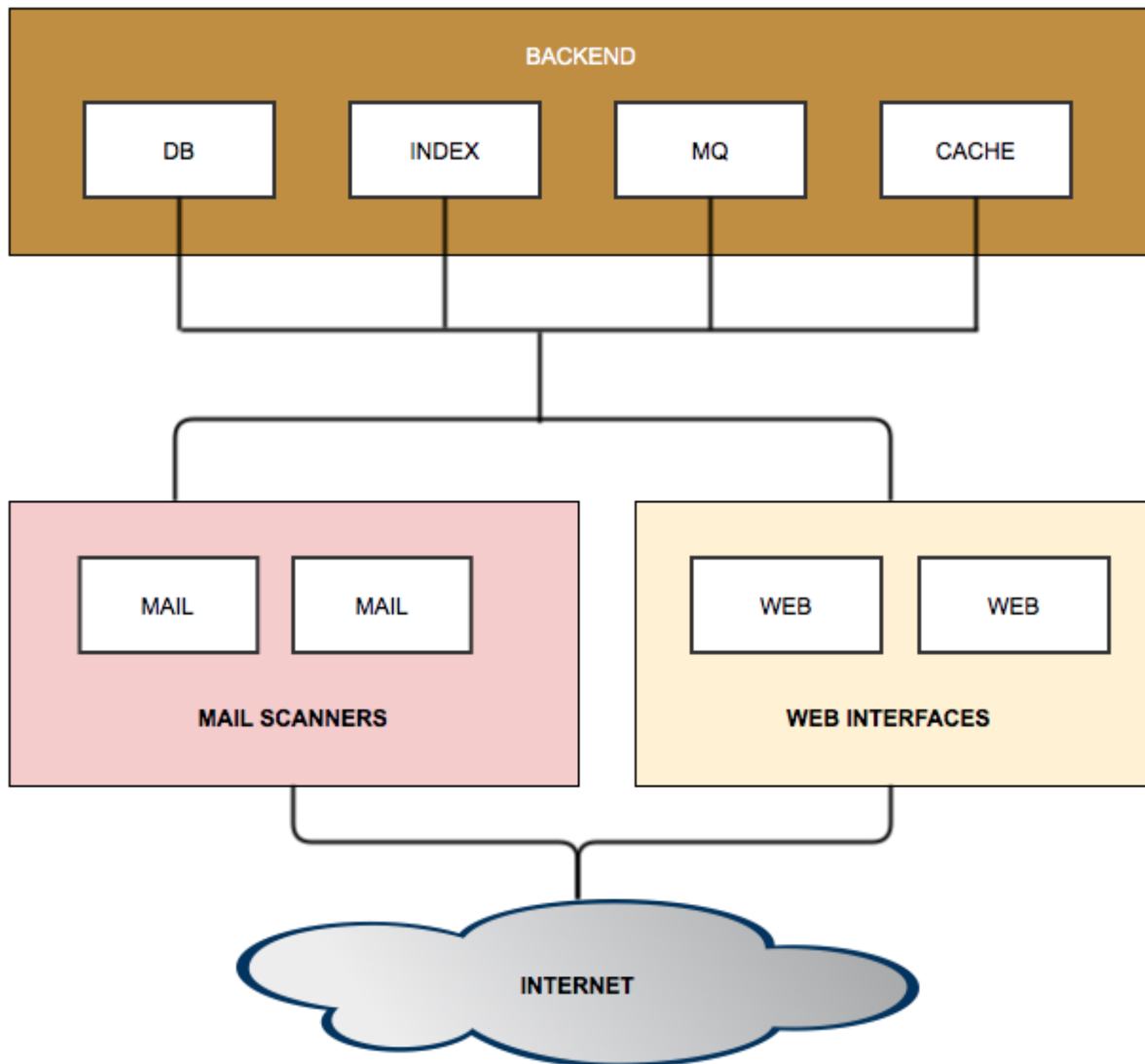
## 1.4 Topologies

Baruwa Enterprise Edition can be configured in various topologies. `Standalone` which is the default configuration, and works well in small scale environments in larger environments with higher mail volumes and user numbers as well as stricter uptime requirements clustered topologies should be used.

The supported clustered topologies are described below.

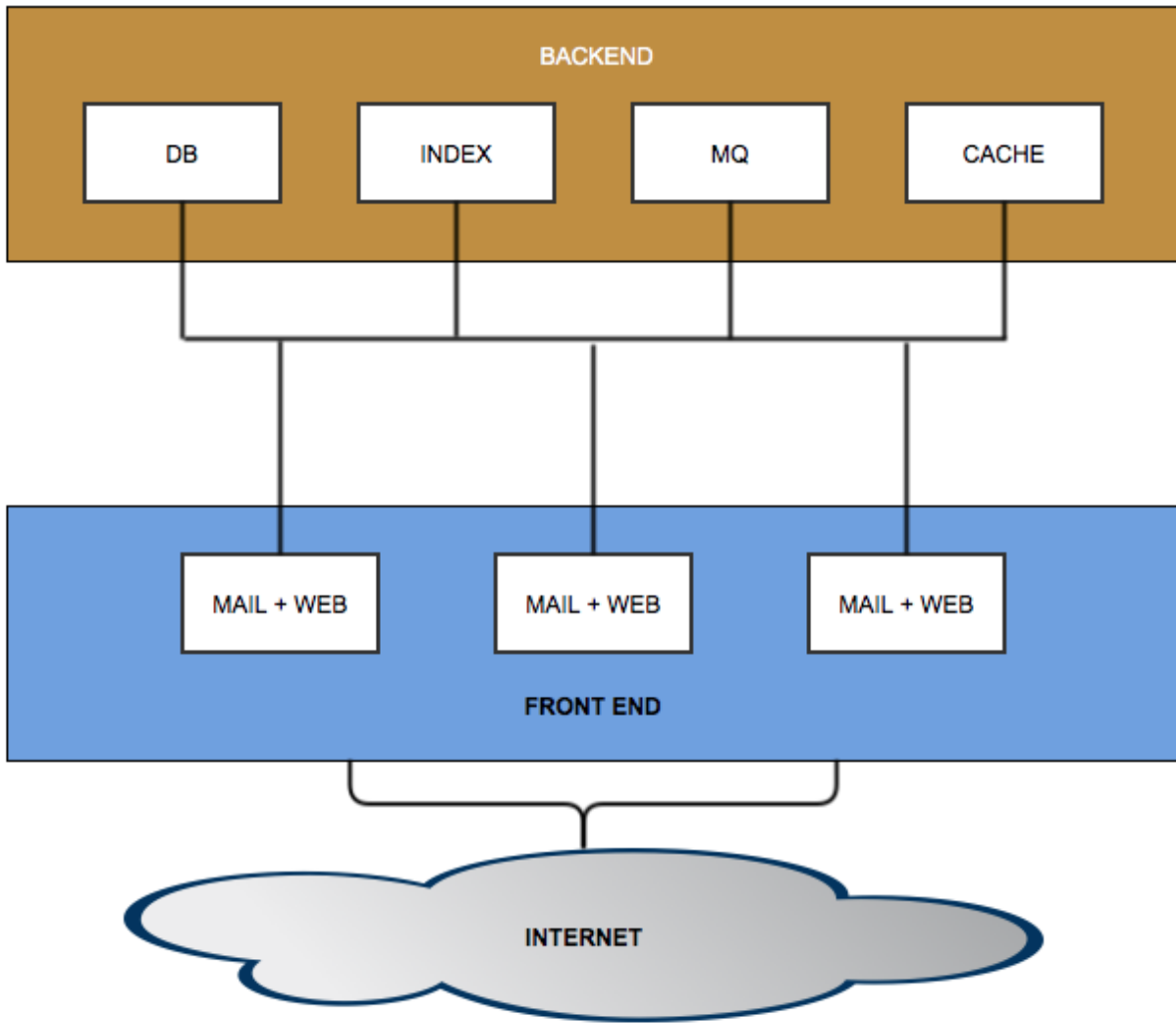
### 1.4.1 Distributed Backend Distributed Frontend

In this topology all the backend components are each installed on standalone systems and the frontend components are also installed on standalone systems. This solution is the recommended for very large environments as it performs better and scales out and in easily.



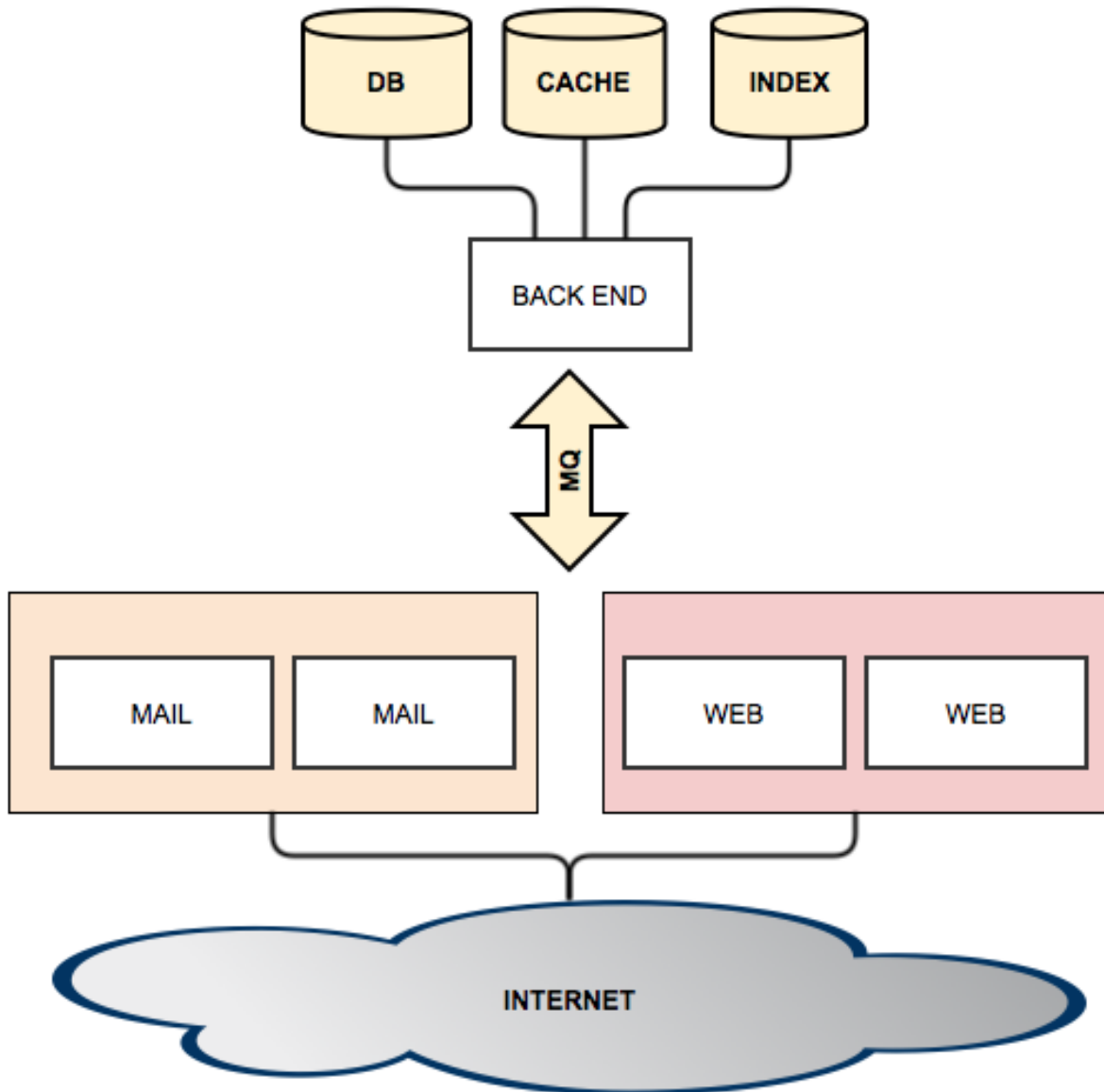
### 1.4.2 Distributed Backend Hybrid Frontend

In this topology all the backend components are each installed on standalone systems and the frontend components are combined on to a node. Scaling is achieved by adding additional frontend nodes.



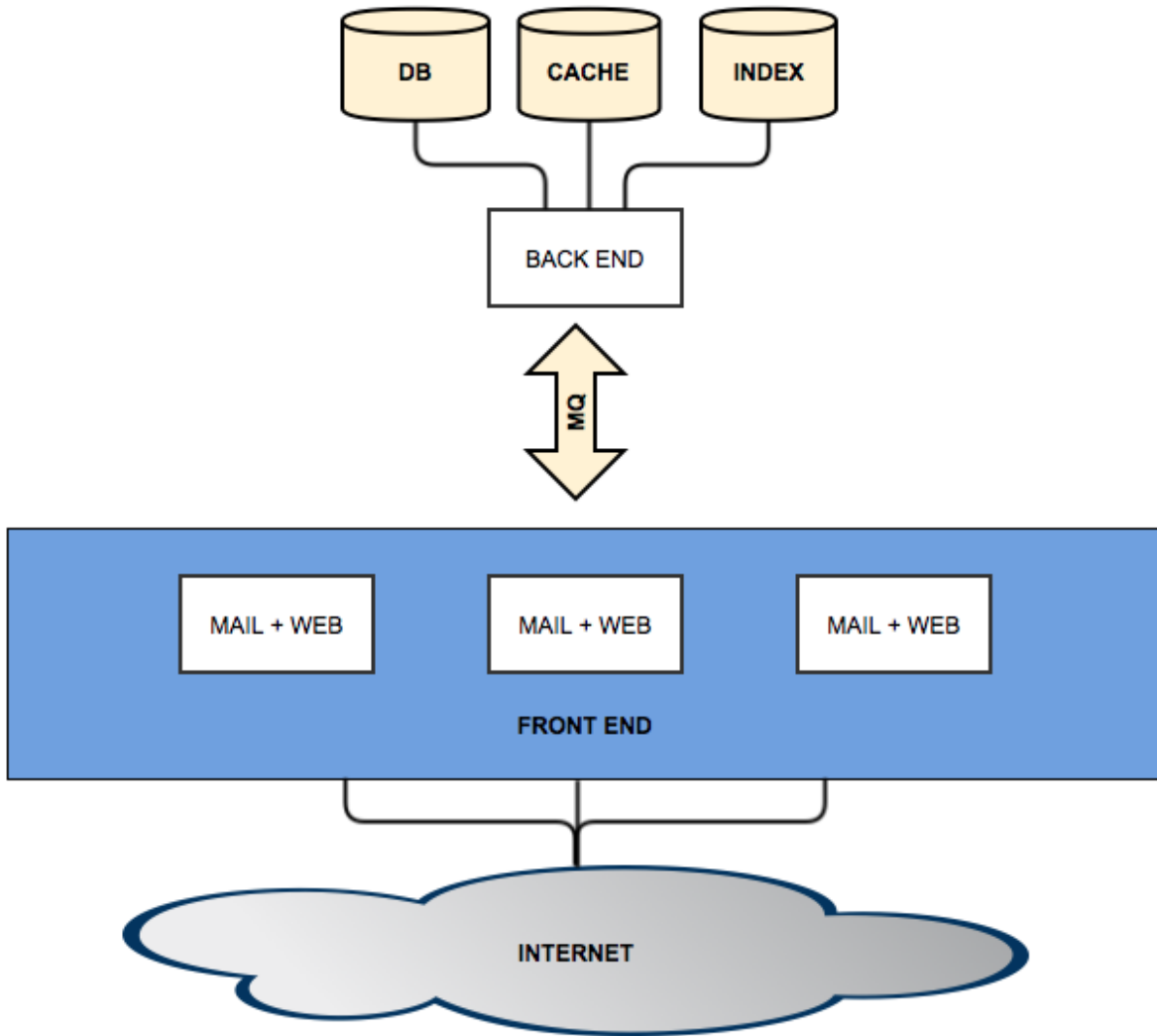
### 1.4.3 Single Backend Distributed Frontend

In this topology all backend components are installed on a single system and the frontend components are each installed on standalone systems. Scaling is achieved by adding additional frontend nodes.



#### 1.4.4 Single Backend Hybrid Frontend

In this topology all backend components are installed on a single system and the frontend components are combined on to a node. Scaling is achieved by adding additional frontend nodes.





## FEATURE LIST

Baruwa Enterprise Edition is a fully featured mail security solution, which is suited to organizations of any size from small to medium businesses to large service providers, carriers and enterprises.

### 2.1 System Features

- Inbound and Outbound protection
- Multi Tenancy
- SMTP Authentication Support
- Per Domain policies
- IPv6 and IPv4 Address Support
- Mail Queue Management
- Multiple Language Support
- Ultra fast full text search
- Spam, Virus, Phishing, Malware protection
- Extensive Spam Detection checks
- AJAX support for most UI operations
- Themes/Skins for rebranding
- Email Address tagging support
- AD/LDAP, POP3, IMAP, SMTP, RADIUS Authentication support
- Customized Linux based OS

### 2.2 Management and Reporting

- Themes/Skins for rebranding
- Signature management / Branding
- Mail queue management and reporting
- Message delivery/relay information
- DKIM management

- Reporting graphs
- Reporting with AJAX enabled query builder
- System status information
- External Syslog support
- Audit trails
- Advanced Setup Wizard Utility
- Centralized Quarantine for large scale cluster deployments
- Import and Export of User accounts and Domains
- REST OAUTH based API
- Easy plug-in authentication to external authentication systems

## **2.3 High Availability**

- No Master clustering
- Active-Active clustering
- Shared Quarantine
- Node Failure Detection and Notification
- Easy clustering of multiple servers

## **2.4 Antispam, AntiSpam, Malware Protection**

- Baruwa Datafeeds reputation services
- Email Header Inspection
- Spam URI and Real-Time Blacklists
- URL Filtering
- Local Sender Reputation
- Quarantine with end user reporting and notification
- Approved/Banned Lists at Global, Domain, and User levels
- Bayesian Statistical Analysis
- Rate limiting
- Malware Detection
- Archive Scanning
- Content Protection
- Forged Sender Address Checks
- Anti-Virus with Spam and Malware signatures
- Reverse DNS Checks
- Denial of service protection



- SPF, DKIM, DMARC

## 2.5 Customer Support

- Free standard email support as part of subscription
- Responsive and knowledgeable support team
- 24x7 Support packages available
- On device support available
- Design and consulting services
- SLA / System maintenance contacts available.
- Remote monitoring services



## OBTAINING BARUWA ENTERPRISE EDITION

If you have a Baruwa Enterprise Edition subscription, you can download ISO image files of the Baruwa Enterprise Edition 6.6.1 installation DVD from the Download Area on the Baruwa website. If you do not have a subscription, you need to purchase one or get a free 30 subscription via the [Baruwa website](#).

### 3.1 Download ISO image

If you have a subscription, follow these steps to obtain the Baruwa Enterprise Edition 6.6.1 ISO image files:

1. Visit the Download area at <https://downloads.baruwa.com>
2. You will be prompted for a login, enter your Mailing list Login and Password.
3. Click iso, click the 6.6.1 directory then click Baruwa-6.6.1.iso.

After you download an ISO image file of the installation DVD from the Baruwa website, you can:

- Burn it to a physical CD/DVD
- Use it as an ISO image for installation in virtual environments.

### 3.2 Making an Installation CD/DVD

You can make an installation DVD using the CD or DVD burning software on your computer.

Make sure that your disc burning software is capable of burning discs from image files. Although this is true of most disc burning software, exceptions exist. In particular, note that the disc burning feature built into Windows XP and Windows Vista cannot burn DVDs; and that earlier Windows operating systems did not have any disc burning capability installed by default at all. Therefore, if your computer has a Windows operating system prior to Windows 7 installed on it, you need separate software for this task. Examples of popular disc burning software for Windows that you might already have on your computer include Nero Burning ROM and Roxio Creator.

Most widely used disc burning software for Linux, such as Brasero and K3b has the built-in ability to burn discs from ISO image files.

The exact series of steps that produces a DVD from an ISO image file varies greatly from computer to computer, depending on the operating system and disc burning software installed. Consult your disc burning software's documentation for detailed information on burning DVDs.



## PLANNING FOR INSTALLATION

### 4.1 Hardware Compatibility

Hardware compatibility is particularly important if you have an older system or a system that you built yourself. Baruwa Enterprise Edition 6.6.1 should be compatible with most hardware in systems that were factory built within the last two years.

However, hardware specifications change almost daily, so it is difficult to guarantee that your hardware is 100% compatible.

One consistent requirement is your processor. Baruwa Enterprise Edition 6.6.1 supports, at minimum, all 64-bit implementations of Intel micro-architecture from P6 and onwards and AMD 64-bit micro-architecture from Athlon and onwards.

### 4.2 Supported Installation Hardware

For installation of Baruwa Enterprise Edition on AMD64 and Intel 64 systems, The following installation targets are supported:

- Hard drives connected by a standard internal interface, such as SCSI, SATA, or SAS
- BIOS/firmware RAID devices
- Fibre Channel Host Bus Adapters and multipath devices are also supported. This need to be done under expert mode and Vendor-provided drivers may be required for certain hardware.

The following virtualization technologies are supported:

- Xen block devices on Intel processors in Xen virtual machines.
- VirtIO block devices on Intel processors in KVM virtual machines.

#### 4.2.1 Minimum and Recommended Hardware

The bare minimum system requirements for all in one system are:

- 4GB RAM
- Multicore Intel/AMD 64-bit CPU
- 5 GB OS
- 10 GB Data

The recommended system requirements for all in one system are:

- 8GB RAM
- Multicore Intel/AMD 64-bit CPU
- 5 GB OS
- 100 GB Data

---

**Note:** The amount of resources allocated to system is directly related to the amount of email the system will be processing as well as the number of users connected to the web interface. Please scope your system resources based on the projections of email and web traffic.

---

## 4.3 RAID and Other Disk Devices

Baruwa Enterprise Edition 6.6.1 uses mdraid instead of dmraid for installation onto Intel BIOS RAID sets. These sets are detected automatically, and devices with Intel ISW metadata are recognized as mdraid instead of dmraid. Note that the device node names of any such devices under mdraid are different from their device node names under dmraid. Therefore, special precautions are necessary when you migrate systems with Intel BIOS RAID sets.

Local modifications to `/etc/fstab`, `/etc/crypttab` or other configuration files which refer to devices by their device node names will not work in Baruwa Enterprise Edition 6.6.1. Before migrating these files, you must therefore edit them to replace device node paths with device UUIDs instead. You can find the UUIDs of devices with the `blkid` command.

### 4.3.1 Hardware Raid

RAID, or Redundant Array of Independent Disks, allows a group, or array, of drives to act as a single device. Configure any RAID functions provided by the mainboard of your computer, or attached controller cards, before you begin the installation process. Each active RAID array appears as one drive within Baruwa Enterprise Edition.

### 4.3.2 Software Raid

You can use the Baruwa Enterprise Edition installation program to create Linux software RAID arrays, where RAID functions are controlled by the operating system rather than dedicated hardware.

In order to configure software raid you need to select the Expert install option at the boot screen.

### 4.3.3 Disk Space

Before you start the installation process, you must:

- have enough unpartitioned disk space for the installation
- have one or more partitions that may be deleted

The standard partitioning scheme which is generated when the expert mode is not selected is as follows:

Mount point	Size	FS	Comments
/	5GB	EXT4	Root partition
Swap	3GB		Max size 3GB
/var		XFS	Rest of the disk.

### 4.3.4 Partitioning scheme

Should you choose to run the install in expert mode, please partition the system to provide the bulk of disk space to the /var partition.

It is advisable to have the /var partition on a standalone partition with a file system that does not limit the number of files such as EXT4 and XFS.

---

**Note:** There is no need to create a /home partition for this system, as no home directories will be created. The default partition scheme does create a /home partition with the largest allocation, you need to change that.

---

## 4.4 Network Firewall

Baruwa Enterprise Edition requires the following ports open to allow for proper functioning.

PORT	PROTOCOL	DIRECTION	DESCRIPTION
25	TCP	INBOUND/OUTBOUND	SMTP TRAFFIC
465	TCP	INBOUND	TLS SMTP TRAFFIC
587	TCP	INBOUND	SMTP SUBMISSION
80	TCP	INBOUND/OUTBOUND	WEB TRAFFIC
443	TCP	INBOUND/OUTBOUND	WEB TRAFFIC
53	TCP/UDP	OUTBOUND	DNS TRAFFIC
123	UDP	OUTBOUND	NTP TRAFFIC
2703	TCP	OUTBOUND	RAZOR TRAFFIC
24441	TCP/UDP	OUTBOUND	PYZOR TRAFFIC
873	TCP/UDP	OUTBOUND	UPDATES TRAFFIC

## 4.5 DNS

DNS is critical for the operation of any email system, Baruwa Enterprise Edition is no exception.

A local caching server is installed and setup after the configuration has been completed. This local caching server is independent of your other DNS systems and resolves from the root. If your DNS zones are not resolvable externally then this local caching system will not be able to resolve those names. To enable you resolve names that are only configured locally on your other DNS systems you need to add forward zones for those domains in the /etc/named.conf file and restart the service.

Baruwa Enterprise Edition is designed to use this local caching server, any changes to the /etc/resolv.conf file to use external DNS servers will be overwritten.

The use of public DNS servers such as Google, OpenDNS or your ISP's name servers is discouraged as these servers will be throttled by URIBL and DNSBL servers thus leading to poor performance of your system.

If however you would like to use you own DNS infrastructure that does not process excessive URIBL and DNSBL queries then, you can setup forwarding to your name servers in the /etc/named.conf file and restart the service.

## 4.6 Clustering

If you would like to setup a cluster system, please review the *Clustering* chapter then, review the supported *Topologies* and the available *System Profiles* and choose which ones to implement prior to starting the installation.

The recommended installation order for distributed topologies is:

1. Database System
2. Search Index System
3. Message Queue System
4. Cache System
5. Nodes

## 4.7 System Profiles

Baruwa Enterprise Edition can be installed on a standalone server or distributed with various components on different servers. A distributed setup is required if you want to run a cluster.

The available system profiles are described below.

### 4.7.1 Standalone System

This is the default setup and is used for non clustered setups. All the components are installed on one server. Choose this option if you only want to run one server.

### 4.7.2 Backend System

This setup installs all the backend components on to one server, the backend components that are installed are:

- Database Server
- Message Queue Server
- Search Index Server
- Cache Server

This setup can be used with a clustered setup of several nodes. You have to setup one server as a backend system in a basic cluster setup.

### 4.7.3 Web and Mail System

This is a frontend system it provides the mail and web interfaces, mail is delivered to the server and at the same time it serves as the web interface for both administration as well as end user access. This system requires a backend system or distributed backend systems. You can have several of these nodes scaling up or down as demand grows or drops.

### 4.7.4 Mail System

This is a front-end system that is dedicated to processing mail, it does not provide a web interface for administration as well as user access. You setup this kind of system if you want dedicated servers processing mail only. You can have several of these nodes scaling up or down as demand grows or drops.



### **4.7.5 Web Interface System**

This is a front-end system that is dedicated to providing web interface access for administration as well as user access. You setup this kind of system if you want dedicated servers providing only web access. You can have several of these nodes scaling up or down as demand grows or drops.

### **4.7.6 Search Index System**

This is a backend server in a distributed system, it provides the backend indexing functionality. You setup this profile if you want a dedicated server providing search indexing.

### **4.7.7 Database System**

This is a backend server in a distributed system, it provides the backend database functionality. You setup this profile if you want a dedicated server providing database functionality.

### **4.7.8 Message Queue System**

This is a backend server in a distributed system, it provides the message queue functionality. You setup this profile if you want a dedicated server providing message queue functionality.

### **4.7.9 Cache System**

This is a backend server in a distributed system, it provides the cache functionality. You setup this profile if you want a dedicated server providing cache functionality.

### **4.7.10 Expert installation**

This profile is for users would would like to setup the system by themselves, only use this if you know what you are doing.



## INSTALLATION

---

**Note:** This section describes a new installation, if you are upgrading from an older version please refer to the *Upgrading* section.

---

### 5.1 Overview

To install Baruwa Enterprise Edition from a DVD, place the DVD in your DVD drive and boot your system from the DVD.

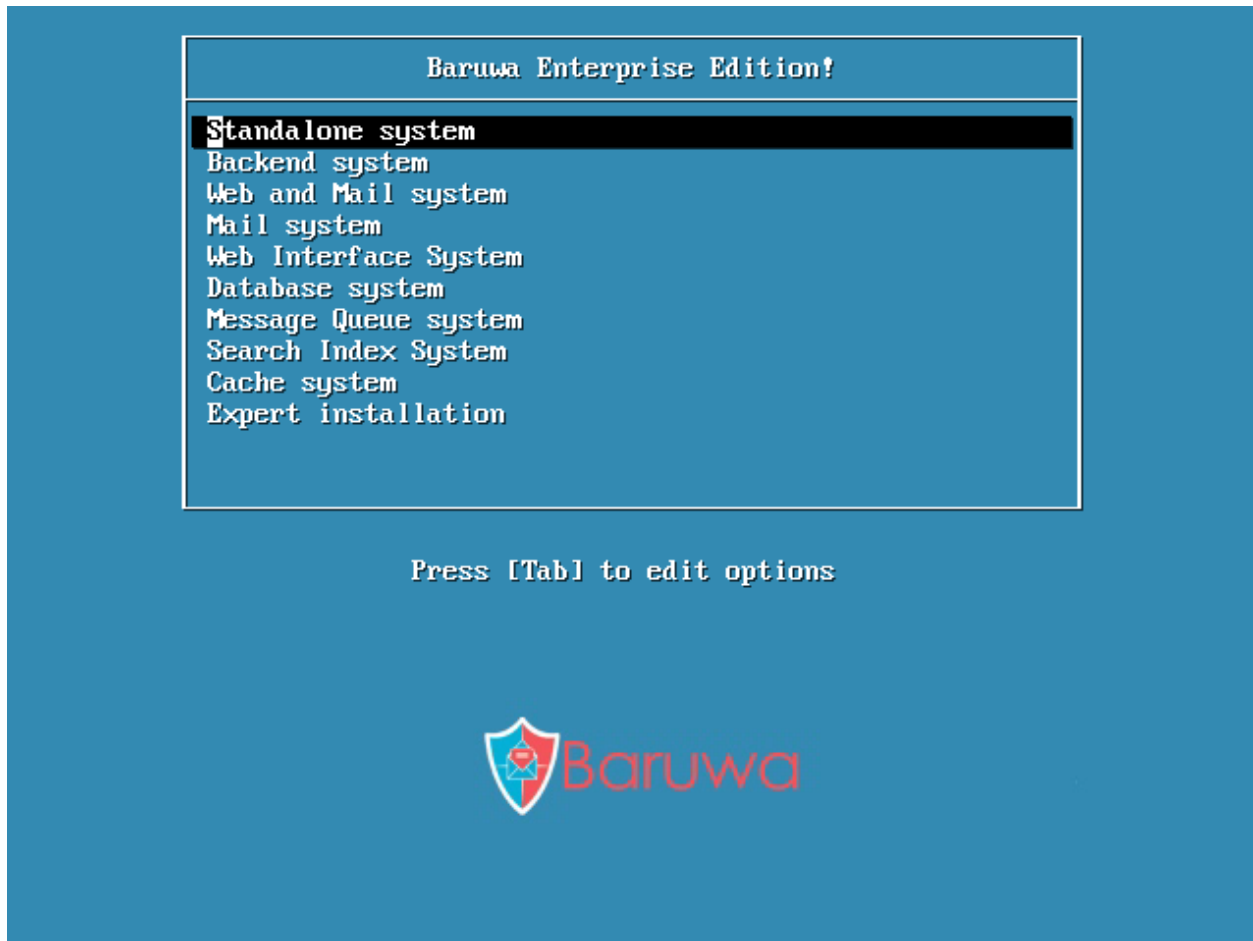
The installation program then probes your system and attempts to identify your DVD drive. It starts by looking for an IDE (also known as an ATAPI) DVD drive.

If your DVD drive is not detected, and it is a SCSI DVD, the installation program prompts you to choose a SCSI driver. Choose the driver that most closely resembles your adapter. You may specify options for the driver if necessary; however, most drivers detect your SCSI adapter automatically.

If the DVD drive is found and the driver loaded, the installer will present you with the option to perform a media check on the DVD. This will take some time, and you may opt to skip over this step. However, if you later encounter problems with the installer, you should reboot and perform the media check before calling for support. From the media check dialog, continue to the next stage of the installation process.

### 5.2 Boot Menu

The boot media displays a graphical boot menu with several options. If no key is hit within 60 seconds, the default boot option runs. To choose the default, either wait for the timer to run out or hit Enter on the keyboard. To select a different option than the default, use the arrow keys on your keyboard, and hit Enter when the correct option is highlighted. If you want to customize the boot options for a particular option, press the Tab key. To access the boot: prompt at which you can specify custom boot options, press the Esc key and then hit Enter.



The following boot menu options are available, these options are install profiles you need to select specific profile you would like to install. The default profile is `Standalone` which installs the full Baruwa Enterprise Edition system to a single server.

- Standalone System
- Backend System
- Web and Mail System
- Mail System
- Web Interface System
- Search Index System
- Database System
- Message Queue System
- Cache System
- Expert installation

The install profiles are described in detail at *System Profiles*

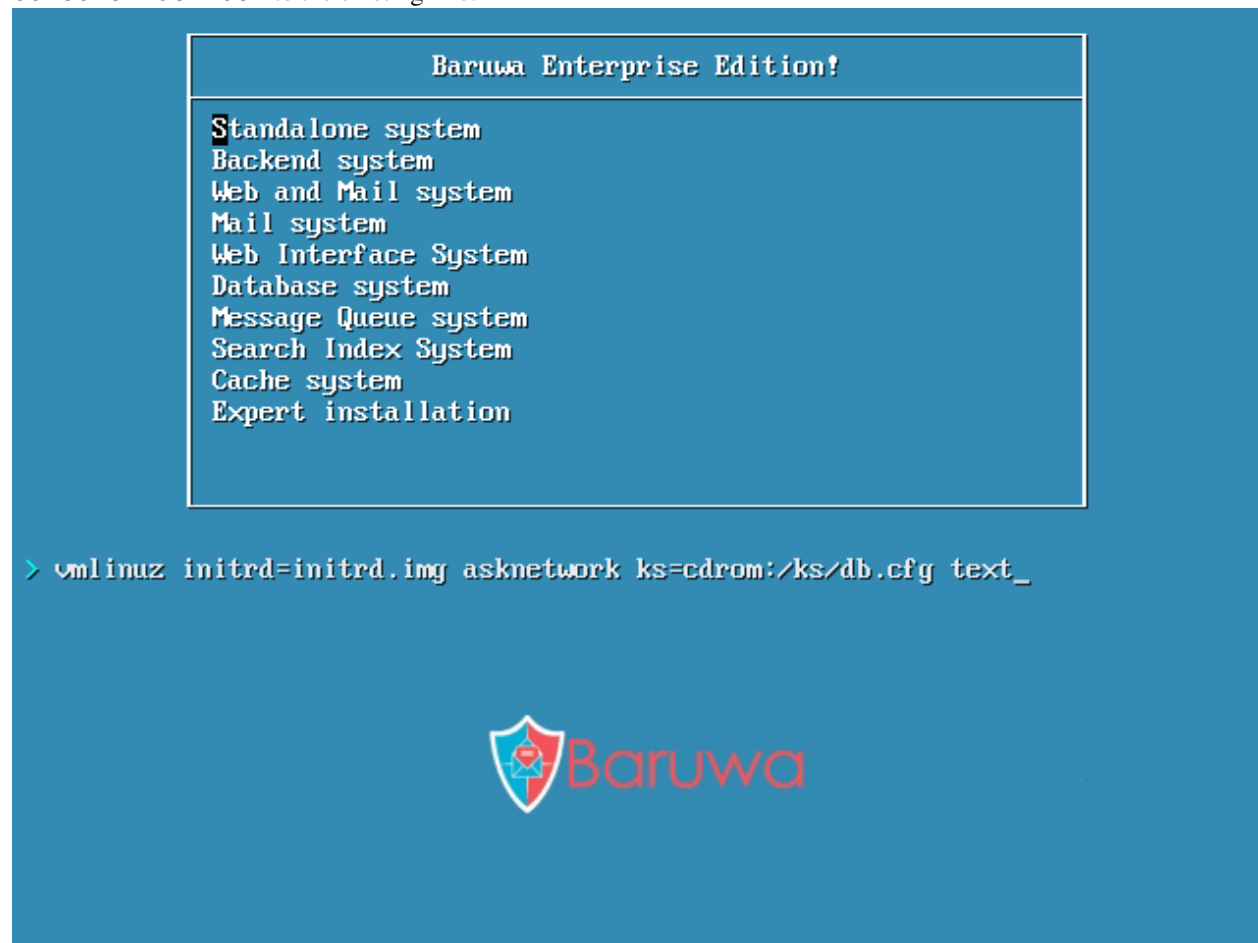
### 5.2.1 Additional Boot Options

While it is easiest to boot using a DVD and perform a graphical installation, sometimes there are installation scenarios where booting in a different manner may be needed. This section discusses additional boot options available for Baruwa Enterprise Edition.

To perform a text mode installation, select the install profile and press the Tab key then append `text` to the existing line.

ISO images have an SHA256 checksum embedded in them. To test the checksum integrity of an ISO image, select the install profile and press the Tab key then append `mediacheck` to the existing line.

If you need to perform the installation in serial mode, select the install profile and press the Tab key then append `console=<device>` to the existing line.



### 5.2.2 Verifying Media

The DVD offers an option to verify the integrity of the media. Recording errors sometimes occur while producing DVD media. An error in the data for package chosen in the installation program can cause the installation to abort. To minimize the chances of data errors affecting the installation, verify the media before installing.

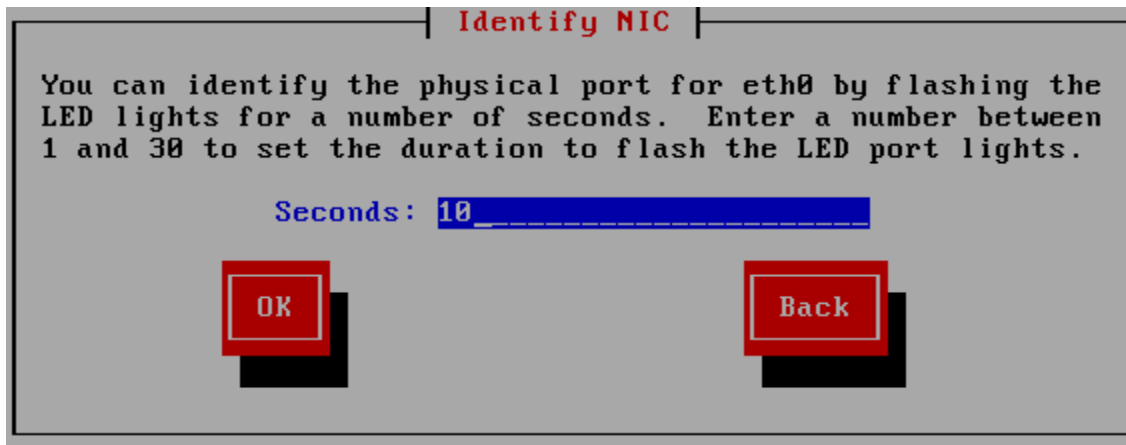
If the verification succeeds, the installation process proceeds normally. If the process fails, create a new DVD using the ISO image you downloaded earlier.

## 5.3 Network Configuration

If your system has more than one network device, the installer presents you with a list of all available devices and prompts you to select one to use during installation. If your system only has a single network device, the installer automatically selects it and does not present this dialog.



If you are not sure which device in the list corresponds to which physical socket on the system, select a device in the list then press the Identify button. The Identify NIC dialog appears.



The sockets of most network devices feature an activity light (also called a link light) — an LED that flashes to indicate that data is flowing through the socket. The installer can flash the activity light of the network device that you selected in the Networking Device dialog for up to 30 seconds. Enter the number of seconds that you require, then press OK. When the installer finishes flashing the light, it returns you to the Networking Device dialog.

When you select a network device, the installer prompts you to choose how to configure TCP/IP.

### 5.3.1 Dynamic IP configuration (DHCP)

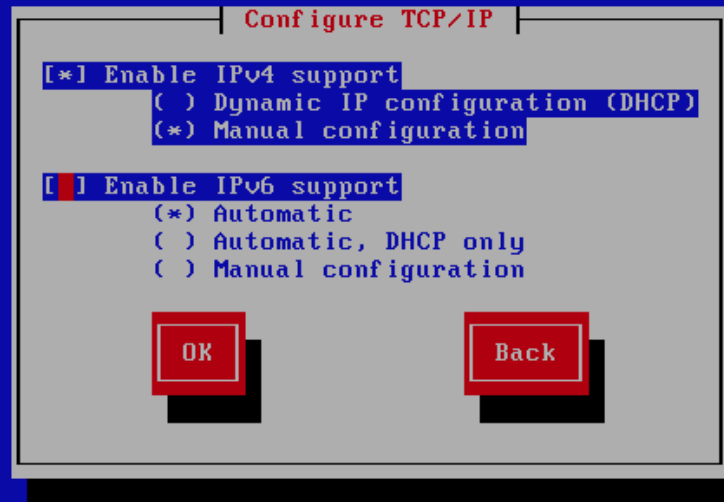
The installer uses DHCP running on the network to supply the network configuration automatically.

### 5.3.2 Manual configuration

The installer prompts you to enter the network configuration manually, including the IP address for this system, the netmask, the gateway address, and the DNS address.

The installer supports the IPv4 and IPv6 protocols. However, if you configure an interface to use both IPv4 and IPv6, the IPv4 connection must succeed or the interface will not work, even if the IPv6 connection succeeds.

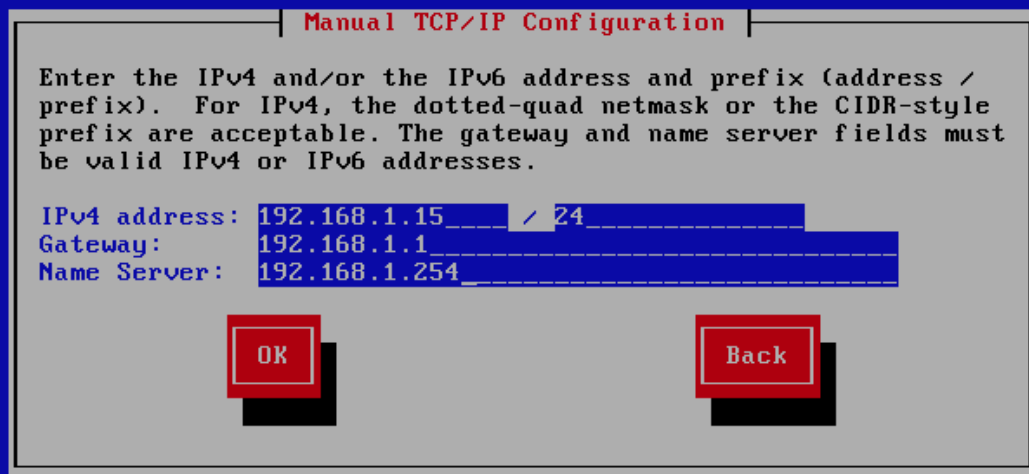
Welcome to Baruwa for x86\_64



<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

The installer prompts you to provide the details in the Manual TCP/IP Configuration dialog:

Welcome to Baruwa for x86\_64



<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Enter the details for your network, then press OK.

You can now proceed to either *Graphical Mode Installation* or *Text Mode Installation*

## 5.4 Graphical Mode Installation

### 5.4.1 Initializing the Hard Disk

If no readable partition tables are found on existing hard disks, the installation program asks to initialize the hard disk. This operation makes any existing data on the hard disk unreadable. If your system has a brand new hard disk with no operating system installed, or you have removed all partitions on the hard disk, click *Yes, discard any data*.

The installation program presents you with a separate dialog for each disk on which it cannot read a valid partition table.

Check the `Apply my choice to all devices with undetected partitions or filesystems` checkbox to apply the same answer to all devices.



### 5.4.2 Time Zone Configuration

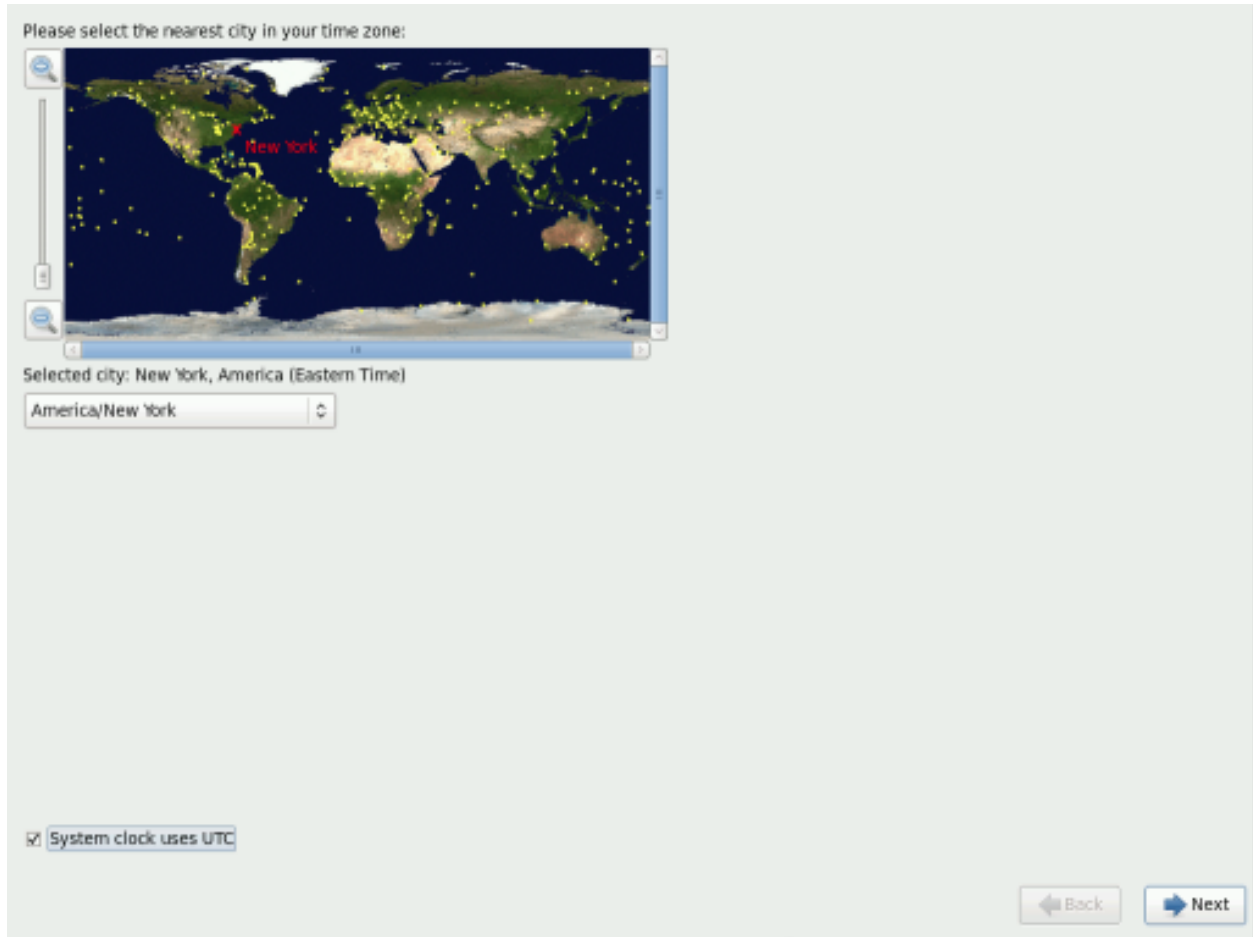
Set your time zone by selecting the city closest to your computer’s physical location. Click on the map to zoom in to a particular geographical region of the world.

Specify a time zone even if you plan to use NTP (Network Time Protocol) to maintain the accuracy of the system clock.

From here there are two ways for you to select your time zone:

- Using your mouse, click on the interactive map to select a specific city (represented by a yellow dot). A red X appears indicating your selection.
- You can also scroll through the list at the bottom of the screen to select your time zone. Using your mouse, click on a location to highlight your selection.



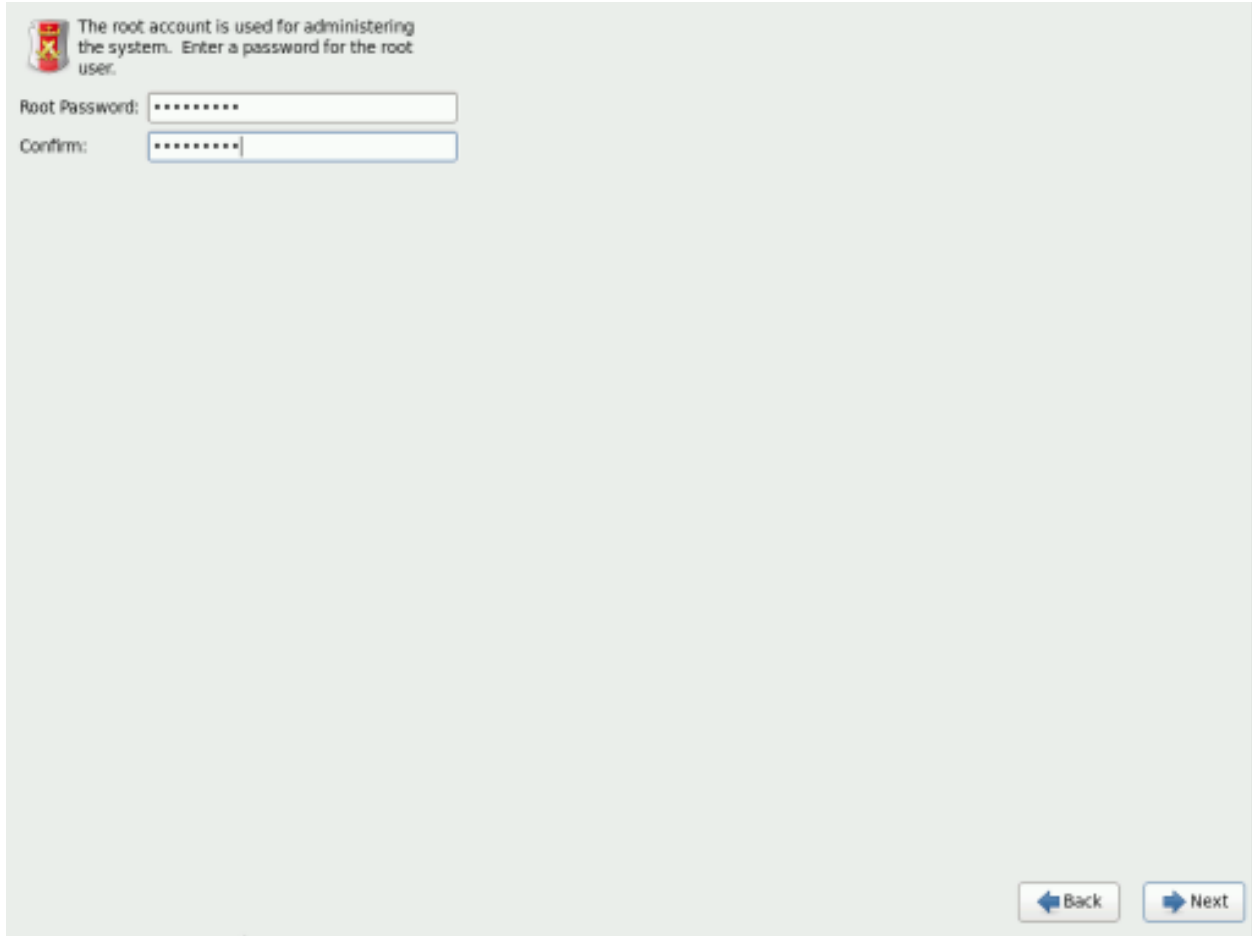


Select System clock uses UTC. The system clock is a piece of hardware on your computer system. Baruwa Enterprise Edition uses the timezone setting to determine the offset between the local time and UTC on the system clock. This behaviour is standard for systems that use UNIX, Linux, and similar operating systems.

Click Next to proceed.

### 5.4.3 Set the Root Password

Setting up a root account and password is one of the most important steps during your installation. The root account is used to install packages, upgrade packages, and perform most system maintenance. Logging in as root gives you complete control over your system.



The installation program prompts you to set a root password for your system. You cannot proceed to the next stage of the installation process without entering a root password.

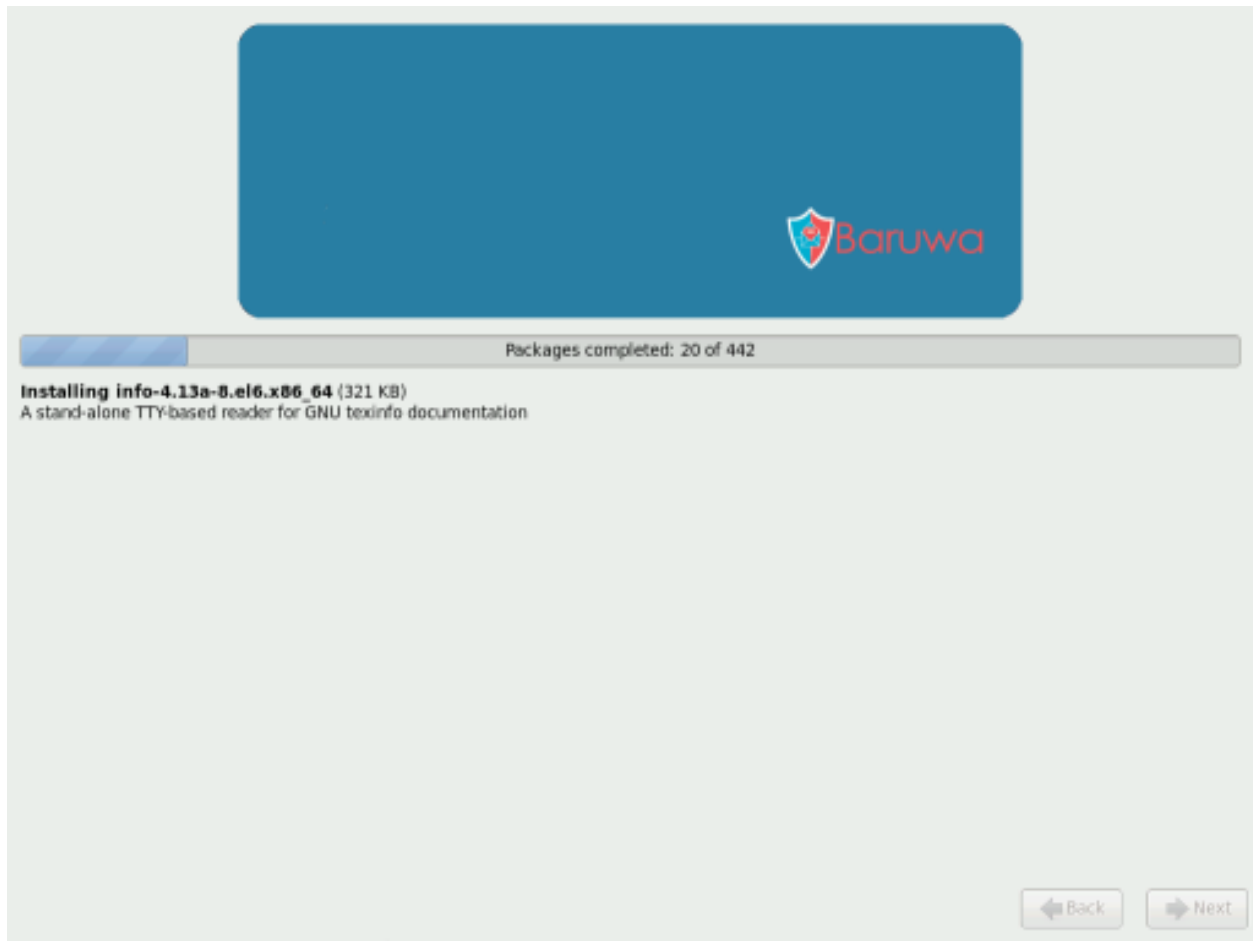
The root password must be at least six characters long; the password you type is not echoed to the screen. You must enter the password twice; if the two passwords do not match, the installation program asks you to enter them again.

You should make the root password something you can remember, but not something that is easy for someone else to guess. Your name, your phone number, qwerty, password, root, 123456, and ant eater are all examples of bad passwords. Good passwords mix numerals with upper and lower case letters and do not contain dictionary words: Aard387vark or 420BmttNT, for example. Remember that the password is case-sensitive. If you write down your password, keep it in a secure place. However, it is recommended that you do not write down this or any password you create.

#### 5.4.4 Installing Packages

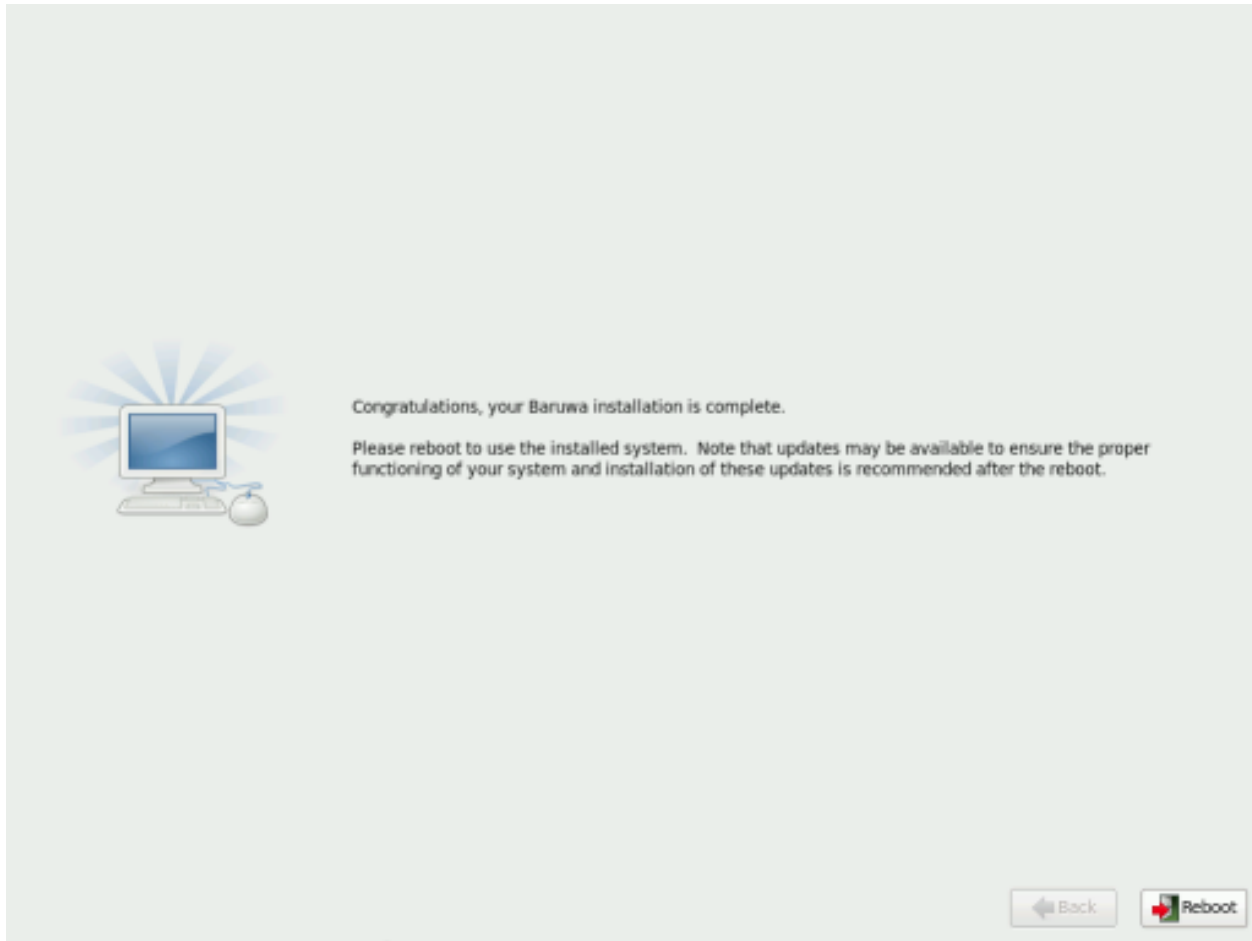
At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the profile you have selected and your computer's speed.

Baruwa Enterprise Edition reports the installation progress on the screen as it writes the selected packages to your system.



For your reference, a complete log of your installation can be found in `/root/install.log` once you reboot your system.

After installation completes, select Reboot to restart your computer. Baruwa Enterprise Edition ejects any loaded discs before the computer reboots.



### 5.4.5 Installation Complete

Congratulations! Your Baruwa Enterprise Edition installation is now complete!

The installation program prompts you to prepare your system for reboot. Remember to remove any installation media if it is not ejected automatically upon reboot.

After your computer's normal power-up sequence has completed, Baruwa Enterprise Edition loads and starts.

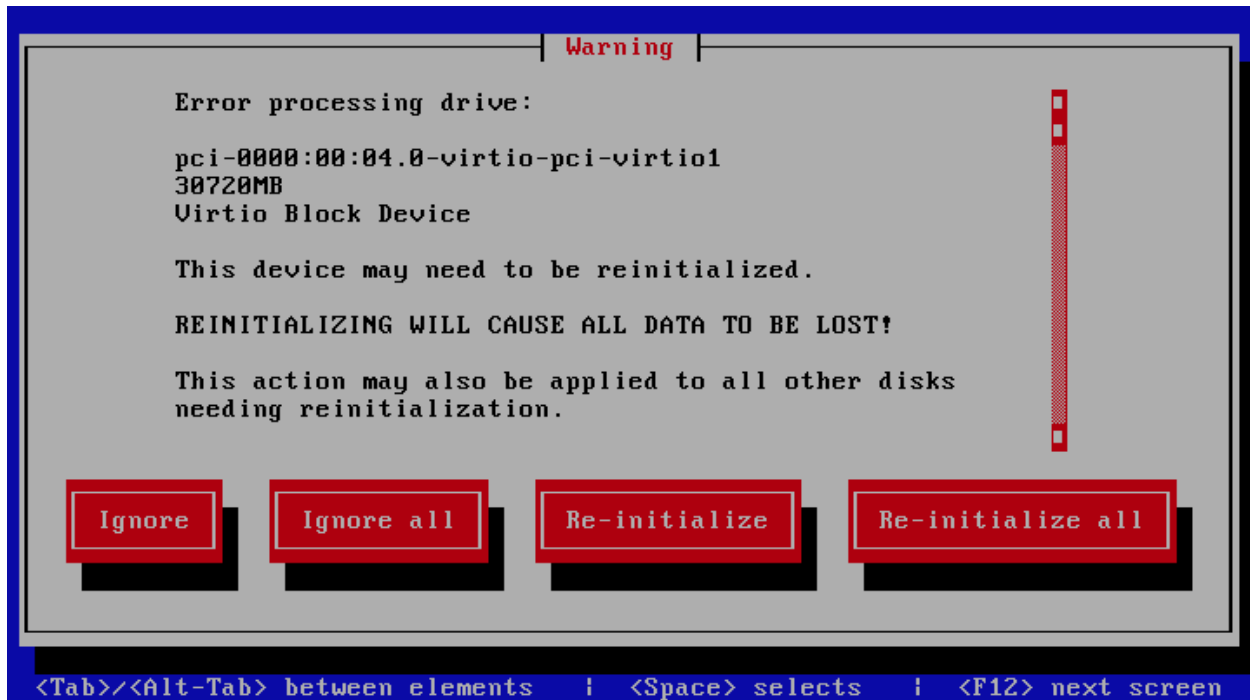
## 5.5 Text Mode Installation

To install in text mode you need to modify the boot options as described in *Additional Boot Options*

### 5.5.1 Initializing the Hard Disk

If no readable partition tables are found on existing hard disks, the installation program asks to initialize the hard disk. This operation makes any existing data on the hard disk unreadable. If your system has a brand new hard disk with no operating system installed, or you have removed all partitions on the hard disk, click `Re-initialize drive`.

The installation program presents you with a separate dialog for each disk on which it cannot read a valid partition table. Click the `Ignore all` button or `Re-initialize all` button to apply the same answer to all devices.

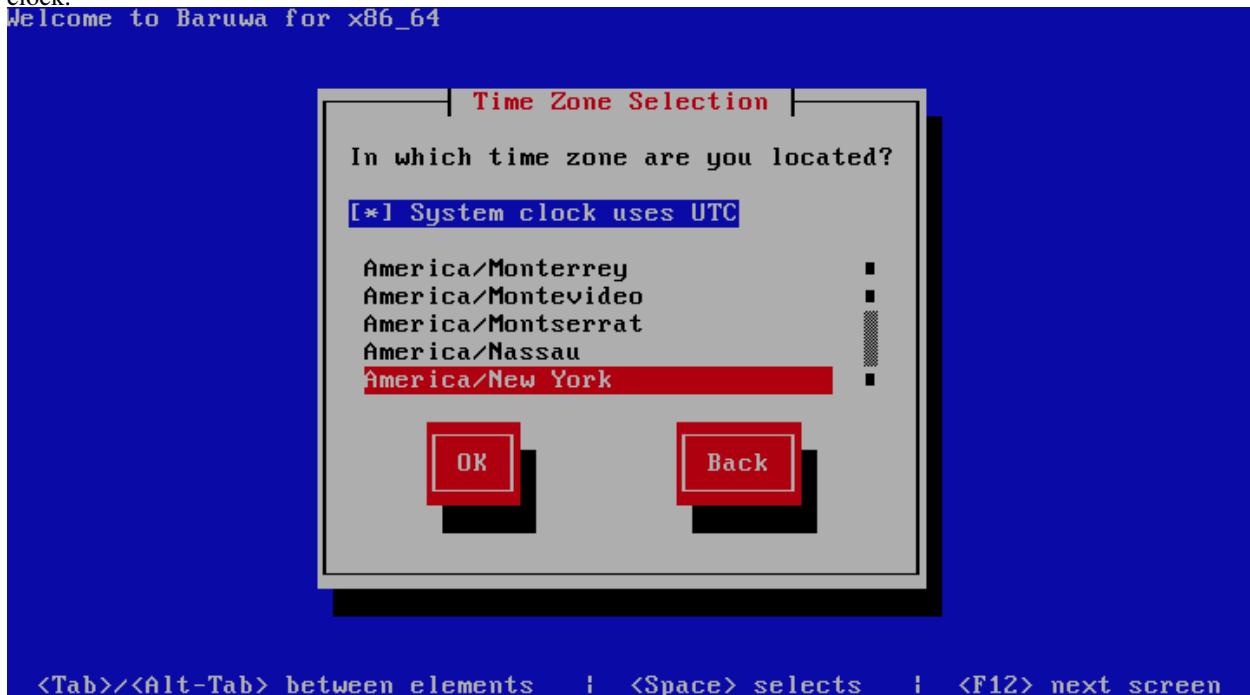


## 5.5.2 Time Zone Configuration

Set your time zone by selecting the city closest to your computer's physical location.

Specify a time zone even if you plan to use NTP (Network Time Protocol) to maintain the accuracy of the system clock.

Welcome to Baruwa for x86\_64

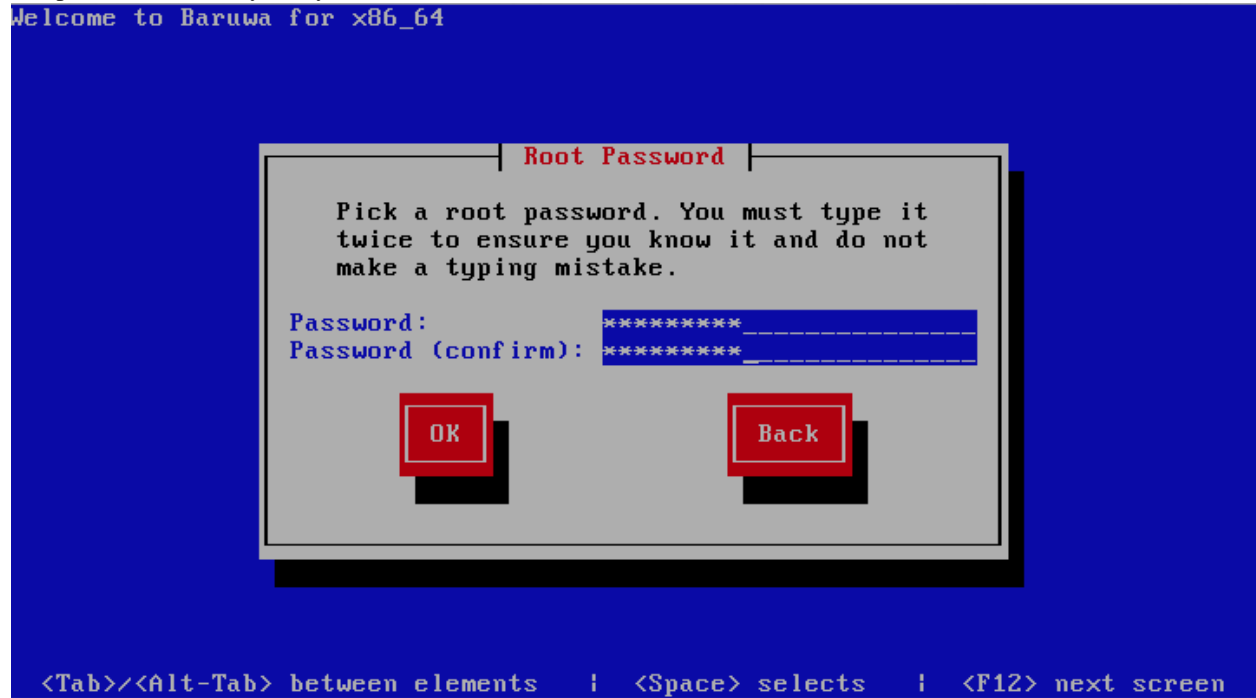


Select System clock uses UTC. The system clock is a piece of hardware on your computer system. Baruwa Enterprise Edition uses the timezone setting to determine the offset between the local time and UTC on the system clock. This

behaviour is standard for systems that use UNIX, Linux, and similar operating systems.

### 5.5.3 Set the Root Password

Setting up a root account and password is one of the most important steps during your installation. The root account is used to install packages, upgrade packages, and perform most system maintenance. Logging in as root gives you complete control over your system.



The installation program prompts you to set a root password for your system. You cannot proceed to the next stage of the installation process without entering a root password.

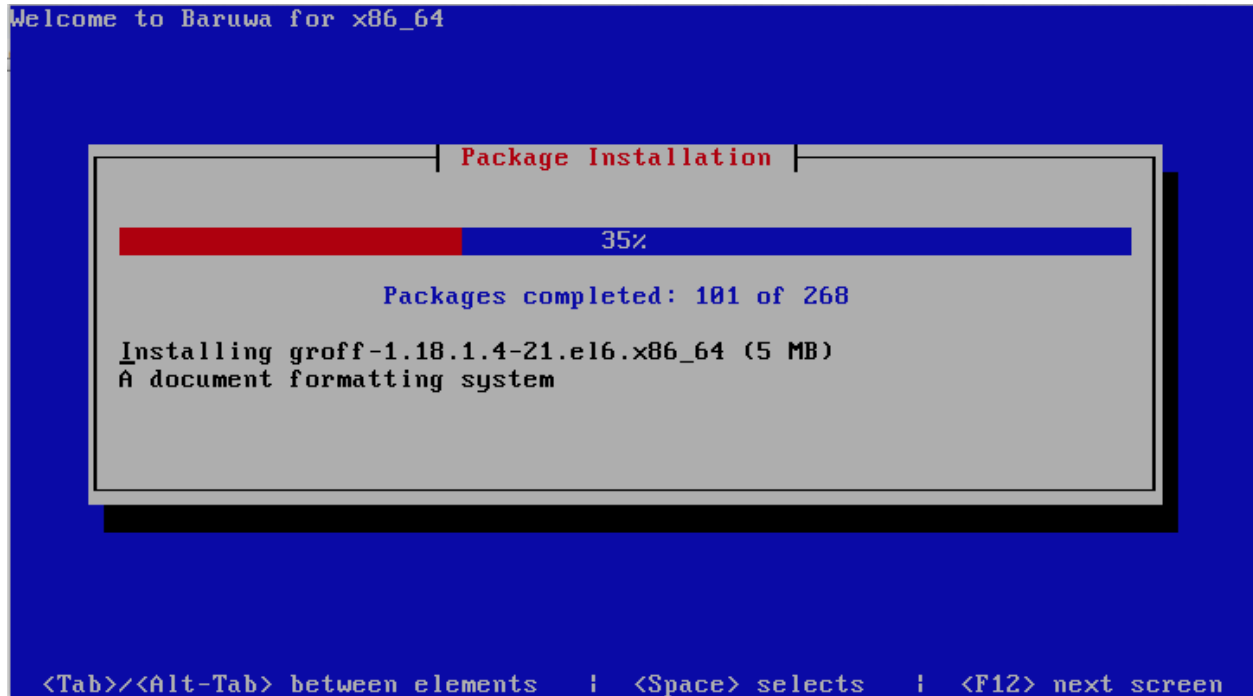
The root password must be at least six characters long; the password you type is not echoed to the screen. You must enter the password twice; if the two passwords do not match, the installation program asks you to enter them again.

You should make the root password something you can remember, but not something that is easy for someone else to guess. Your name, your phone number, qwerty, password, root, 123456, and anteater are all examples of bad passwords. Good passwords mix numerals with upper and lower case letters and do not contain dictionary words: Aard387vark or 420BMttNT, for example. Remember that the password is case-sensitive. If you write down your password, keep it in a secure place. However, it is recommended that you do not write down this or any password you create.

### 5.5.4 Installing Packages

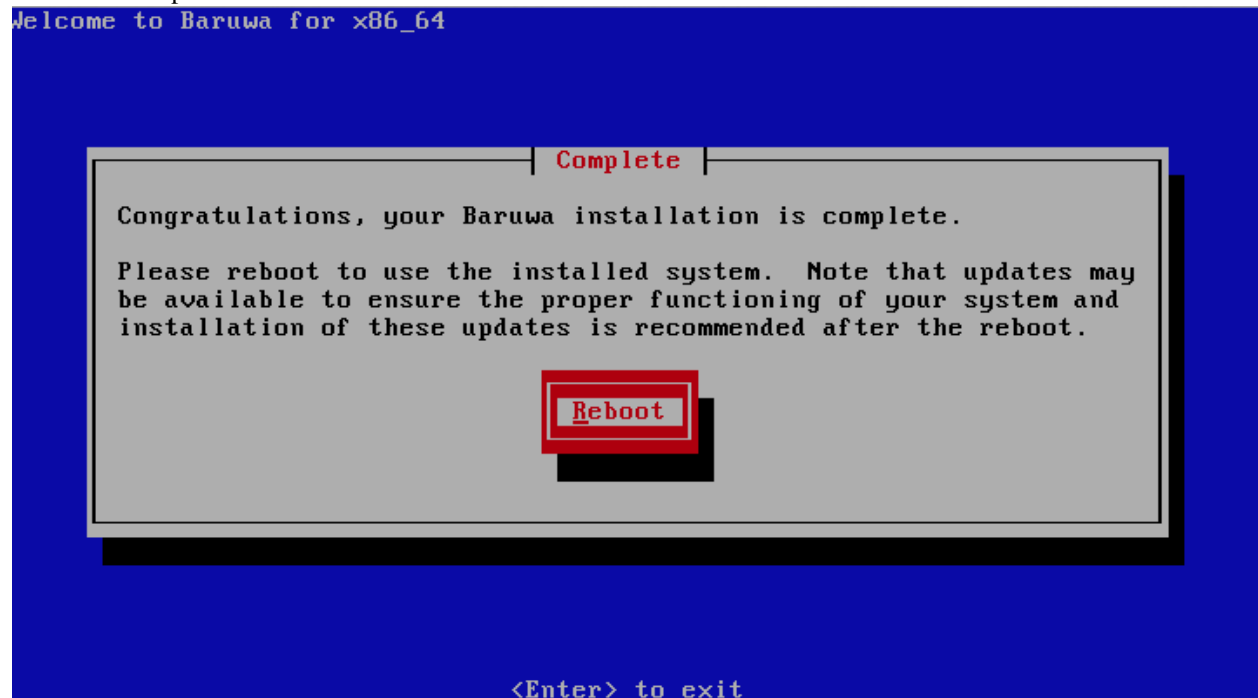
At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the profile you have selected and your computer's speed.

Baruwa Enterprise Edition reports the installation progress on the screen as it writes the selected packages to your system.



For your reference, a complete log of your installation can be found in /root/install.log once you reboot your system.

After installation completes, select Reboot to restart your computer. Baruwa Enterprise Edition ejects any loaded discs before the computer reboots.







## CONFIGURATION

The configuration of Baruwa Enterprise Edition systems has been simplified and fully automated using the `baruwa-setup` utility.

The page describes the configuration of the default standalone system if you are installing a distributed cluster system please refer to *Cluster Configuration*

### 6.1 StandAlone System

This is the default setup and is used for non clustered setups. All the components are installed on one server. Choose this option if you only want to run one server.

### 6.2 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

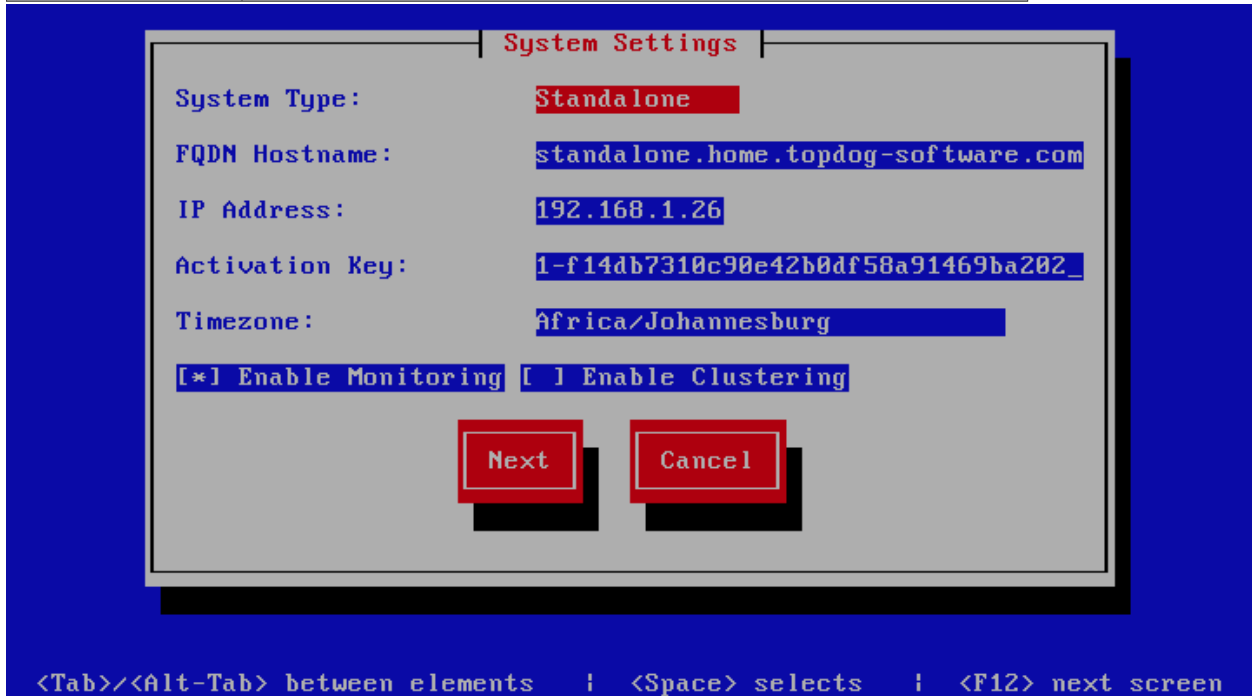
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

#### 6.2.1 System Settings

This screen configures the basic system settings. The description of the options is as follows:

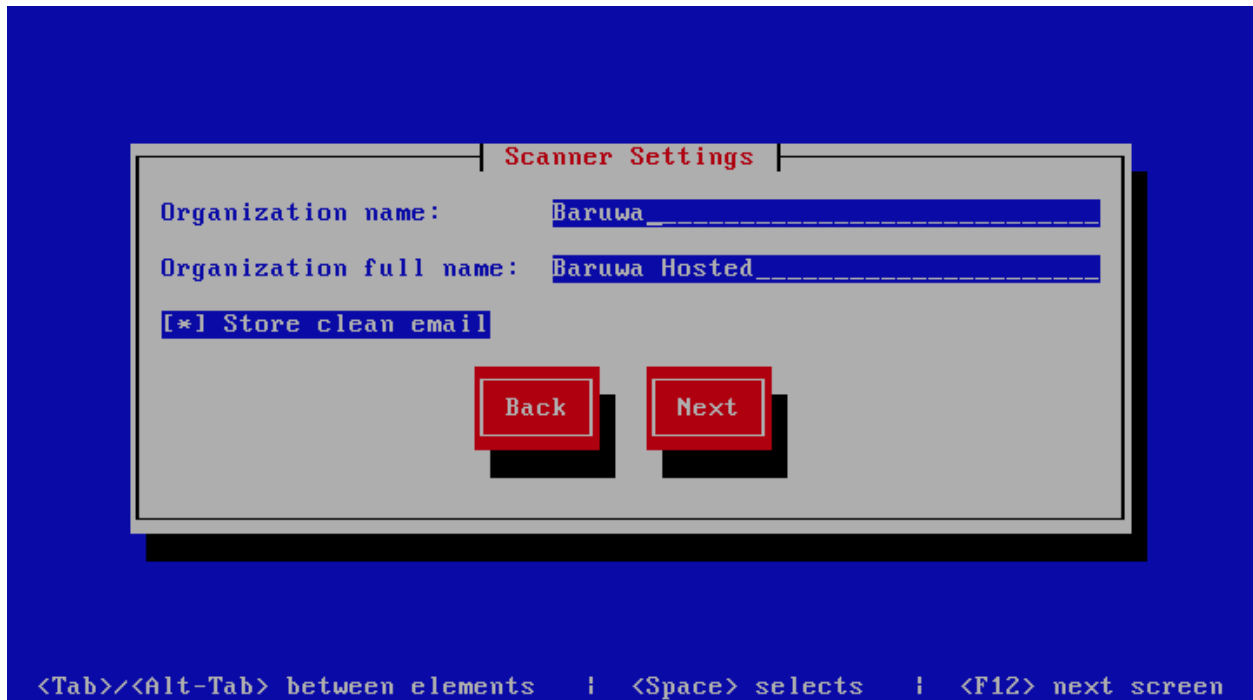
Option	Description
System Type	Set this to Standalone
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service



## 6.2.2 Scanner Settings

This screen sets the email scanner settings, The description of the options is as follows:

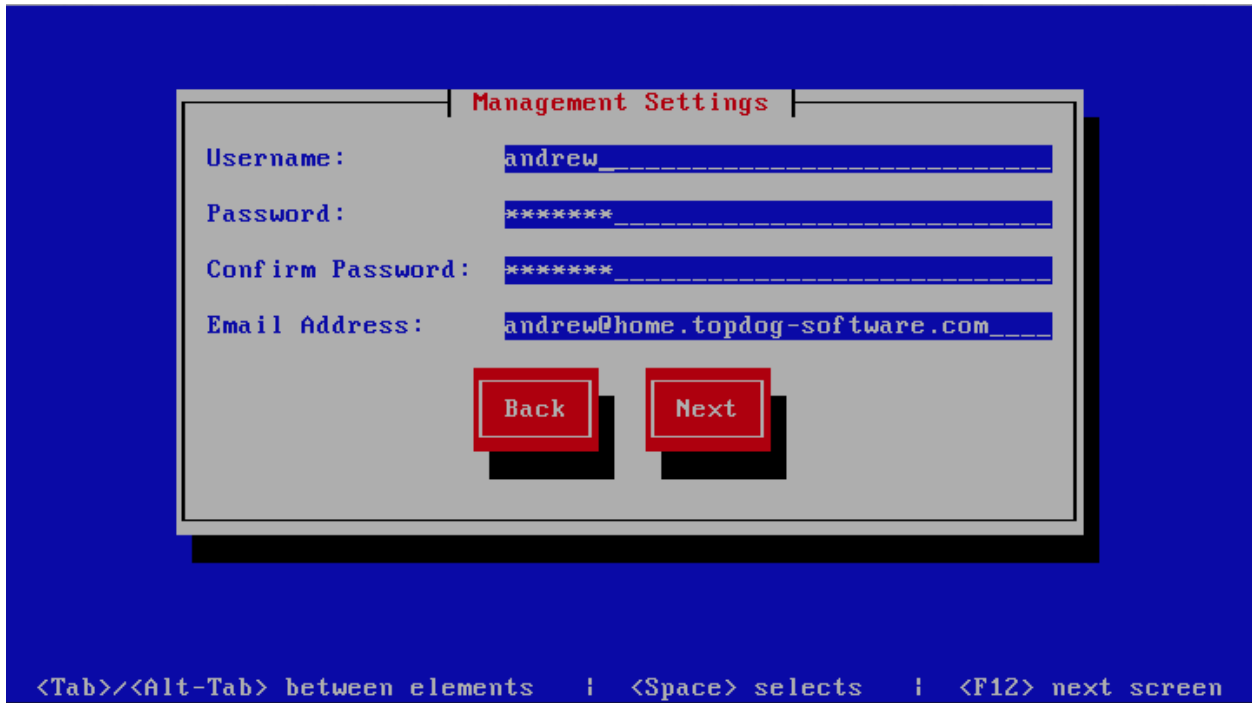
Option	Description
Organization name	<p>Enter a short identifying name for your organisation this is used to make the X-Baruwa headers unique for your organisation Multiple servers within one site should use an identical value here. It must not contain any spaces.</p>
Organization full name	<p>Enter the full name of your organisation, this is used in the signature placed at the bottom of report messages sent by Baruwa. It can include pretty much any text you like. You can make the result span several lines by including “n” sequences in the text. These will be replaced by line-breaks.</p>
Use Shared Quarantine	<p>Check this only if you have setup a shared filesystem for the mail quarantine and configured the server to mount the /var/spool/MailScanner/quarantine directory to it</p>
Store clean mail	<p>Check this if you want to store messages not tagged as SPAM, Use this option only if it is legal in your country</p>



### 6.2.3 Management Settings

The screen sets the management account settings, The description of the options is as follows:

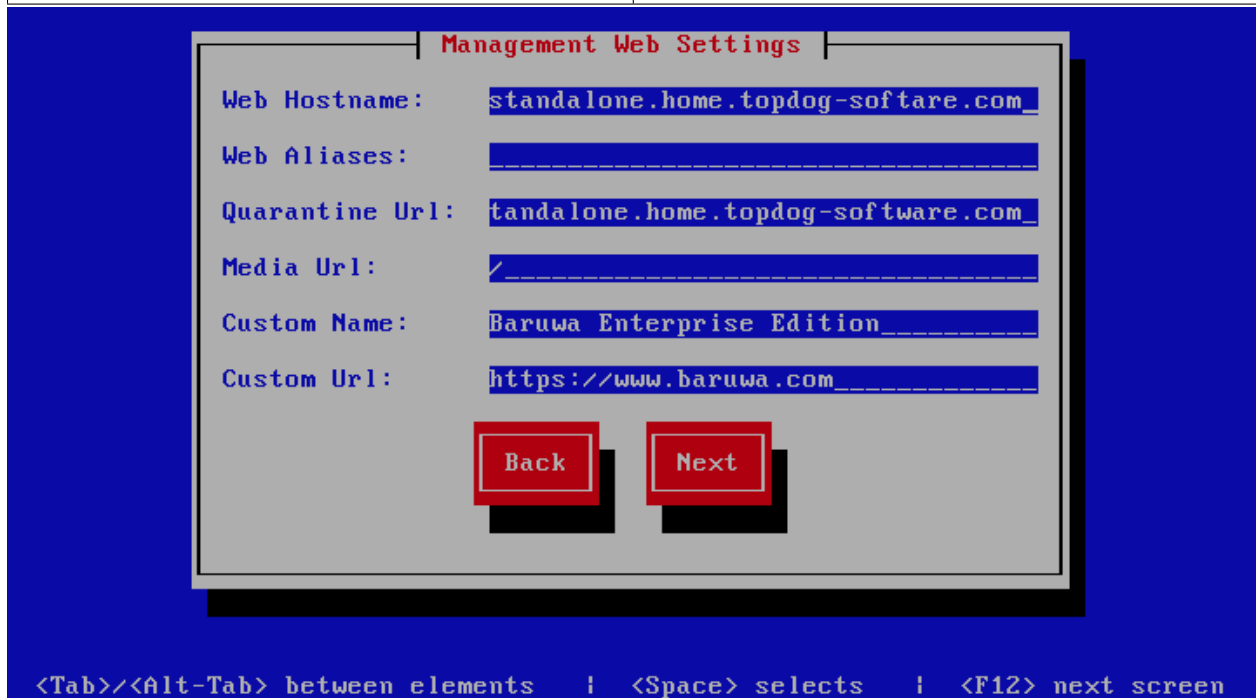
Option	Description
Username	Administrator username
Password	Administrator password, Only strong passwords will be accepted use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address



## 6.2.4 Management Web Settings

The screen sets the management web interface settings, The description of the options is as follows:

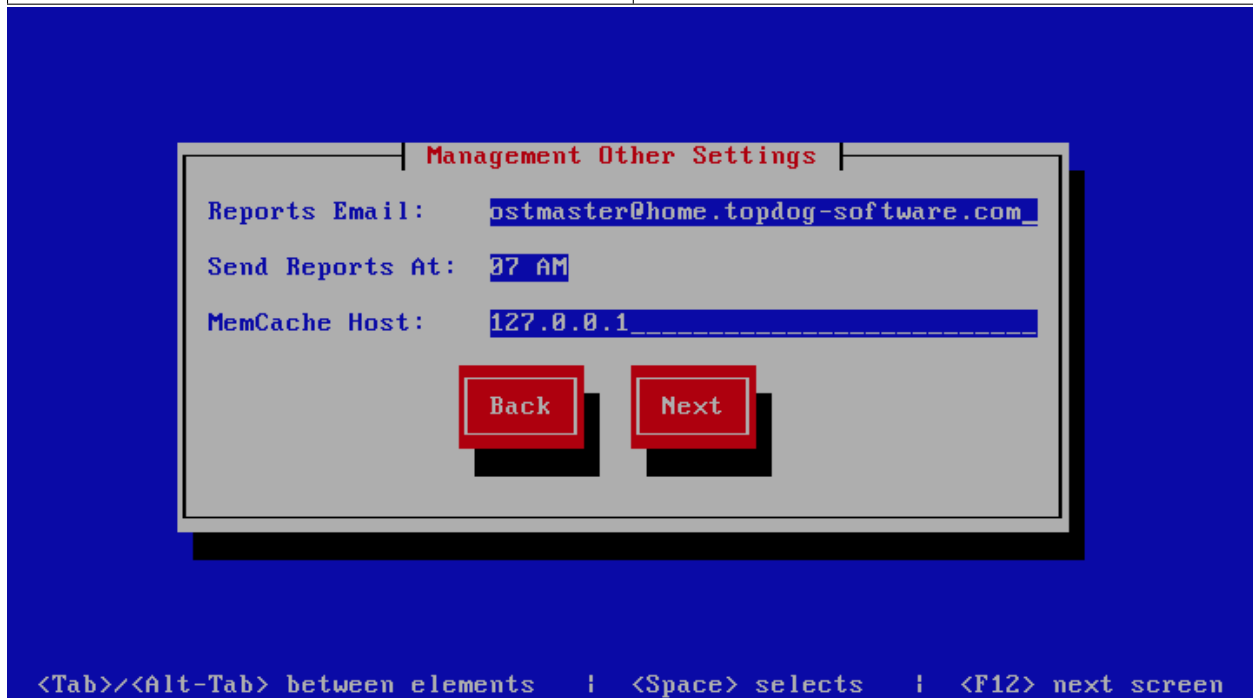
Option	Description
Web Hostname	The hostname to be used to access the web interface
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the web interface as well.
Custom URL	This creates links to your product page within the web interface and email reports that are sent out.



## 6.2.5 Management Other Settings

The screen sets other management settings, The description of the options is as follows:

Option	Description
Reports Email	The email address used to send out email reports
Send Reports At	The hour at which to send reports, this is localized to the users location based on their timezone setting
MemCache Host	The IP address of the Memcache Server



## 6.2.6 Database Settings

The screen sets database settings, The description of the options is as follows:

Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password

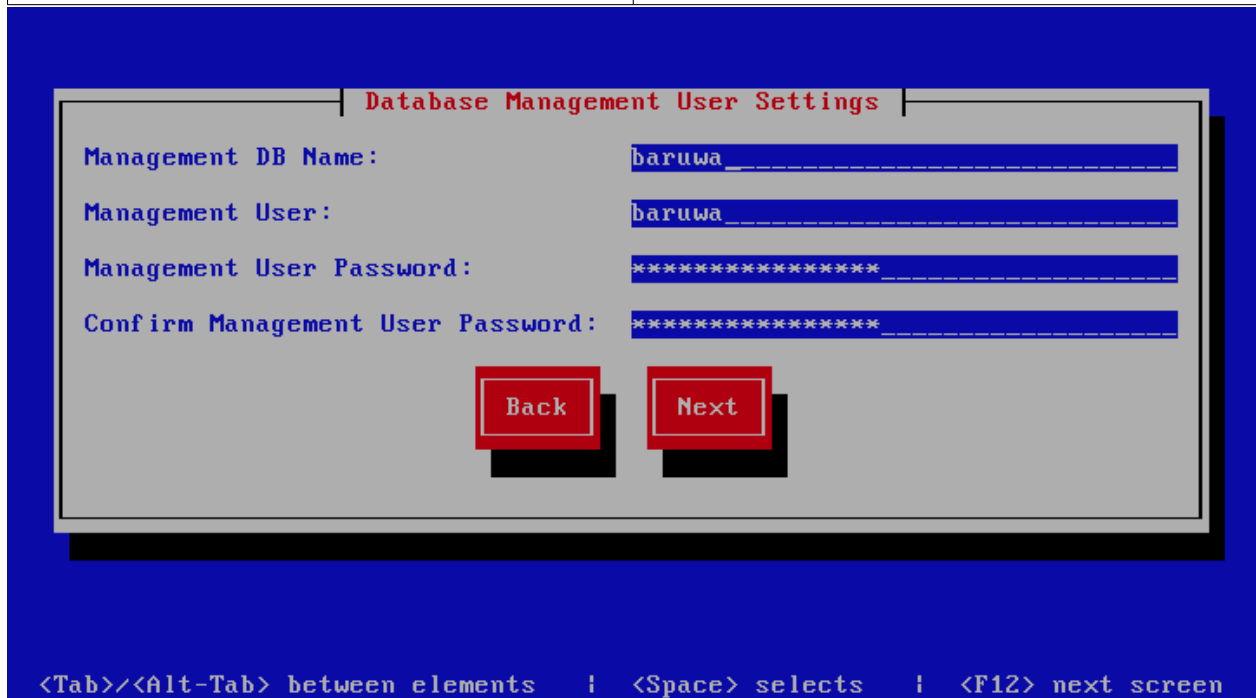


## 6.2.7 Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:



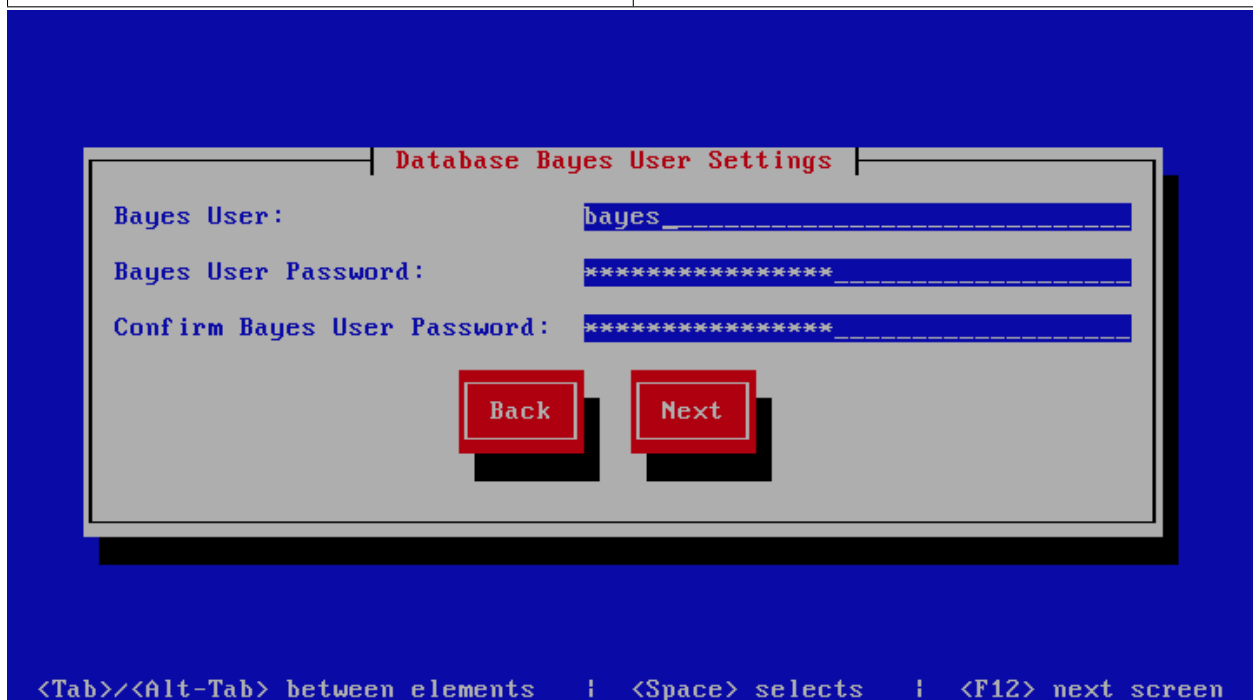
Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password



## 6.2.8 Database Bayes User Settings

The screen sets database bayes user settings, The description of the options is as follows:

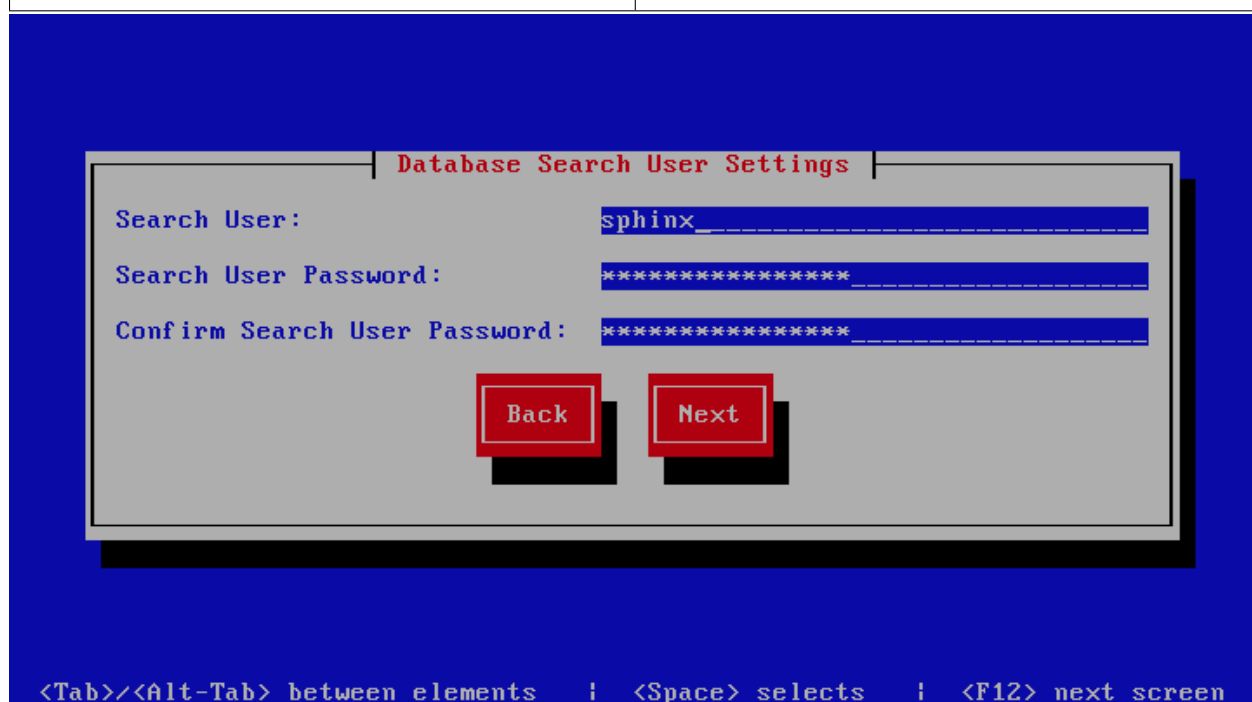
Option	Description
Bayes User	The bayes database username
Bayes User Password	The bayes database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Bayes User Password	Confirm the bayes database user password



### 6.2.9 Database Search User Settings

The screen sets database search user settings, The description of the options is as follows:

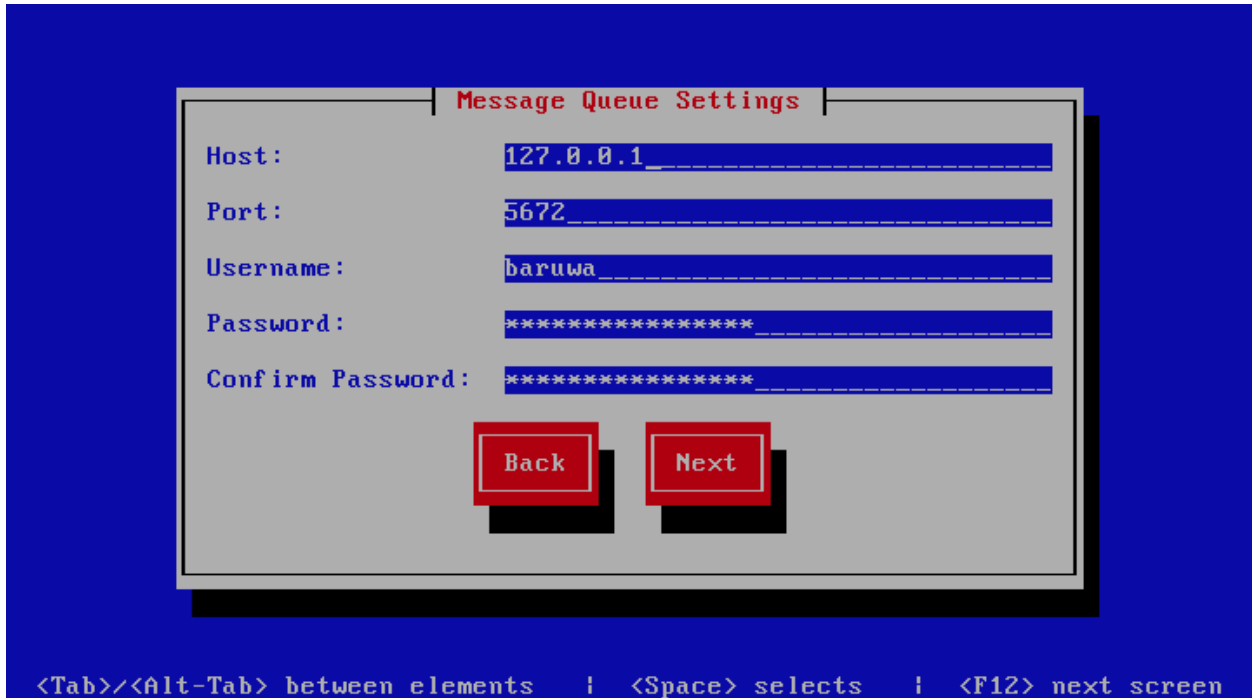
Option	Description
Search User	The search database username
Search User Password	The search database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Search User Password	Confirm the search database user password



### 6.2.10 Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

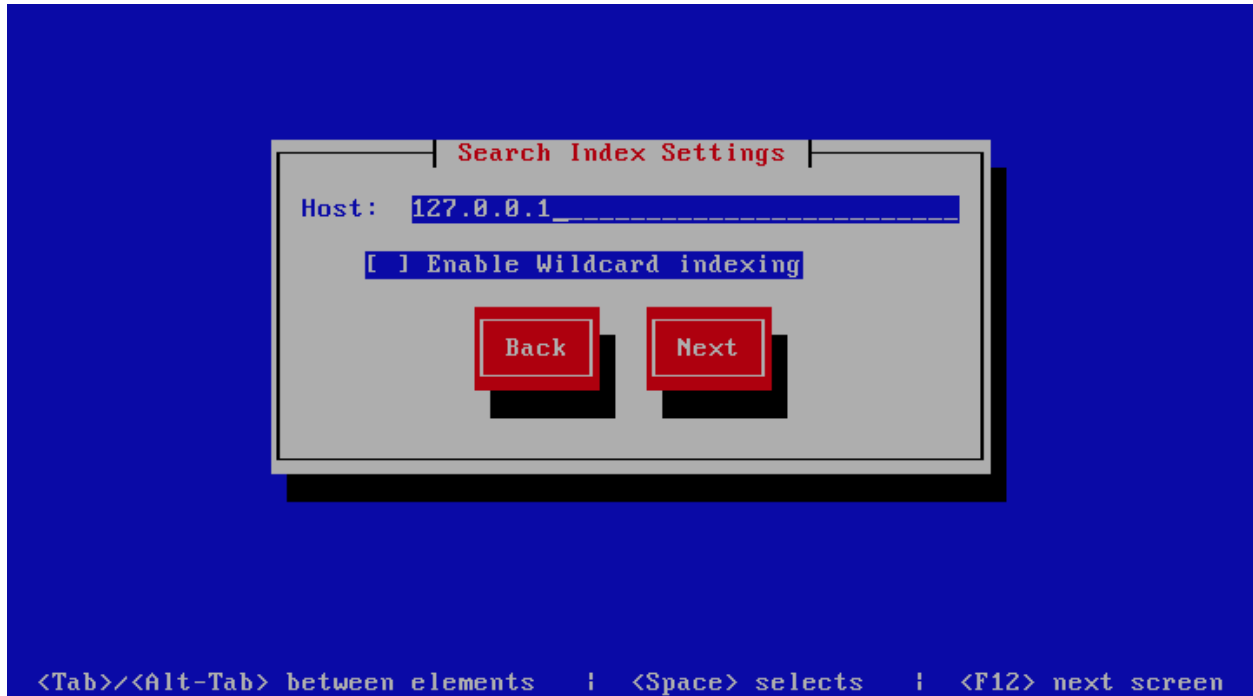
Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### 6.2.11 Search Index Settings

The screen sets search index settings, The description of the options is as follows:

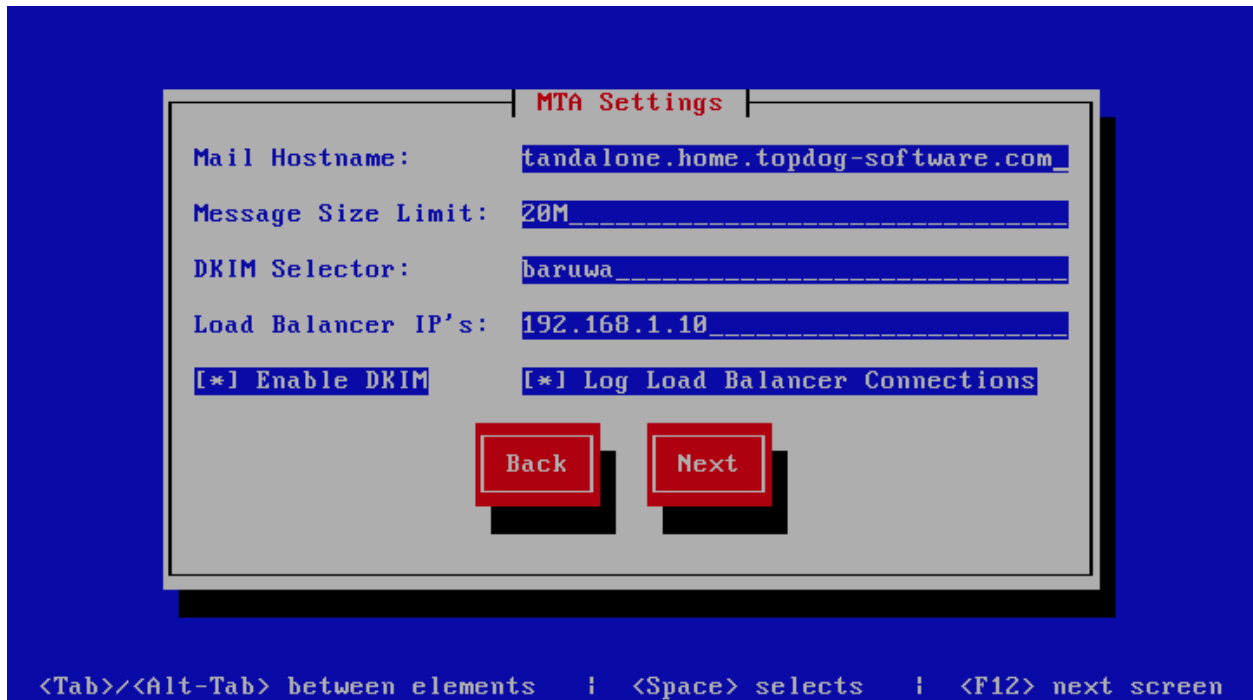
Option	Description
Host	Indexing server IP address
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



### 6.2.12 MTA Settings

The screen sets mta settings, The description of the options is as follows:

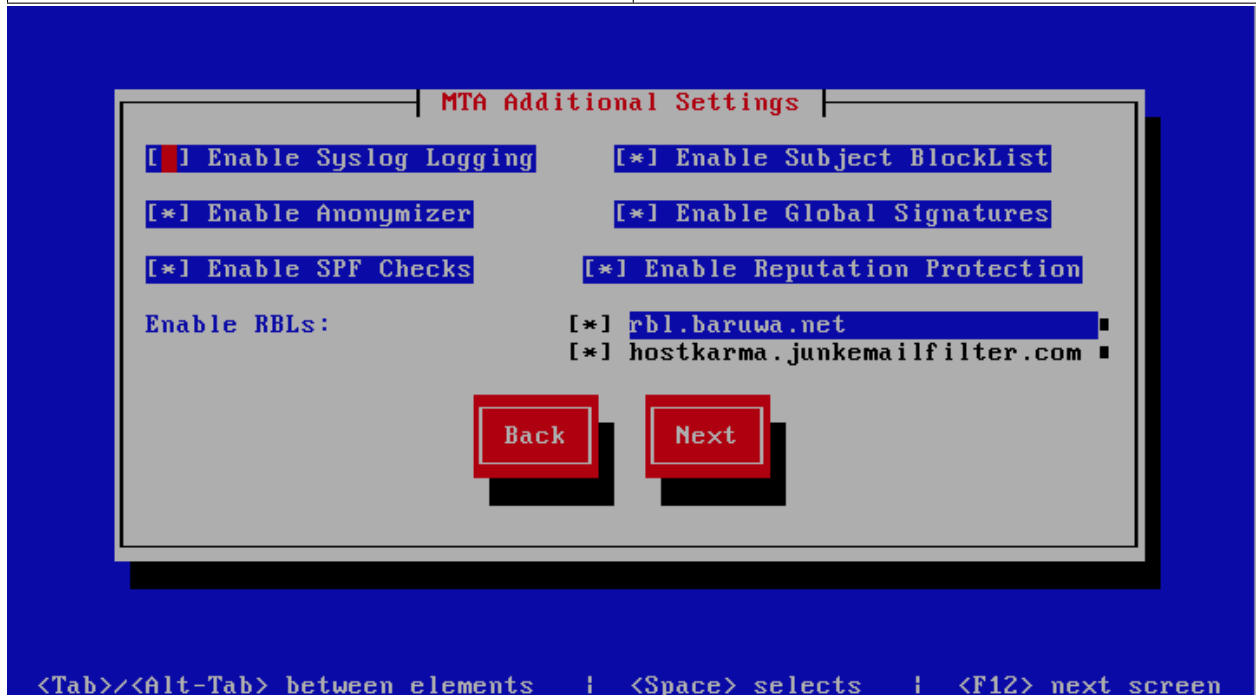
Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable DKIM	Enable DKIM functionality
Log Load Balancer Connections	Log Load Balancer connections to the MTA log



### 6.2.13 MTA Additional Settings

The screen sets MTA additional settings, The description of the options is as follows:

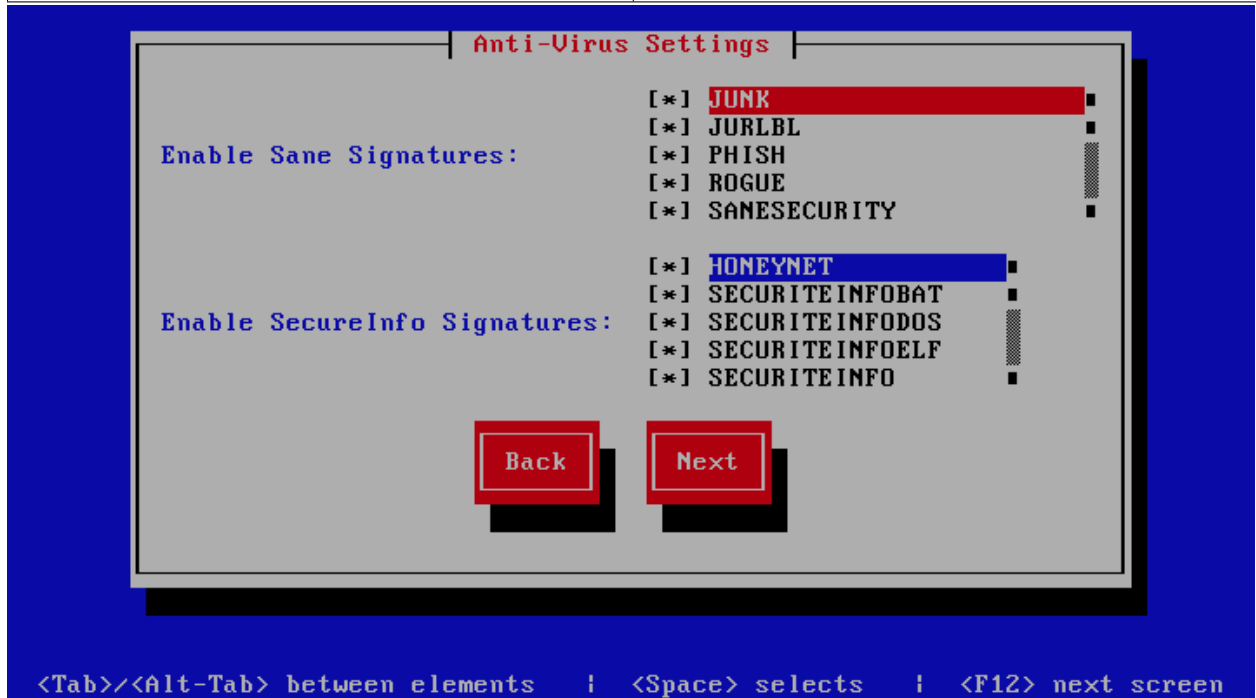
Option	Description
Enable Syslog Logging	Turns on MTA logging to syslog
Enable Subject Blocklist	Enable the blocking by subject functionality
Enable Anonymizer	Enable the Anonymizer functionality
Enable Global Signatures	Enable Global Signatures
Enable SPF Checks	Enable SPF checking functionality
Enable Reputation Protection	Enables functionality to block abusive outbound SMTP requests
Enable RBLs	Select the SMTP time DNSBL's to enable



## 6.2.14 Anti Virus Settings

The screen sets anti virus settings, The description of the options is as follows:

Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Enable SecureInfo Signatures	ClamAV Unofficial SecureInfo signatures to enable

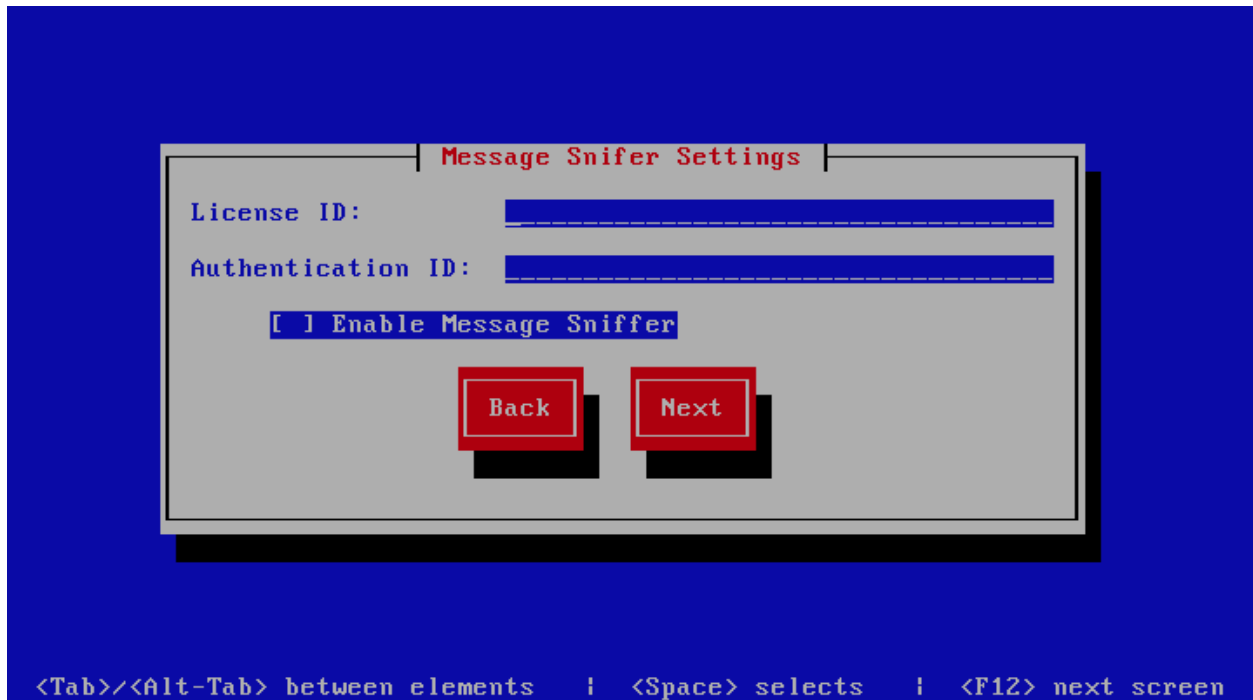


### 6.2.15 Message Sniffer Settings

The screen sets message sniffer settings, The description of the options is as follows:

Option	Description
License ID	Message Sniffer License ID This is emailed to you when you purchase a subscription
Authentication ID	Message Sniffer Authentication ID This is emailed to you when you purchase a subscription





### 6.2.16 SSL/TLS Settings

The Baruwa web interface MUST run over SSL/TLS, other services such as SMTP AUTH only work over SSL/TLS as well. So you need to either purchase a valid SSL certificate or have `baruwa-setup` automatically generate one non recognised SSL certificate for you. If you do not have a CA issued certificate and do not intend on purchasing one then leave the `I have a CA issued Certificate` unchecked.

The certificate that `baruwa-setup` generates will cover the web hostname, web aliases, cluster members and the mail hostname. This means that you should copy this certificate to other cluster hosts that you specified and select `I have a CA issued Certificate` on those hosts when you set them up instead of generating new certificates for them.

**Note:** We have partnered with the SSLShop to bring you discounted SSL certificate pricing. RapidSSL CA signed certificates can be purchased at discounted pricing using the Discount coupon “BARUWA” from <http://www.sslshop.co.za>

If you have a SSL certificate that is issued by a recognised CA and would like Baruwa to use it, install it prior to running `baruwa-setup`. Please NOTE that you need certificates that cover the web hostname and aliases, and the mail hostname. Please check `I have a CA issued Certificate`.

The preferred location to install certificates and keys on the server is under `/etc/pki`. You need to create a directory structure under that and store your certificate under it.

The following example creates a baruwa directory under `/etc/pki` and stores the certificates and keys there:

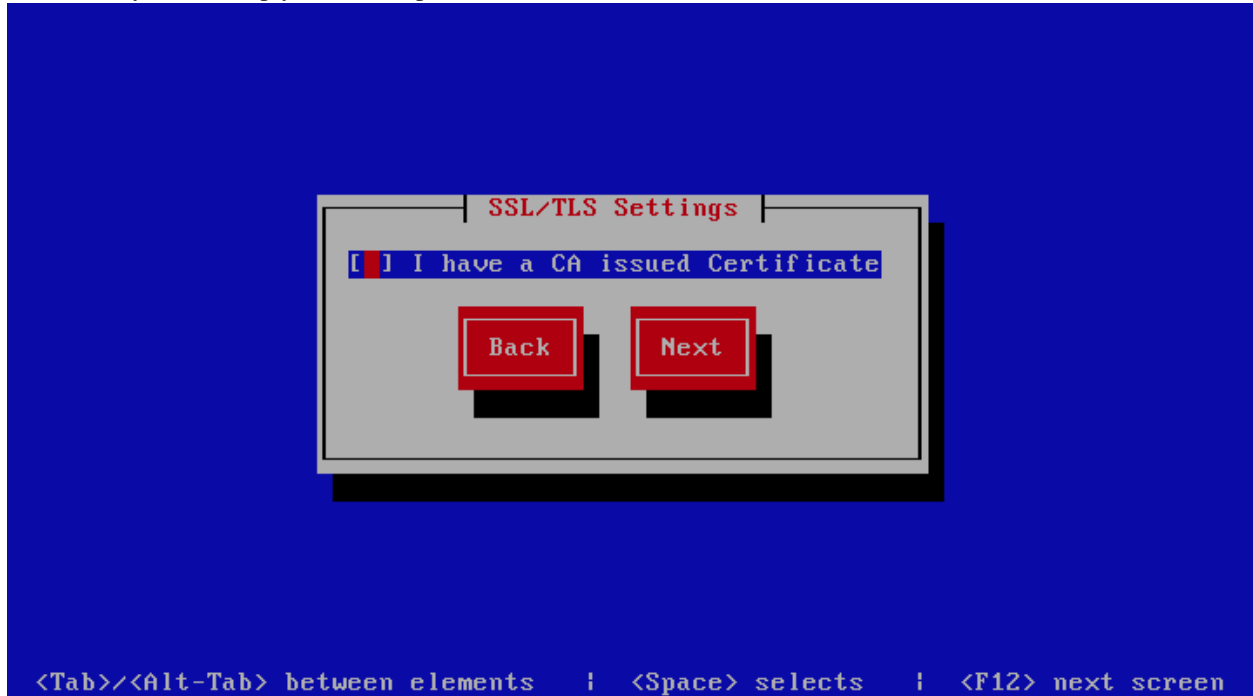
```
mkdir -p /etc/pki/baruwa/{certs,private}
```

Create the following files

- `/etc/pki/baruwa/certs/baruwa.pem` with the contents of your SSL certificate
- `/etc/pki/baruwa/private/baruwa.key` with the contents of your SSL private key

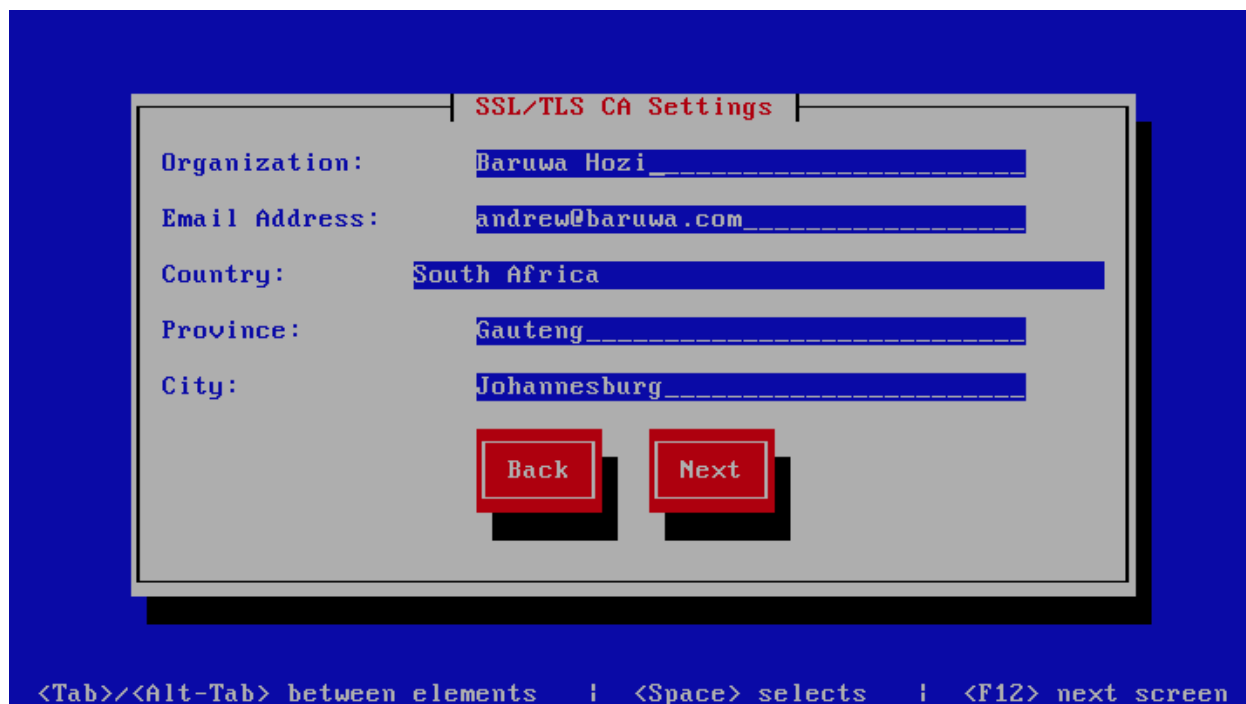
You need to create additional certificate pairs if your web hostname and mail hostname are not the same.

If you have a wildcard certificate with all your names being subdomains of that domain to which the certificate is issued then you can simply create one pair.



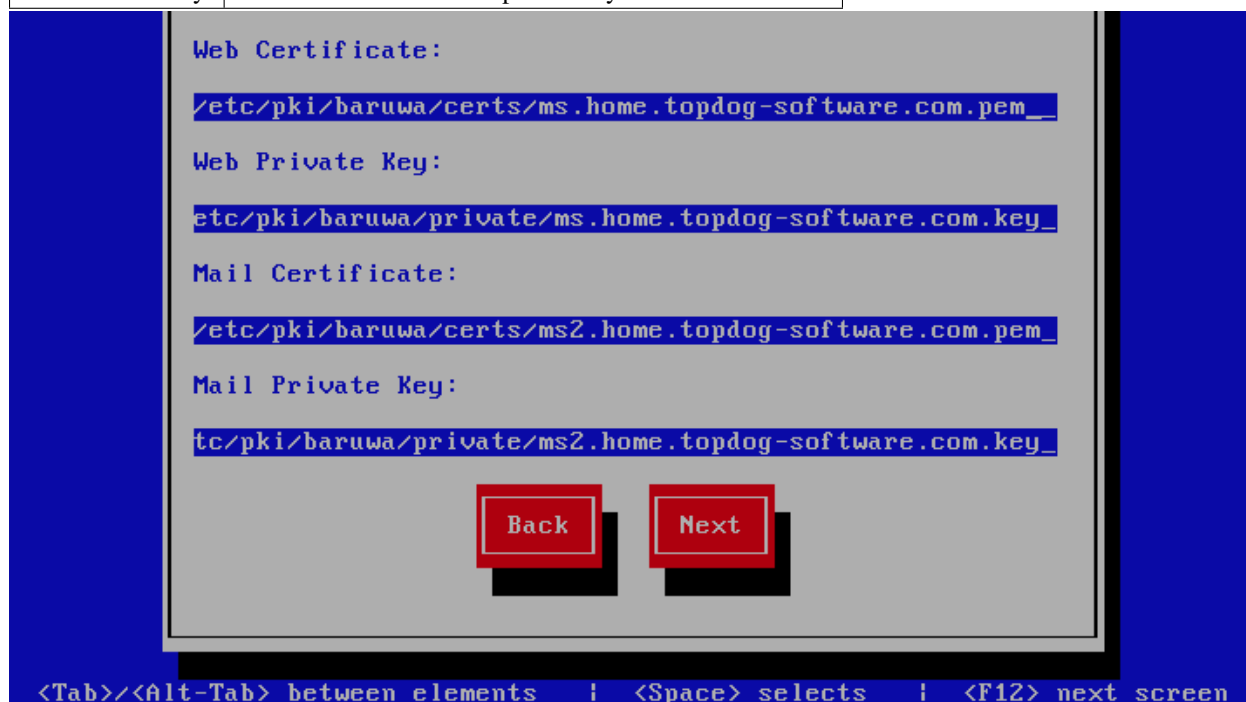
If you left I have a CA issued Certificate unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

Option	Description
Organization	OpenSSL CA Name
Email Address	OpenSSL email address
Country	OpenSSL country code
Province	OpenSSL province
City	OpenSSL city



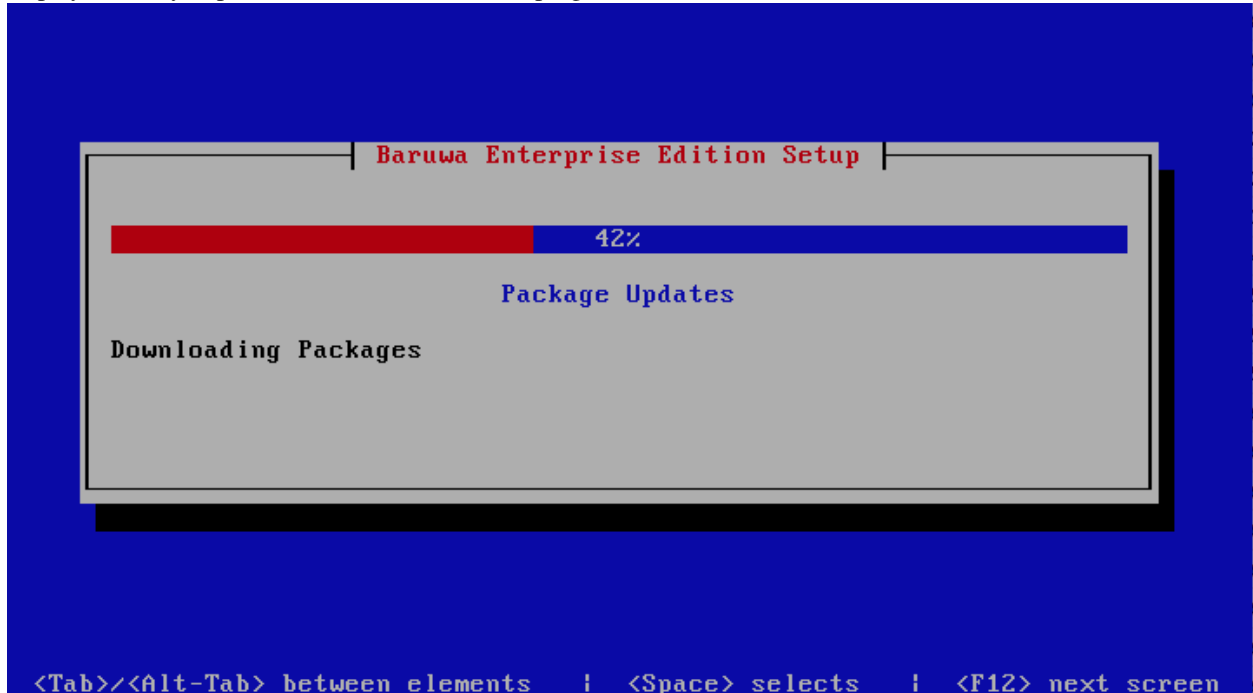
If you checked I have a CA issued Certificate you will be presented with the following screen, you need to specify the locations of your certificates and keys. The description of the options is as follows:

Option	Description
Web Certificate	The location of the web certificate file in PEM format
Web Private Key	The location of the web private key file in PEM format
Mail Certificate	The location of the mail certificate file in PEM format
Mail Private Key	The location of the mail private key file in PEM format



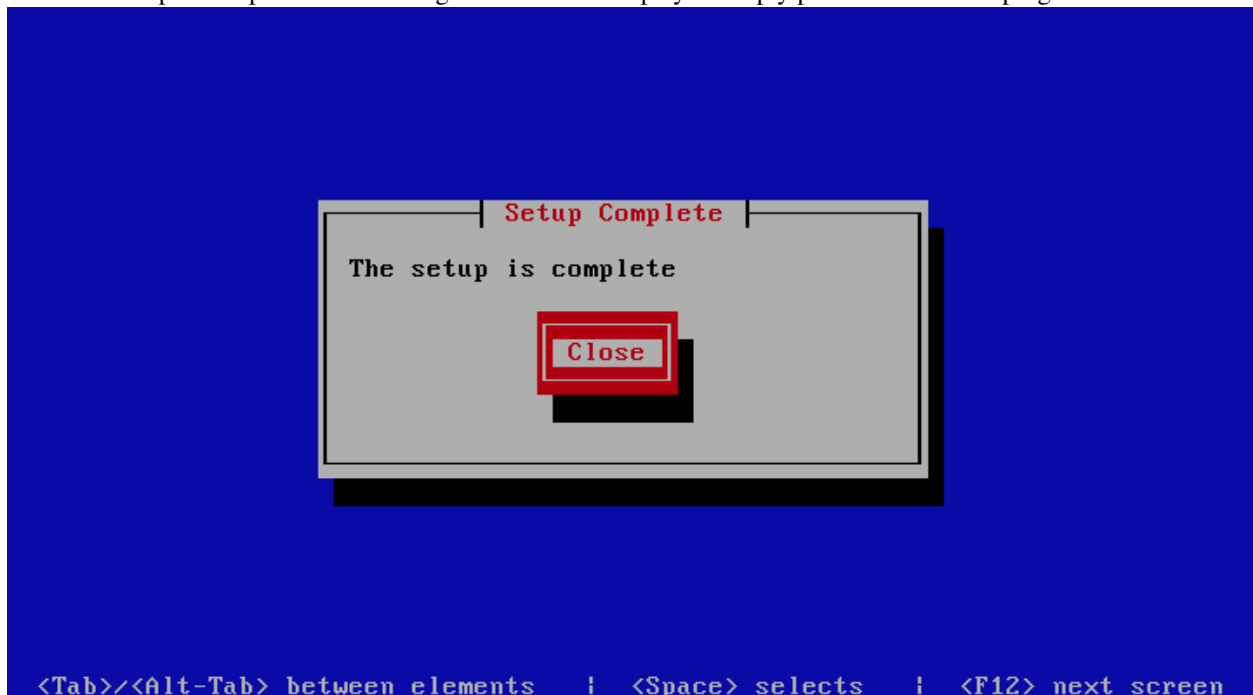
## 6.2.17 Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## 6.2.18 Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 6.3 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a scanning Node*, *Add an Organization*, *Adding a Domain* and *Adding an Account*. This is done through the management web interface.

The exact sequence to follow is:

- Add the Node
- Add an Organization
- Add a Domain Administrator for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add a Domain to the Organization
- Add a delivery server for the Domain
- Add any user accounts to the Domain if not using external authentication

Review the *Administrators guide* and *Advanced configuration* for other configuration and setup options available.



## CLUSTER CONFIGURATION

In a cluster configuration each system has to be configured based on its system type. The available system types are described in *System Profiles*. Please refer to *Clustering* for a more in depth description.

The types are documented below.

### 7.1 Backend System

This setup installs all the backend components on to one server, the backend components that are installed are:

- Database Server
- Message Queue Server
- Search Index Server
- Cache Server

This setup can be used with a clustered setup of several nodes. You have to setup one server as a backend system in a basic cluster setup.

#### 7.1.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

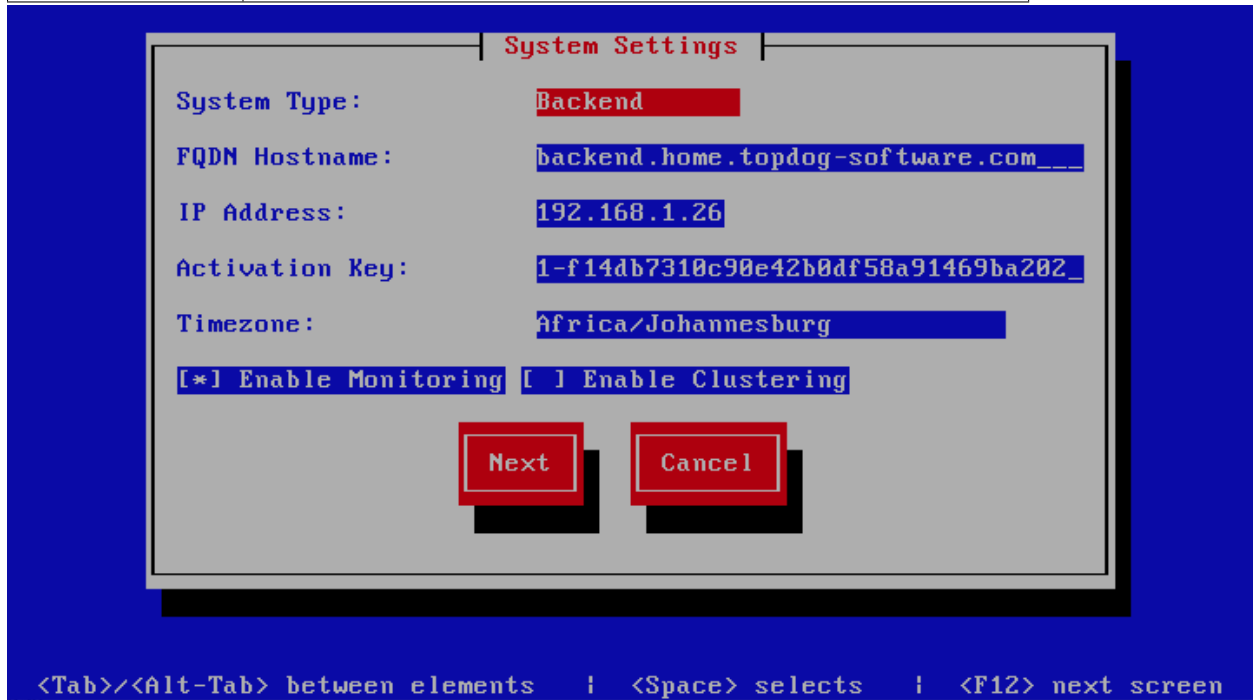
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

## System Settings

This screen configures the basic system settings. The description of the options is as follows:

Option	Description
System Type	Set this to Backend
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service

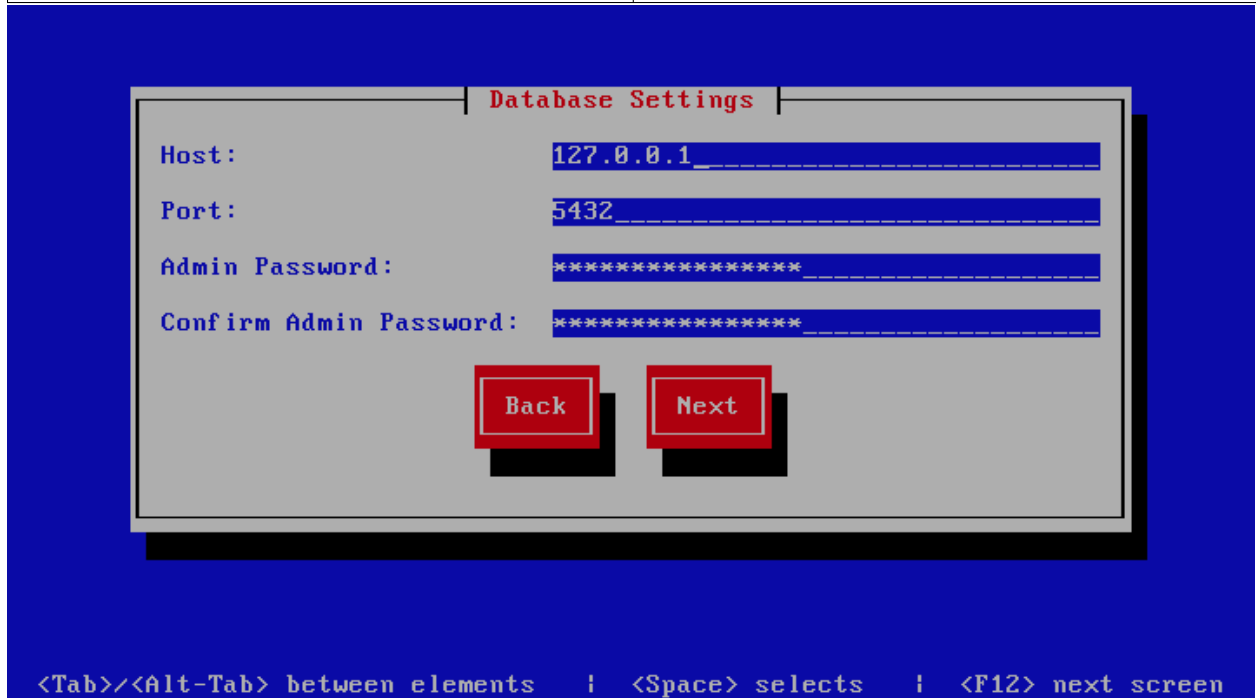


## Database Settings

The screen sets database settings, The description of the options is as follows:



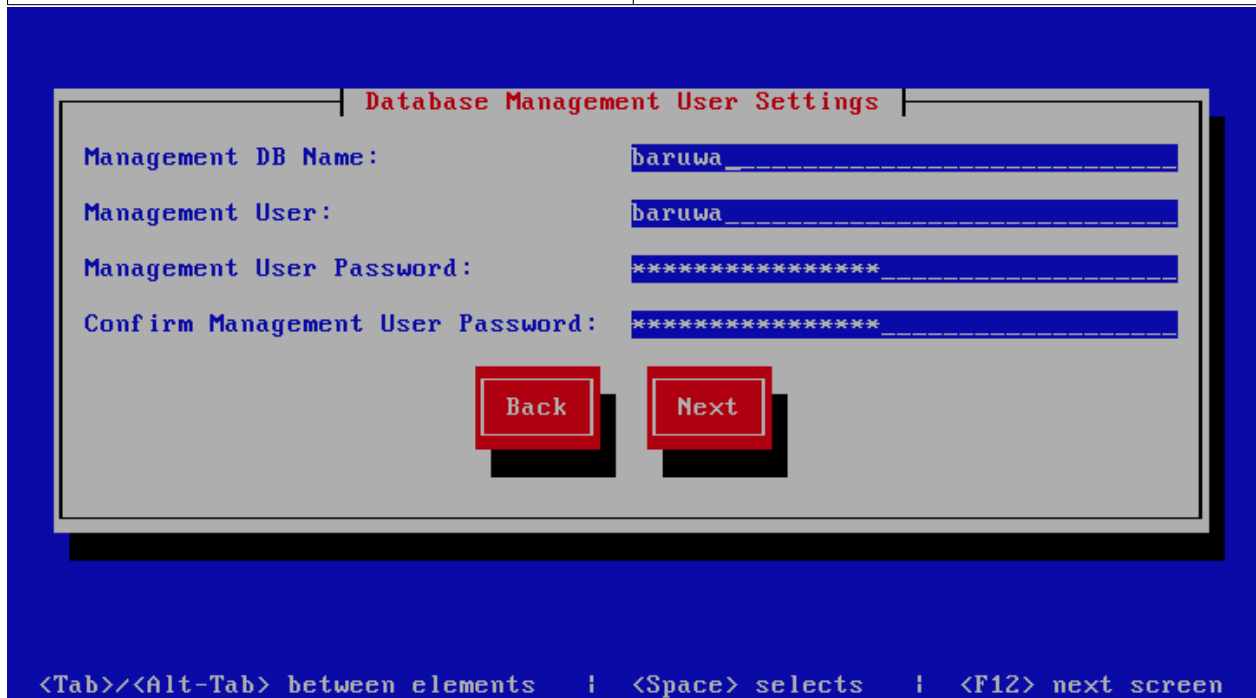
Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password



### Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:

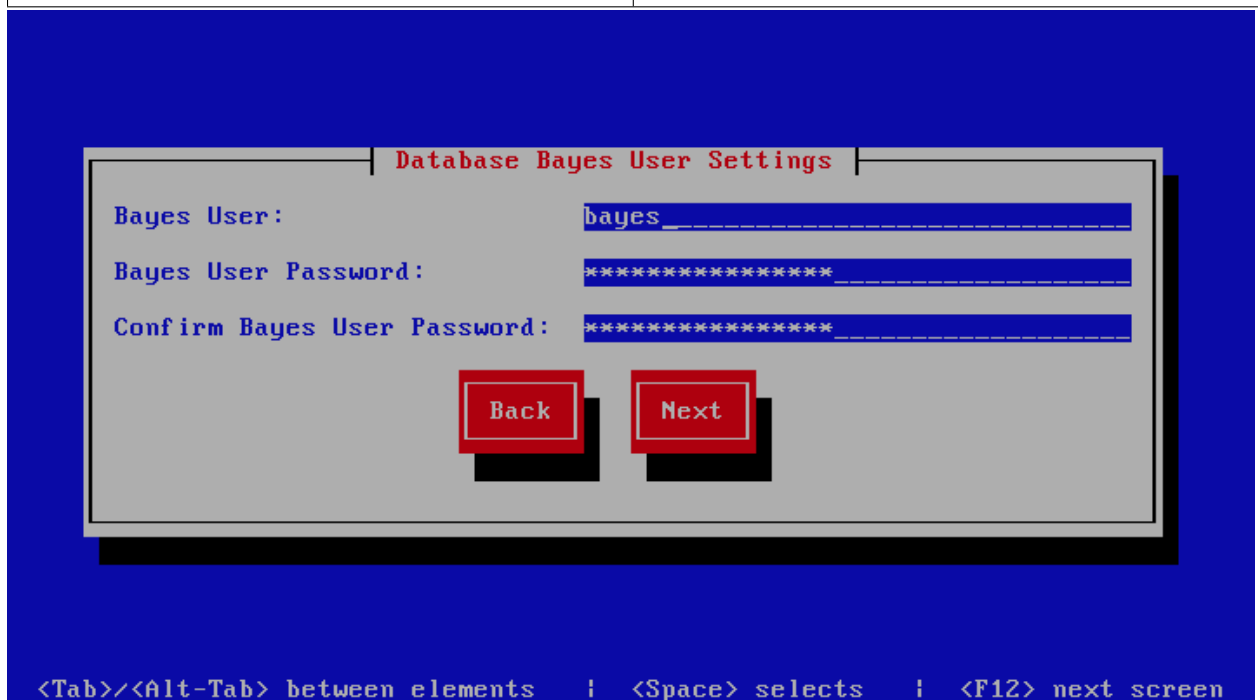
Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password



### Database Bayes User Settings

The screen sets database bayes user settings, The description of the options is as follows:

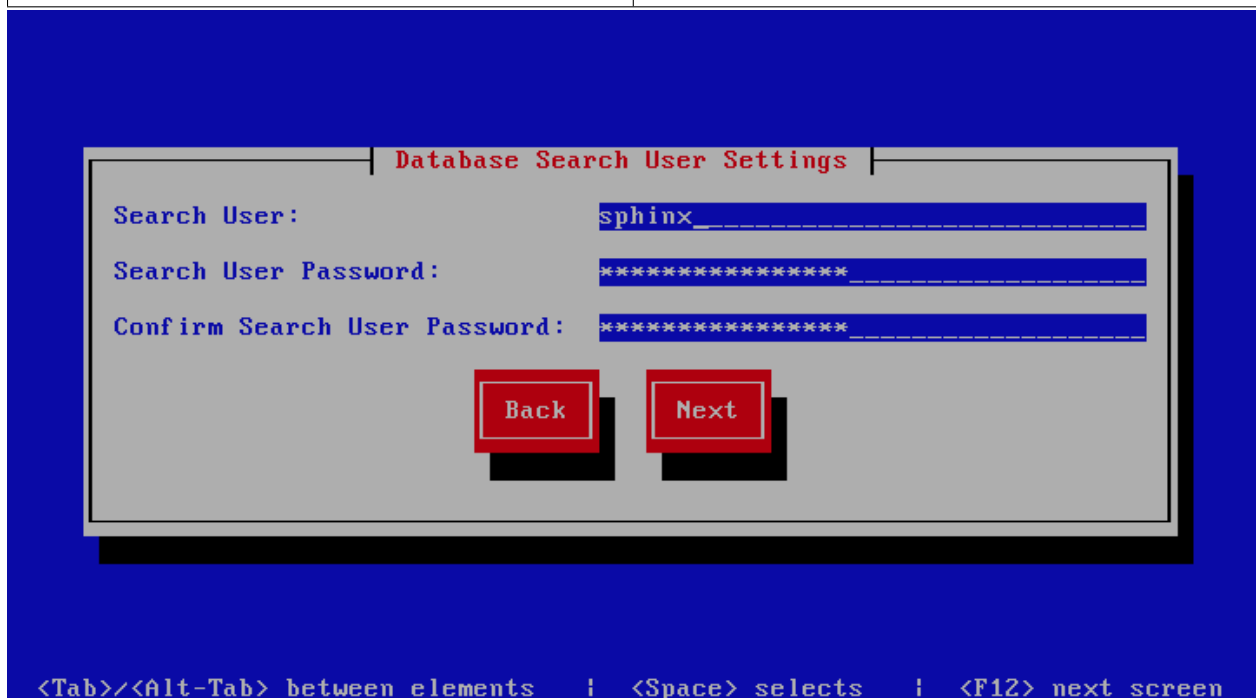
Option	Description
Bayes User	The bayes database username
Bayes User Password	The bayes database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Bayes User Password	Confirm the bayes database user password



### Database Search User Settings

The screen sets database search user settings, The description of the options is as follows:

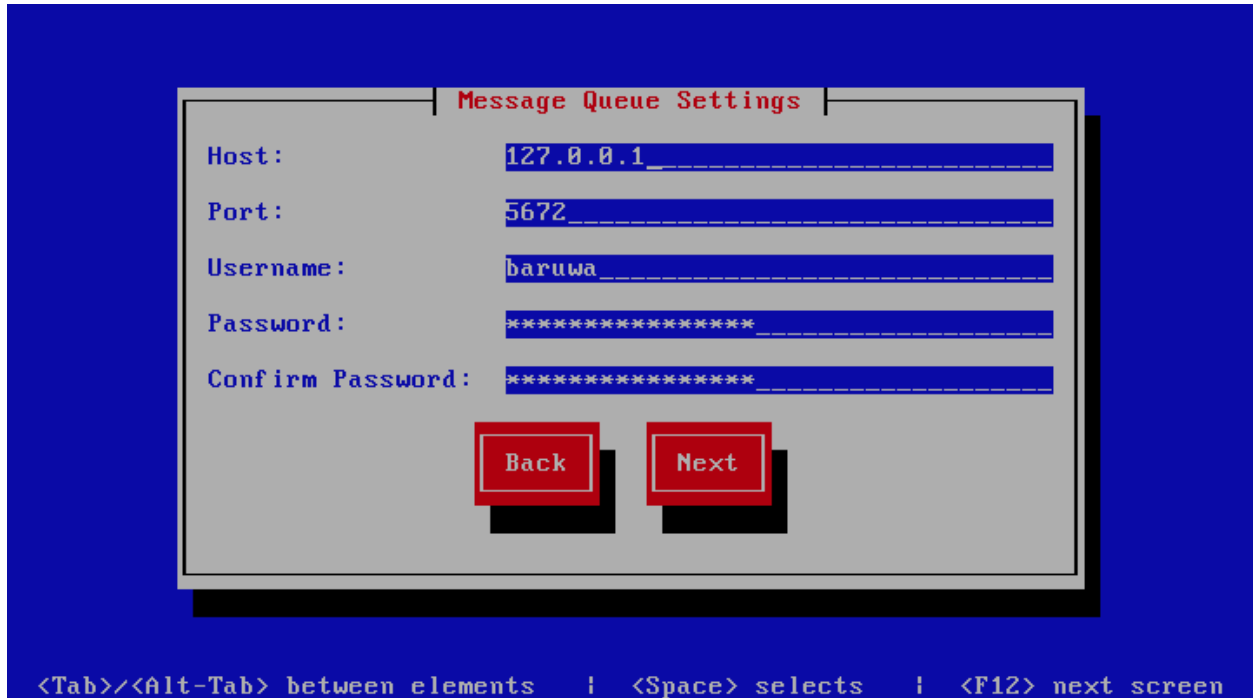
Option	Description
Search User	The search database username
Search User Password	The search database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Search User Password	Confirm the search database user password



### Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

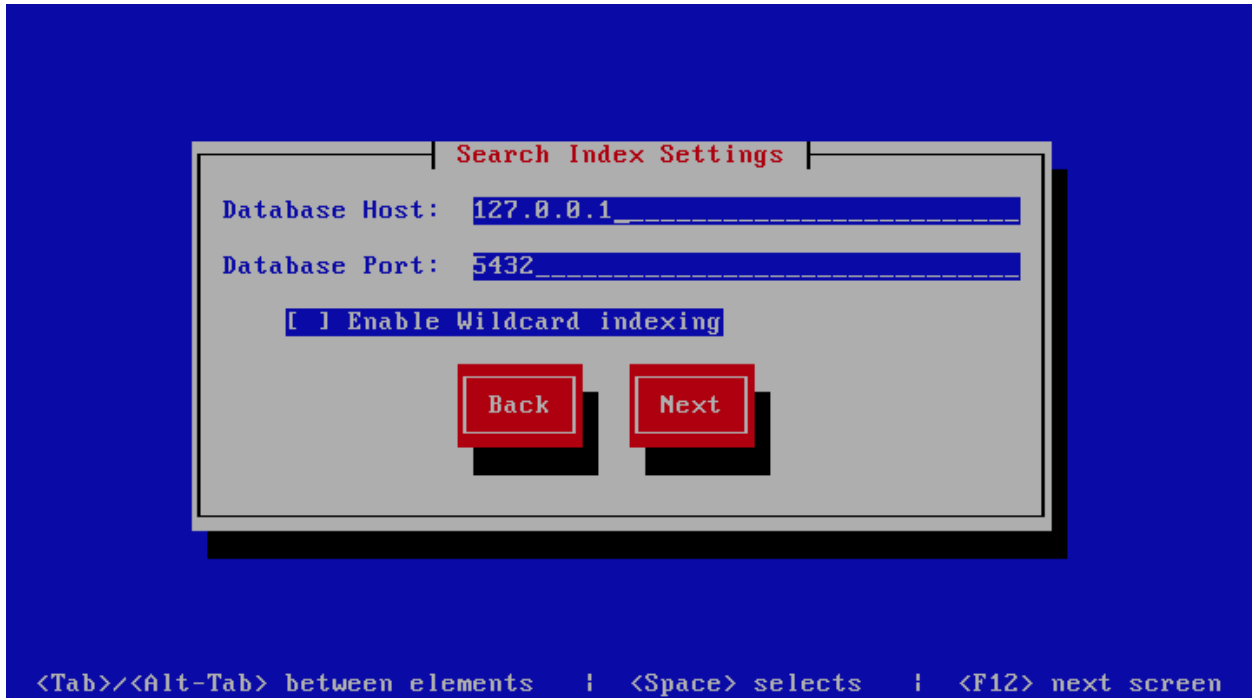
Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### Search Index Settings

The screen sets search index settings, The description of the options is as follows:

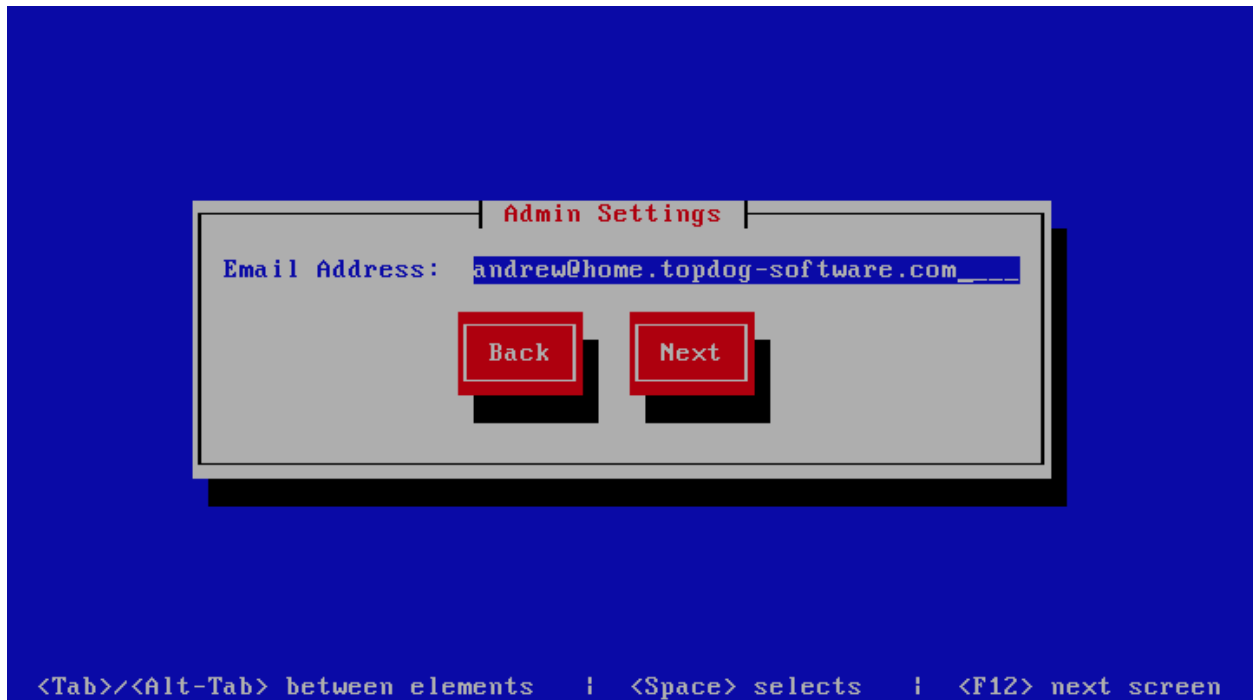
Option	Description
Database Host	Database server IP address
Database Port	Database server Port - leave as default
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



### Admin Settings

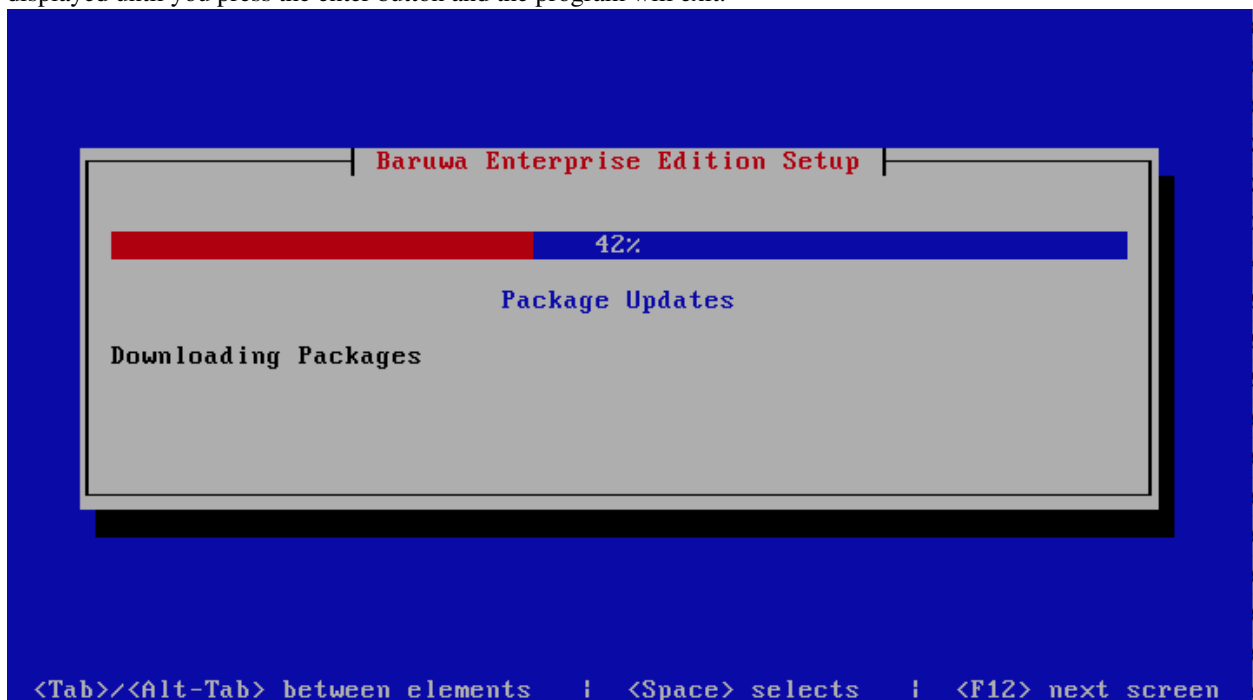
The screen sets admin settings, The description of the options is as follows:

Option	Description
Email Address	This email address will receive system notifications from the host, it is aliased to the root account



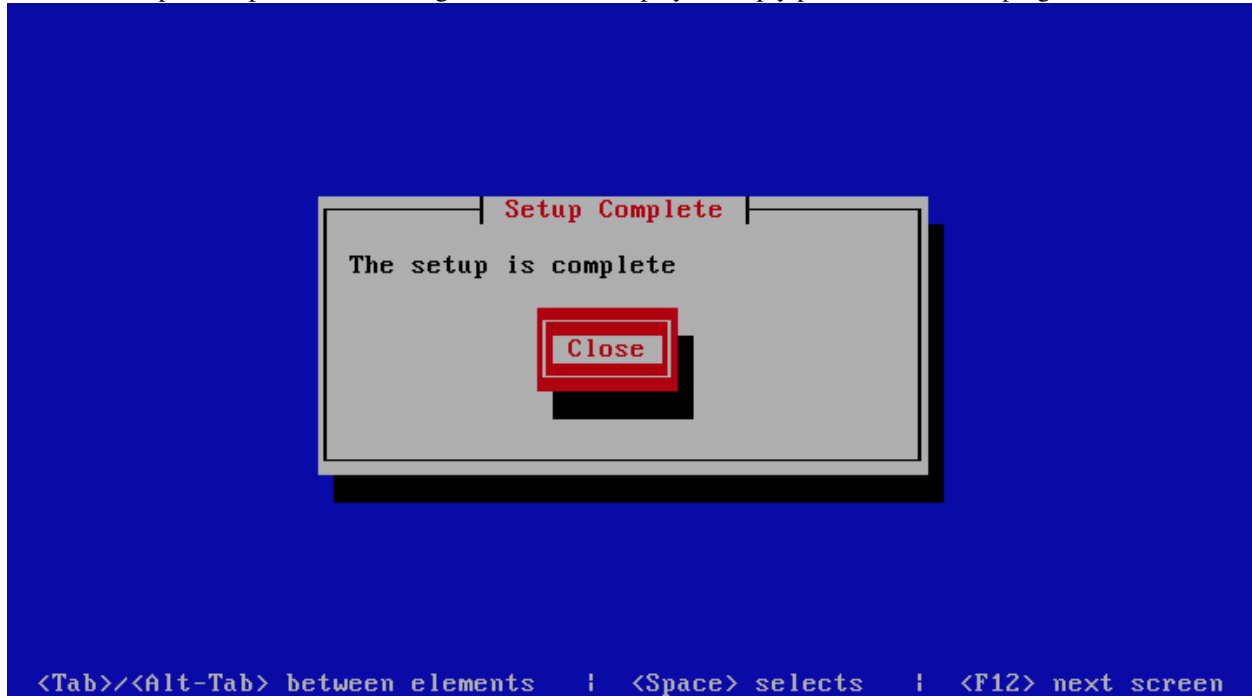
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.2 Database System

This is a backend server in a distributed system, it provides the backend database functionality. You setup this profile if you want a dedicated server providing database functionality.

### 7.2.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

```
# baruwa-setup
```

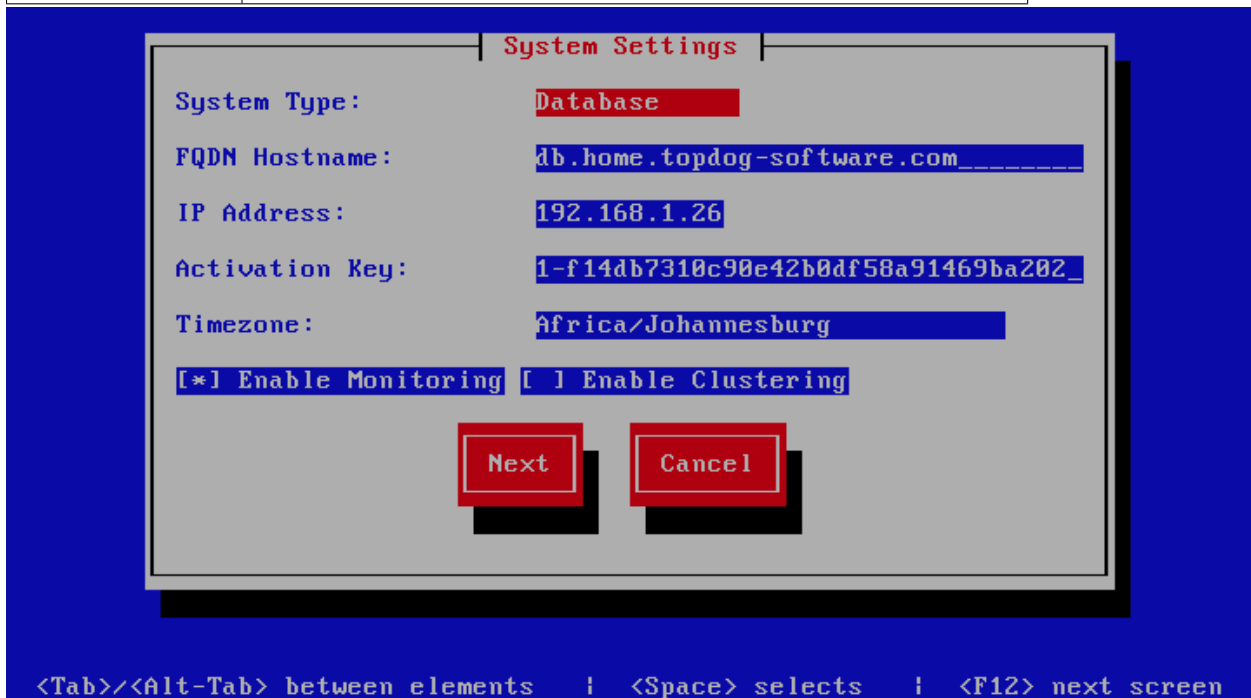


The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

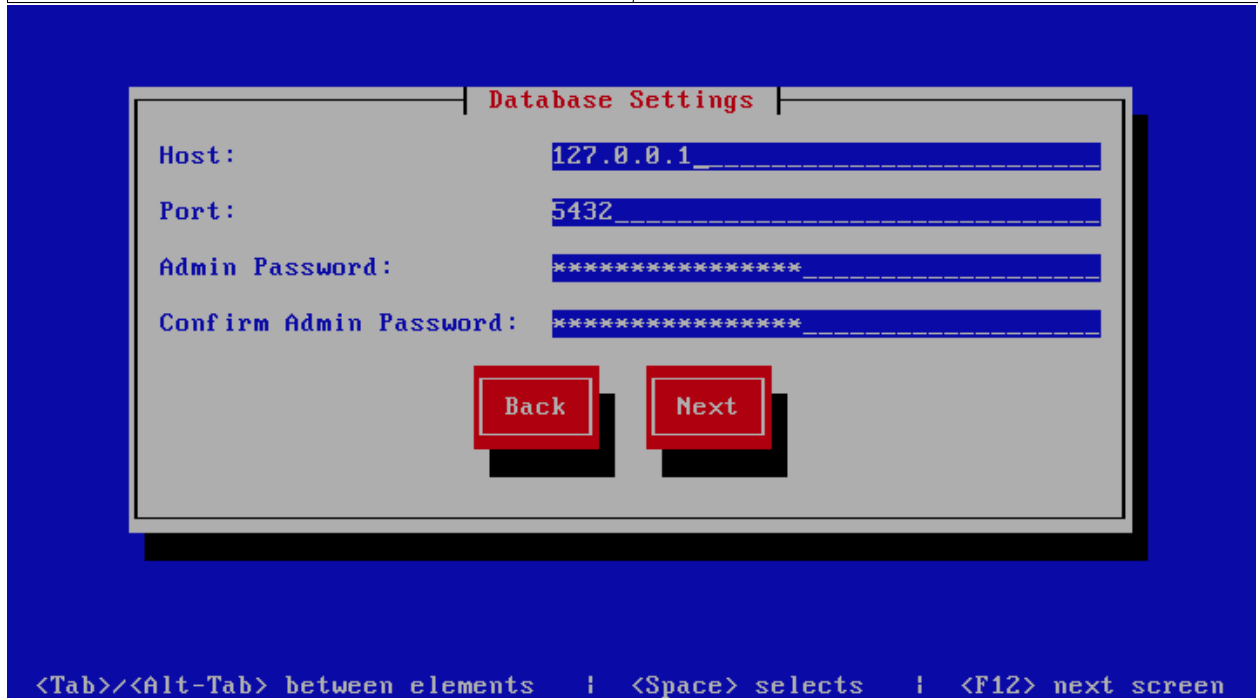
Option	Description
System Type	Set this to Database
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service



### Database Settings

The screen sets database settings, The description of the options is as follows:

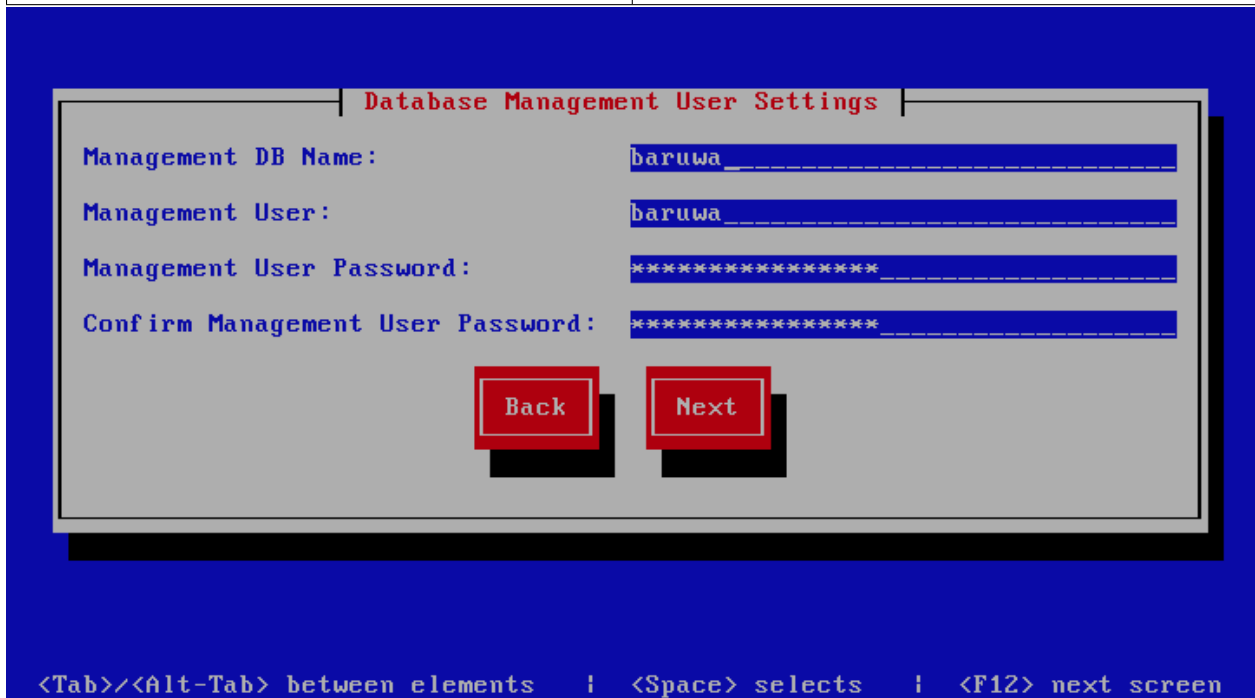
Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password



### Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:

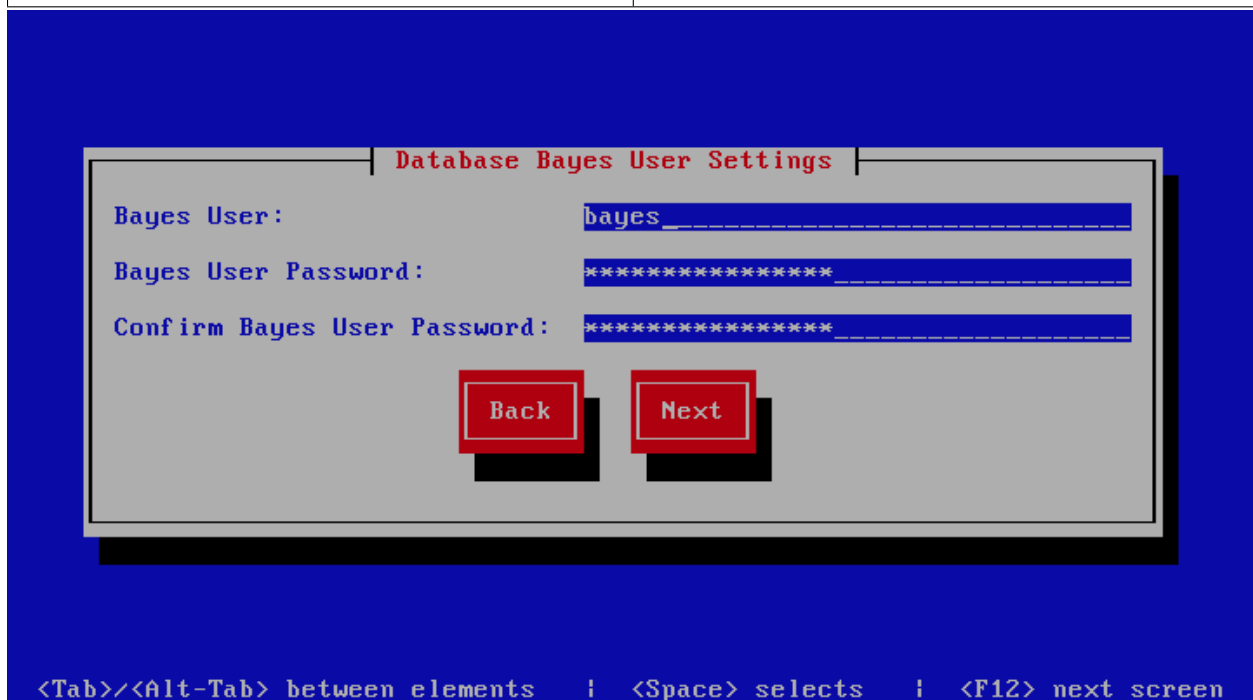
Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password



### Database Bayes User Settings

The screen sets database bayes user settings, The description of the options is as follows:

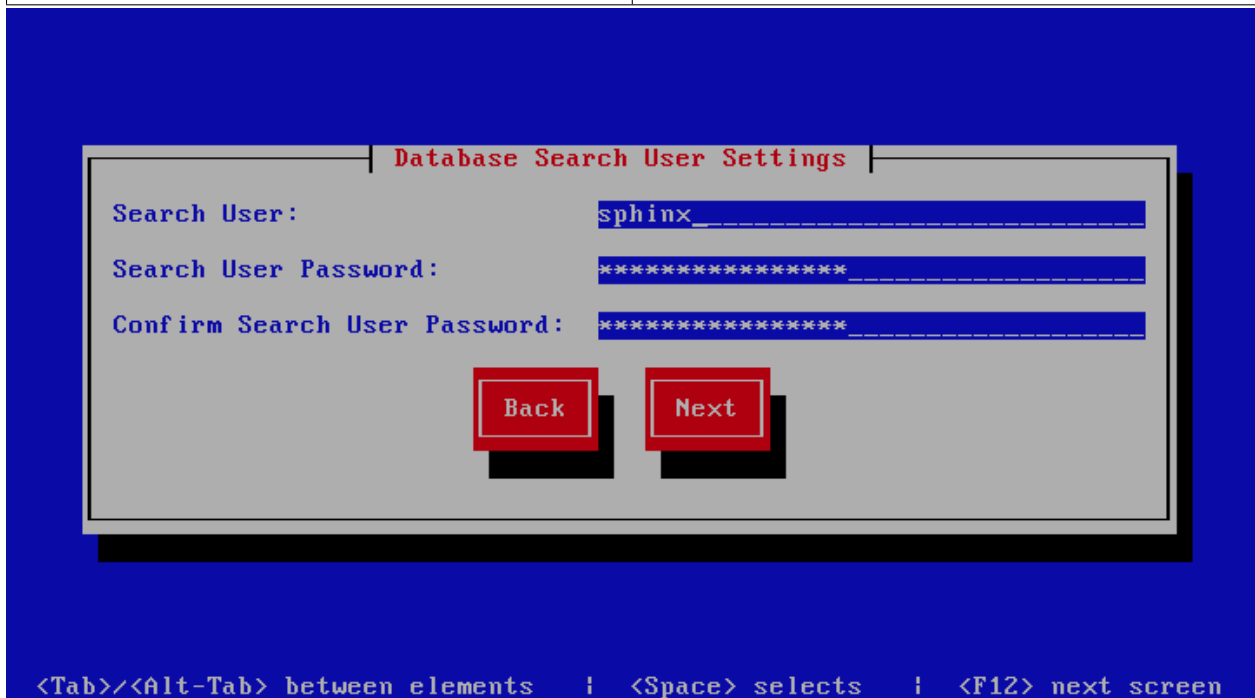
Option	Description
Bayes User	The bayes database username
Bayes User Password	The bayes database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Bayes User Password	Confirm the bayes database user password



### Database Search User Settings

The screen sets database search user settings, The description of the options is as follows:

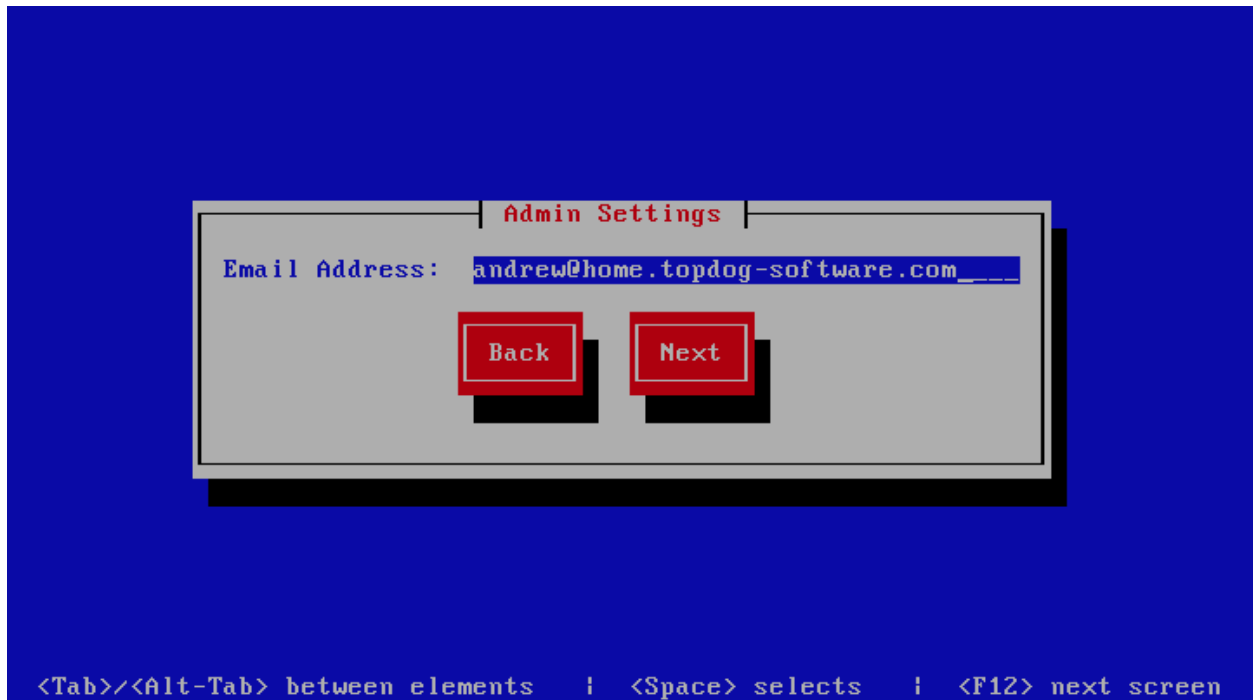
Option	Description
Search User	The search database username
Search User Password	The search database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Search User Password	Confirm the search database user password



### Admin Settings

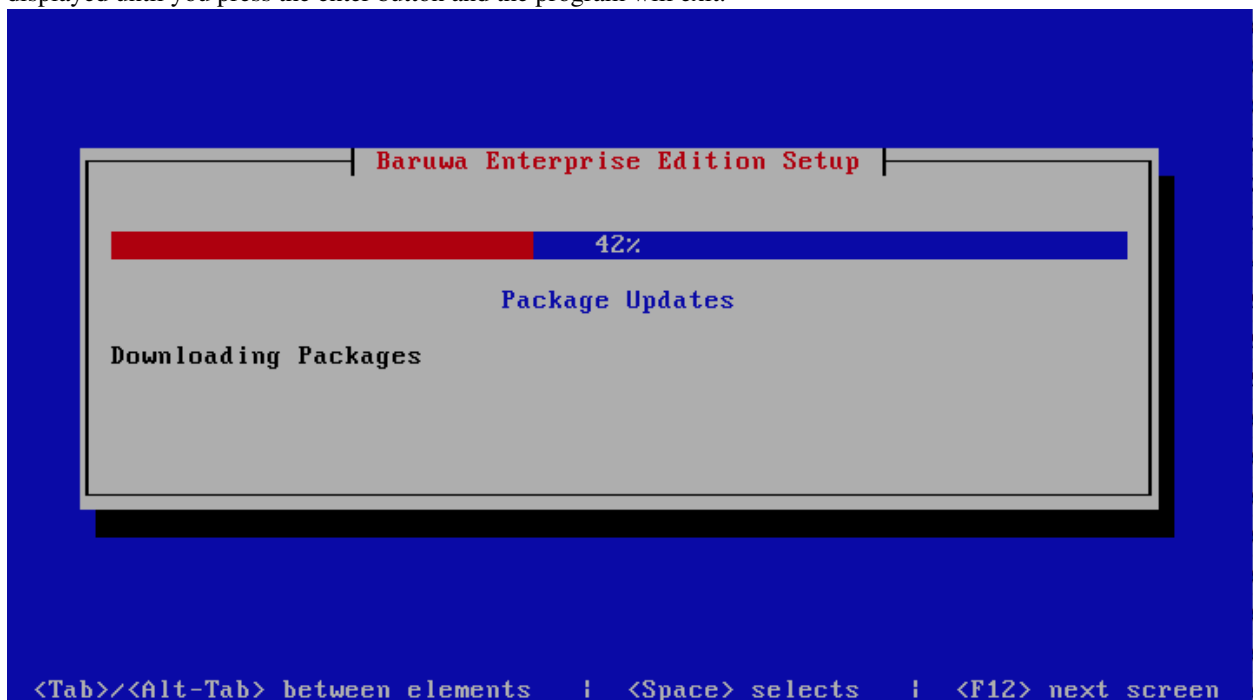
The screen sets admin settings, The description of the options is as follows:

Option	Description
Email Address	This email address will receive system notifications from the host, it is aliased to the root account



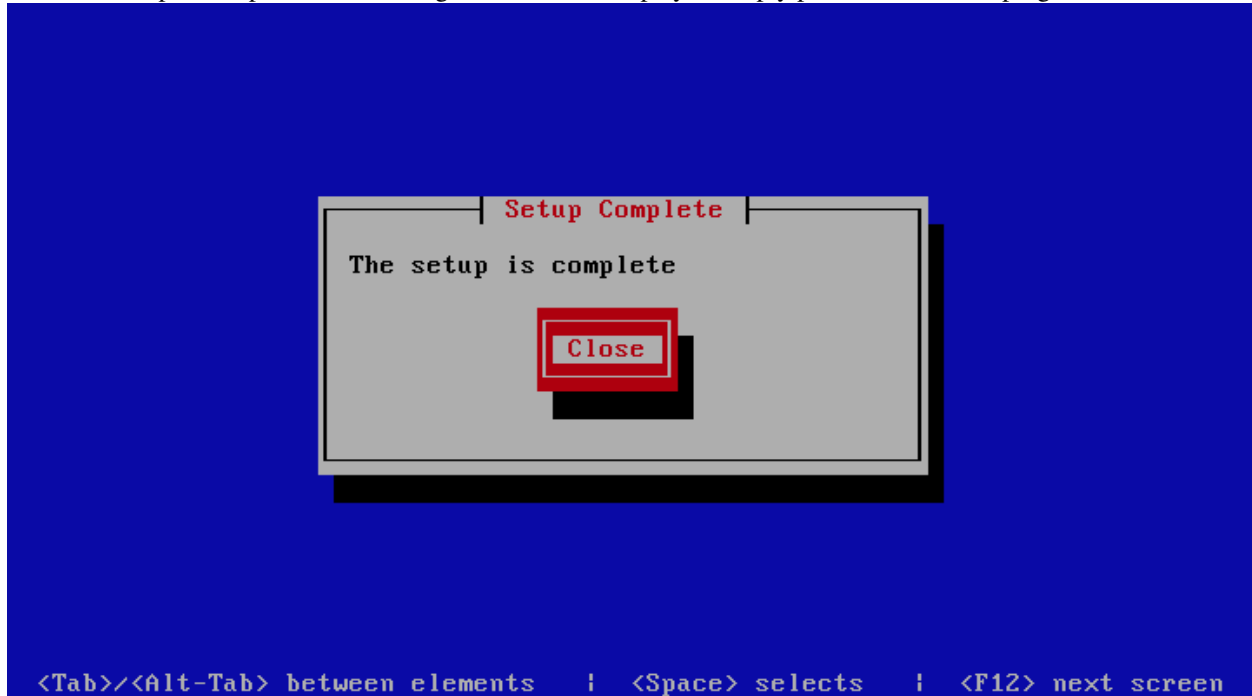
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.3 Search Index System

This is a backend server in a distributed system, it provides the backend indexing functionality. You setup this profile if you want a dedicated server providing search indexing.

### 7.3.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

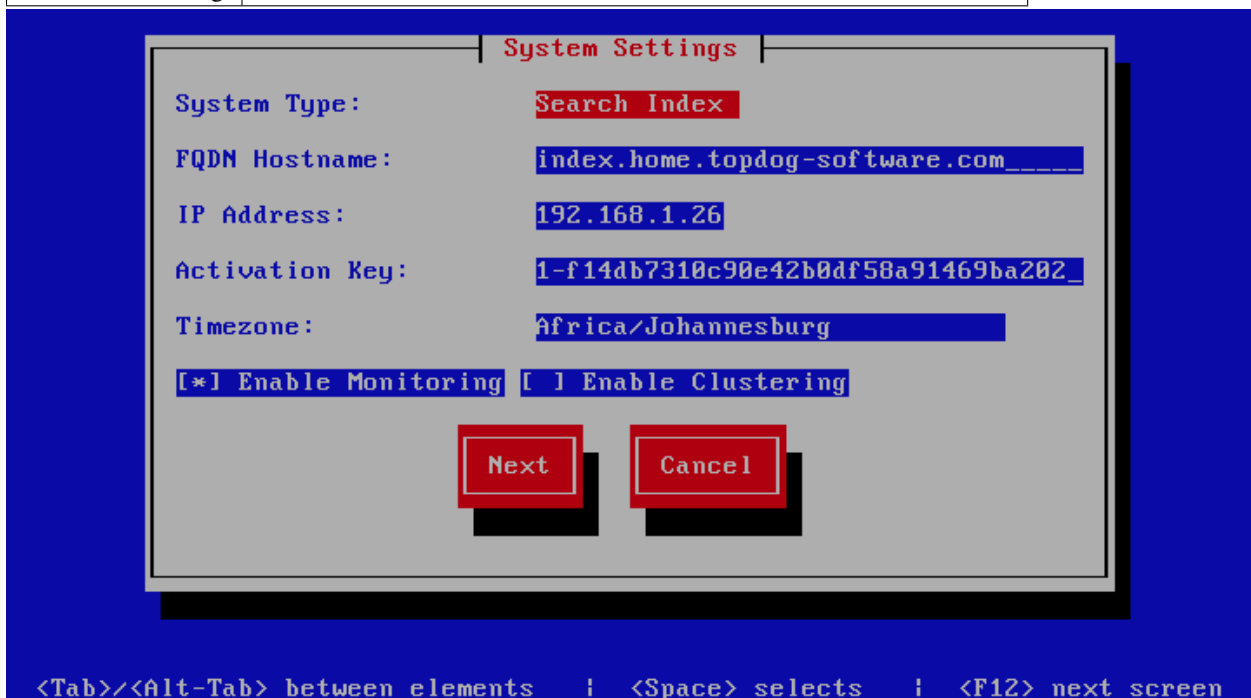
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

Option	Description
System Type	Set this to Search Index
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service

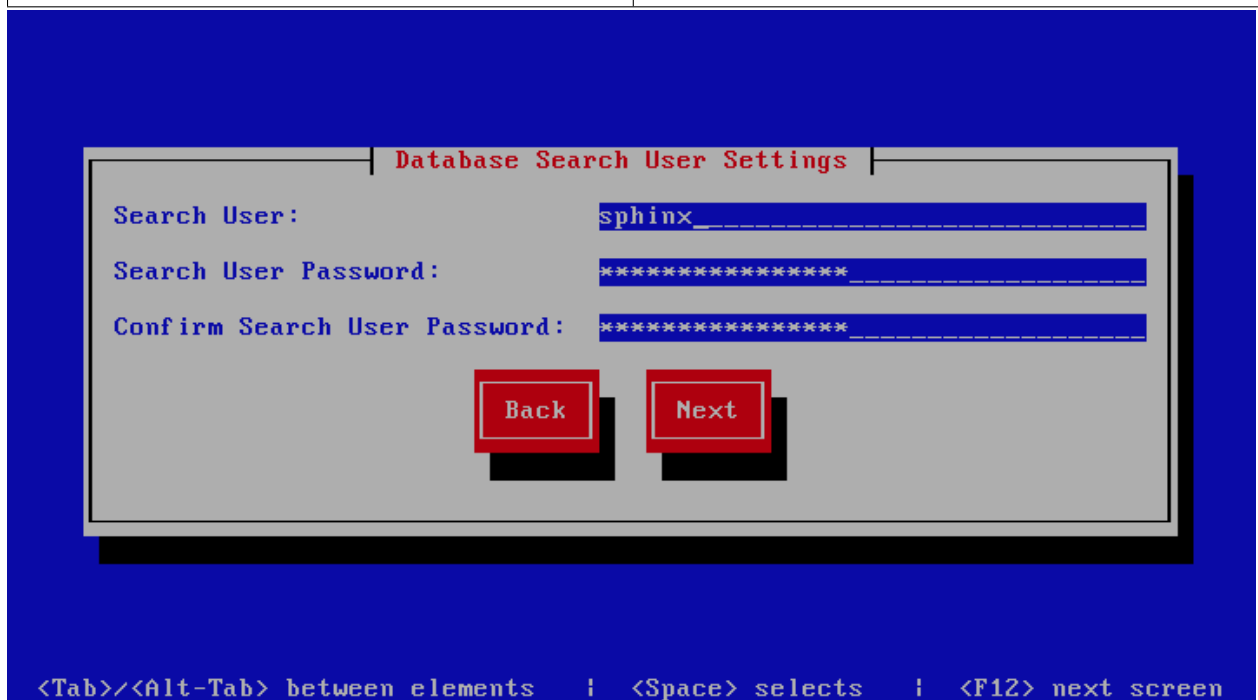


### Database Search User Settings

The screen sets database search user settings, The description of the options is as follows:



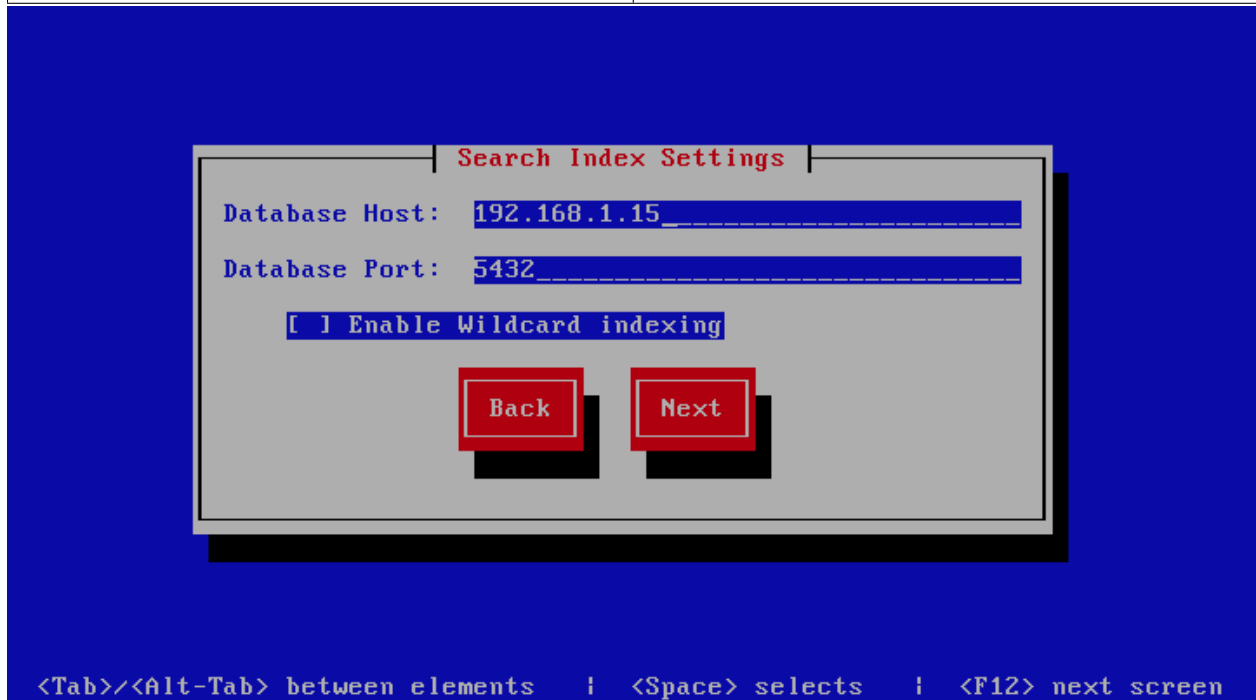
Option	Description
Search User	The search database username
Search User Password	The search database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Search User Password	Confirm the search database user password



### Search Index Settings

The screen sets search index settings, The description of the options is as follows:

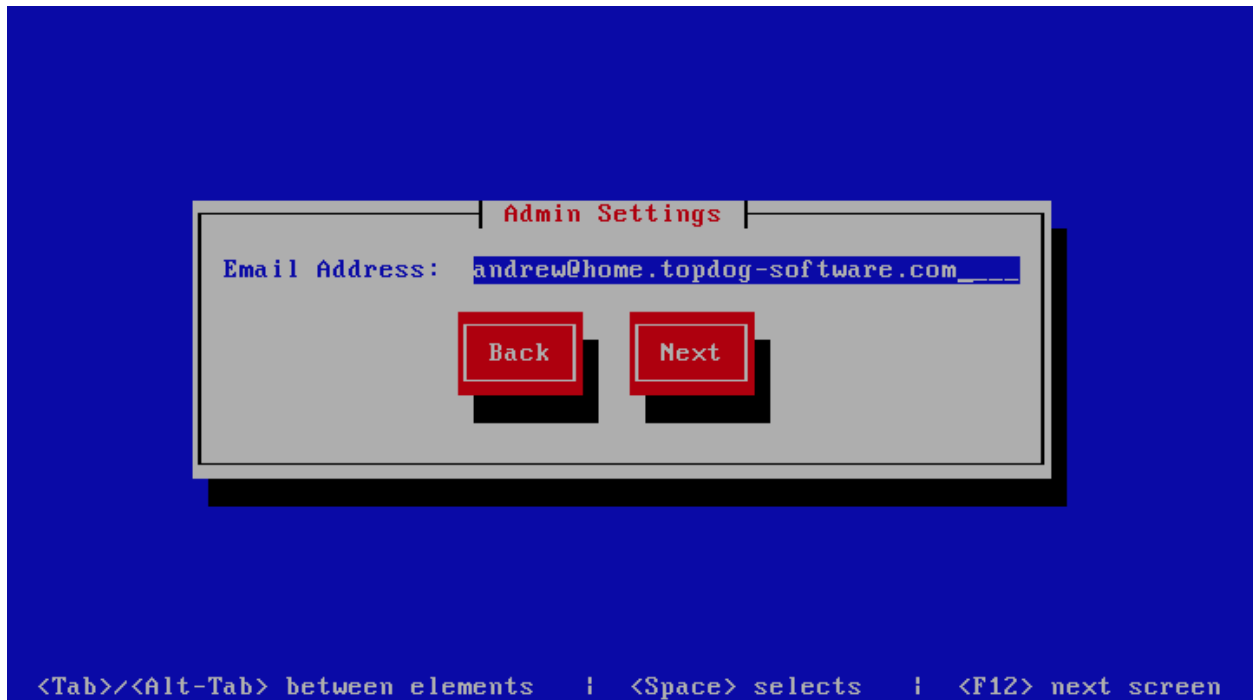
Option	Description
Database Host	Database server IP address
Database Port	Database server Port - leave as default
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



### Admin Settings

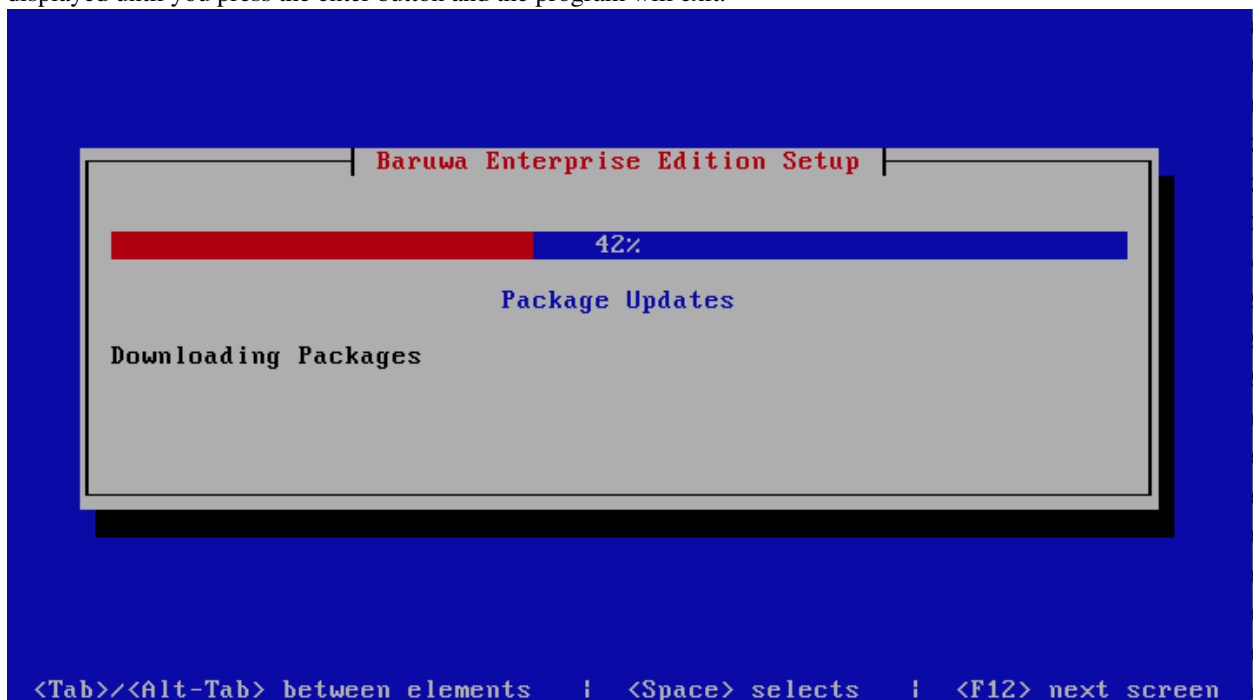
The screen sets admin settings, The description of the options is as follows:

Option	Description
Email Address	This email address will receive system notifications from the host, it is aliased to the root account



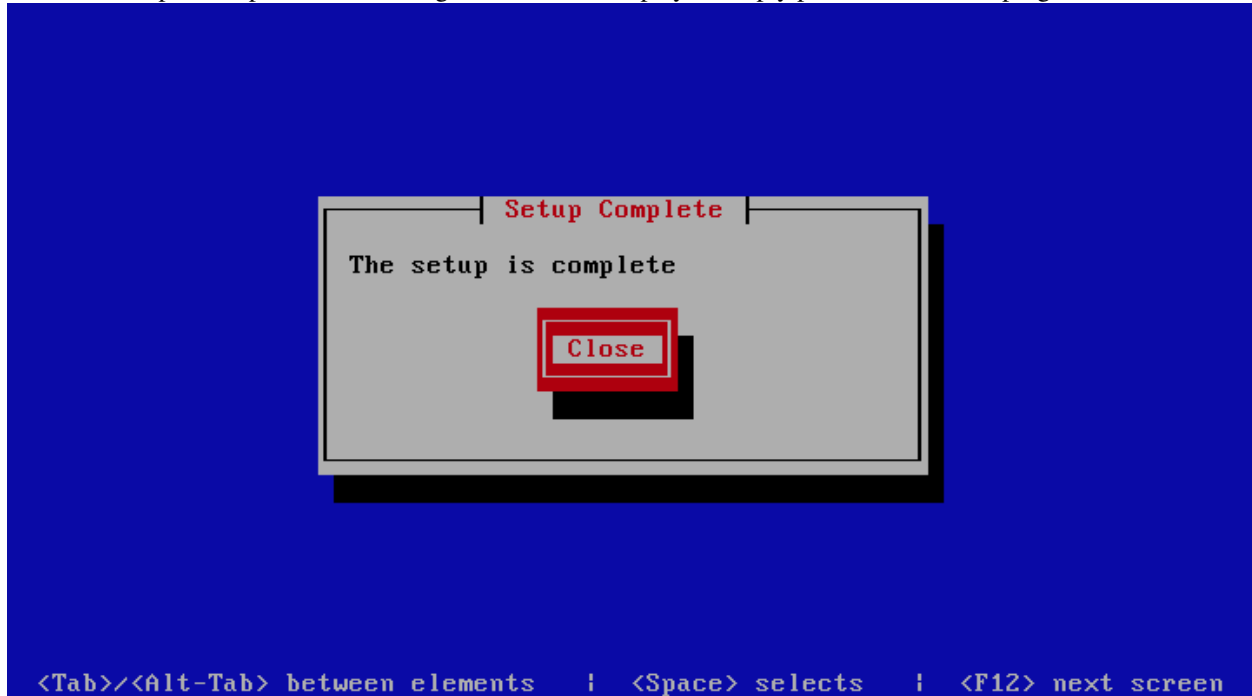
### Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.4 Message Queue System

This is a backend server in a distributed system, it provides the message queue functionality. You setup this profile if you want a dedicated server providing message queue functionality.

### 7.4.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

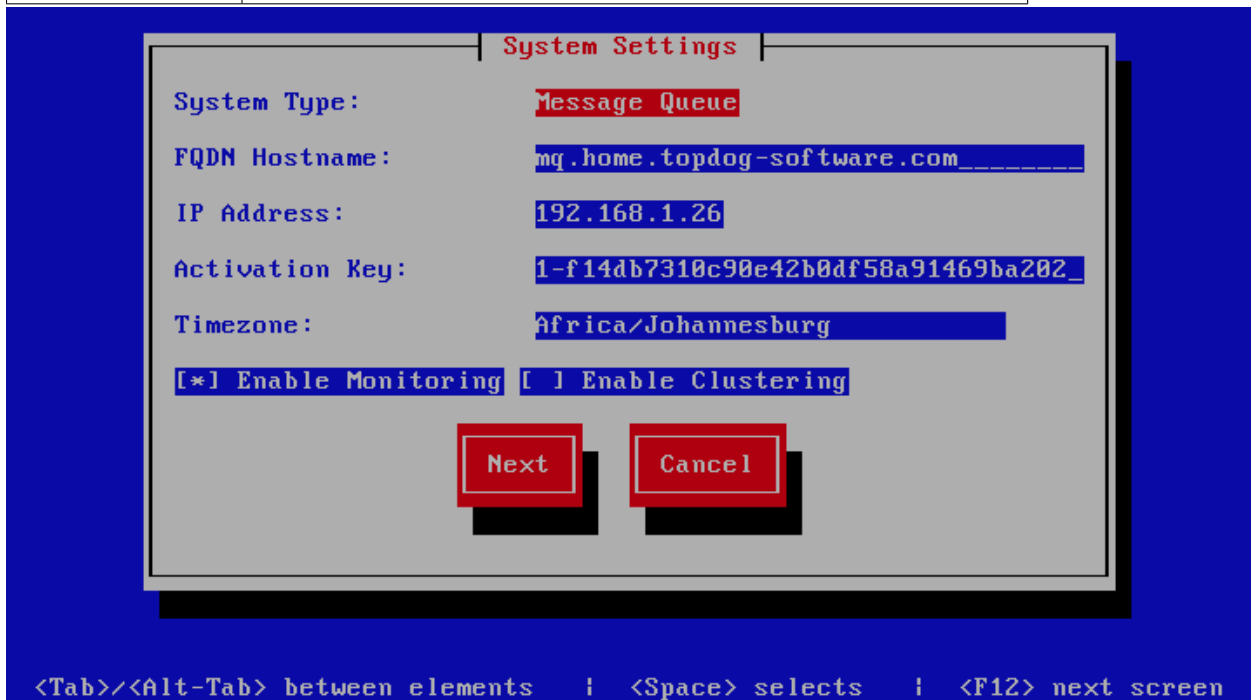
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

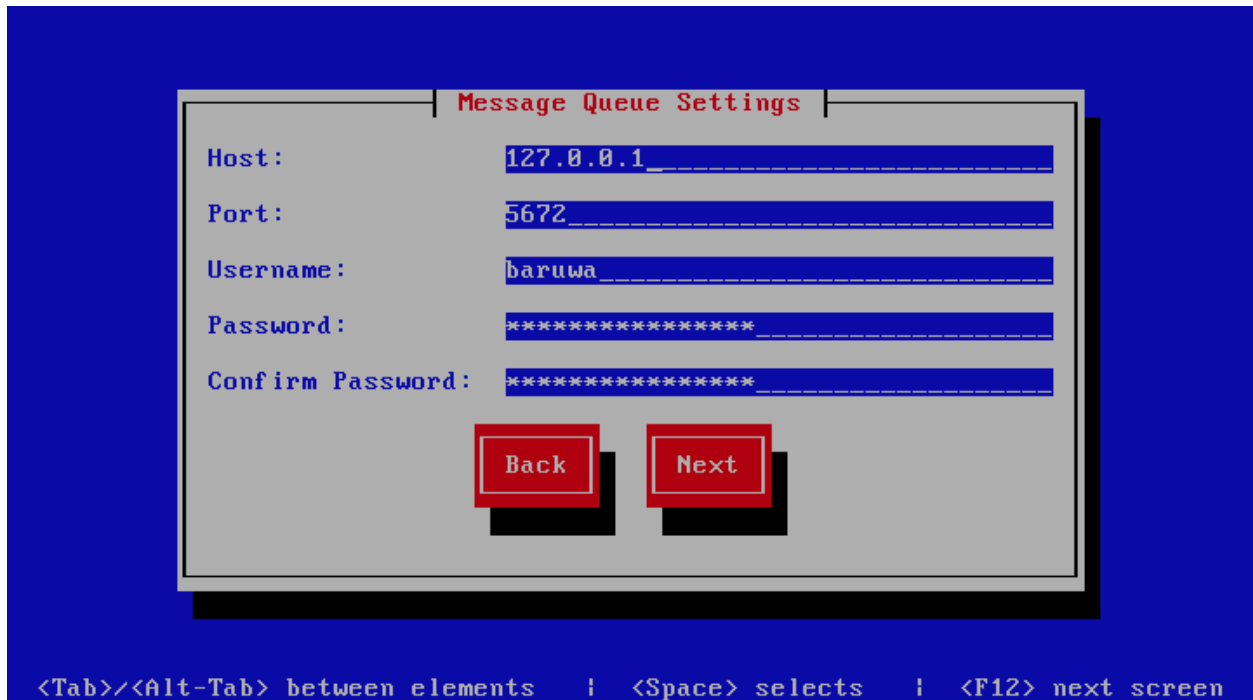
Option	Description
System Type	Set this to Message Queue
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service



### Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### Admin Settings

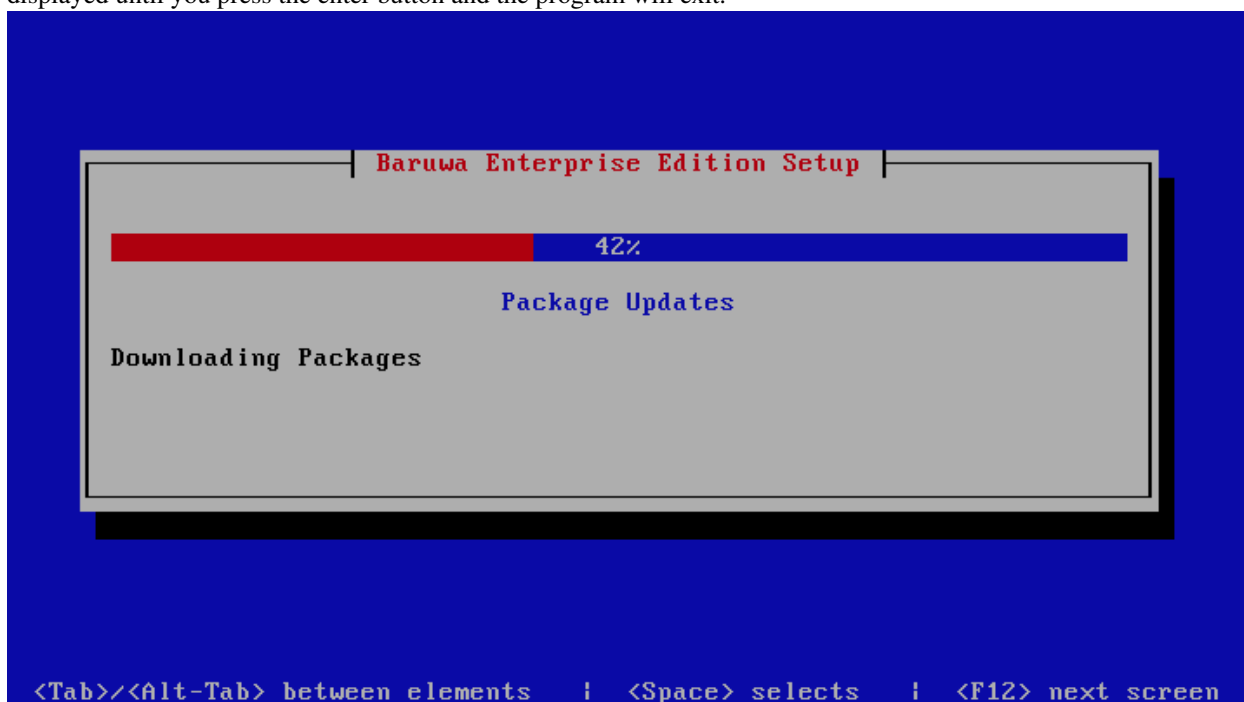
The screen sets admin settings, The description of the options is as follows:

Option	Description
Email Address	This email address will receive system notifications from the host, it is aliased to the root account



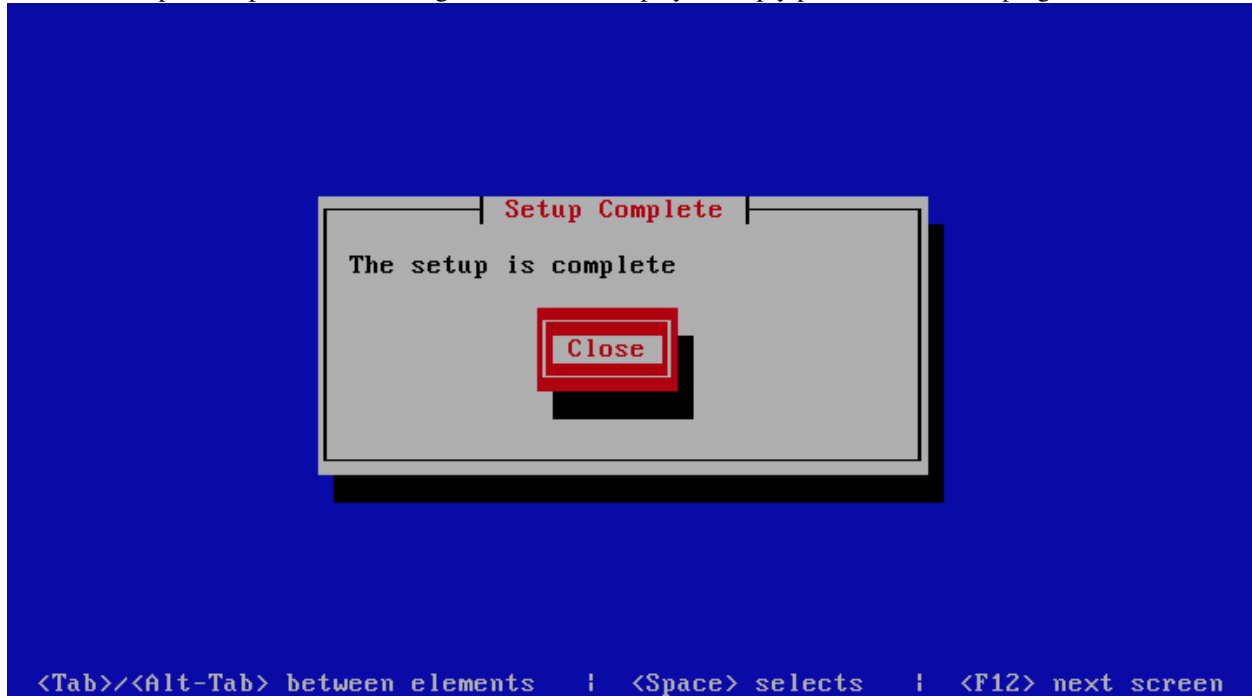
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.5 Cache System

This is a backend server in a distributed system, it provides the cache functionality. You setup this profile if you want a dedicated server providing cache functionality.

### 7.5.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

```
# baruwa-setup
```

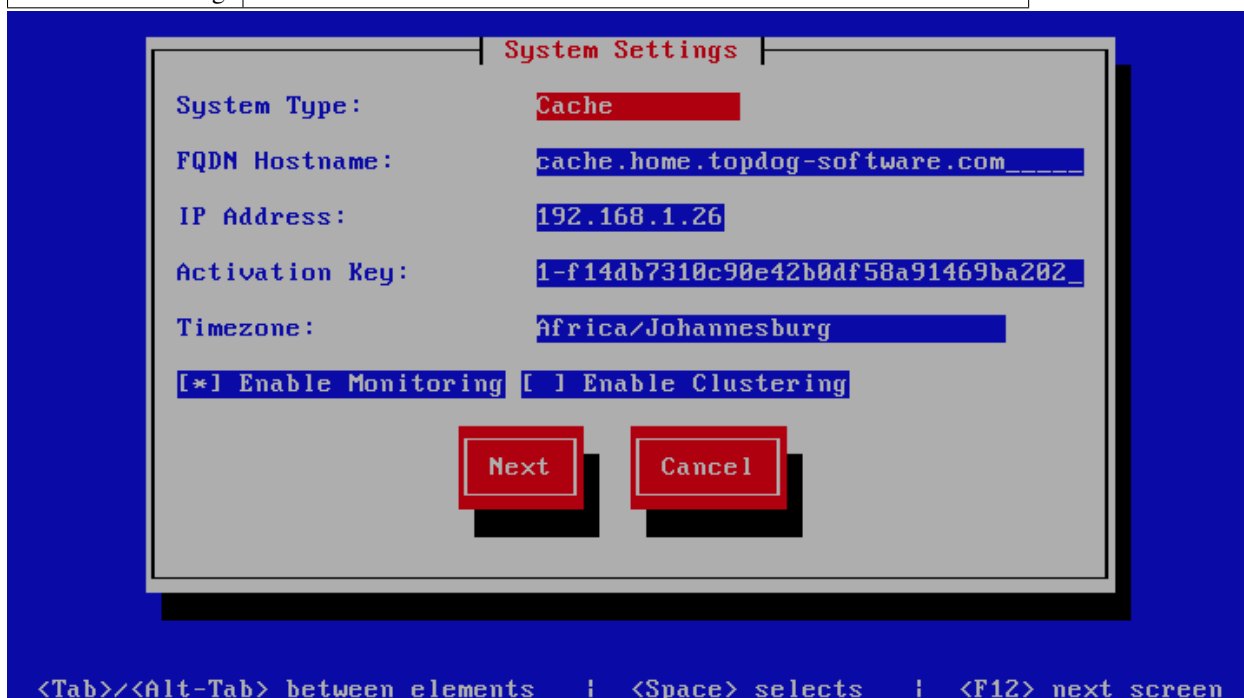


The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

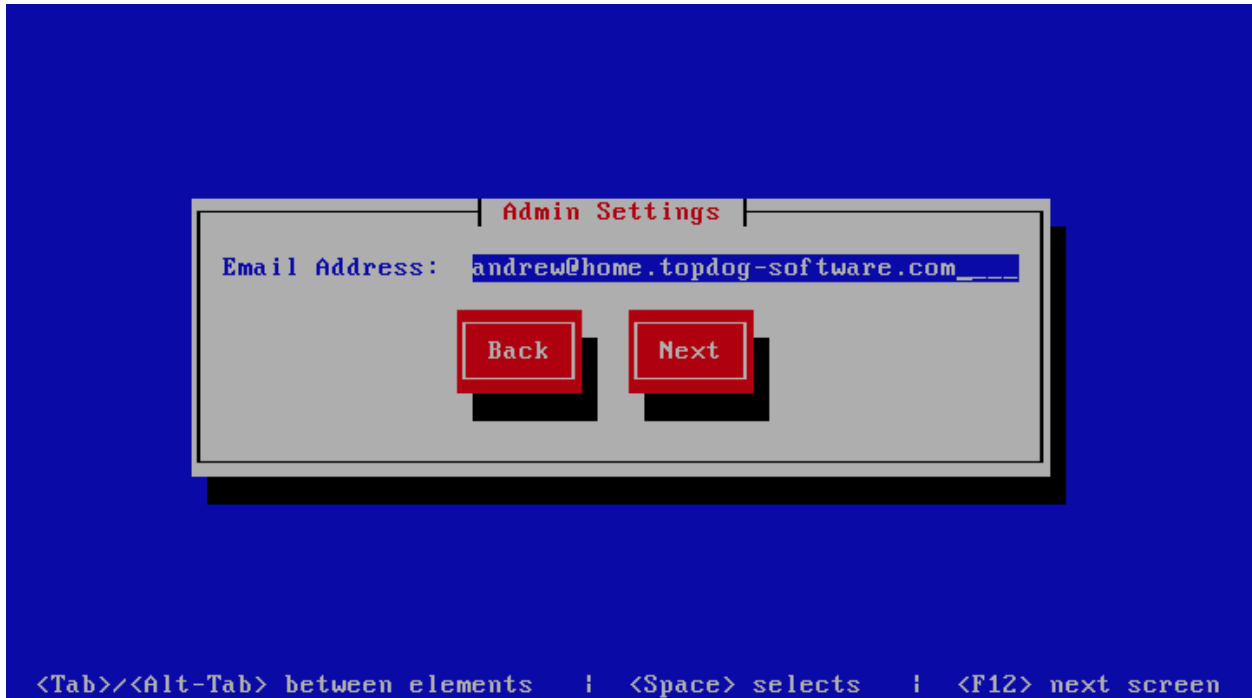
Option	Description
System Type	Set this to Cache
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Do not check this
Enable Monitoring	Check this to enable the NRPE service



### Admin Settings

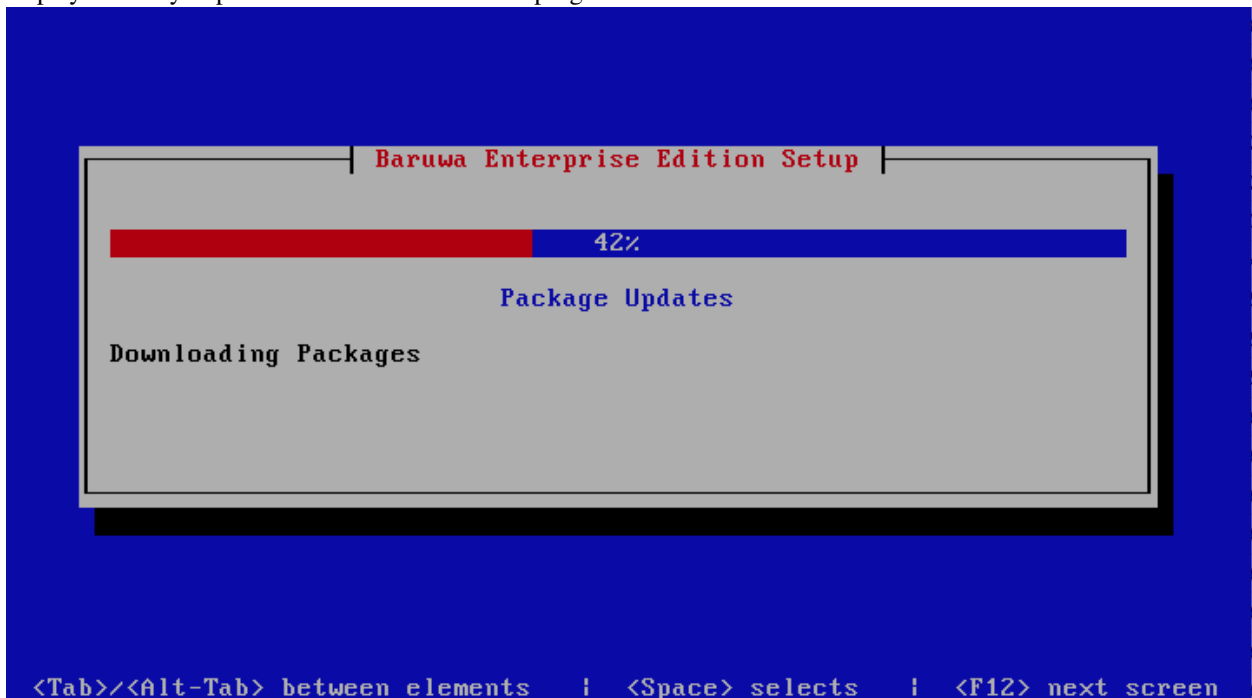
The screen sets admin settings, The description of the options is as follows:

Option	Description
Email Address	This email address will receive system notifications from the host, it is aliased to the root account



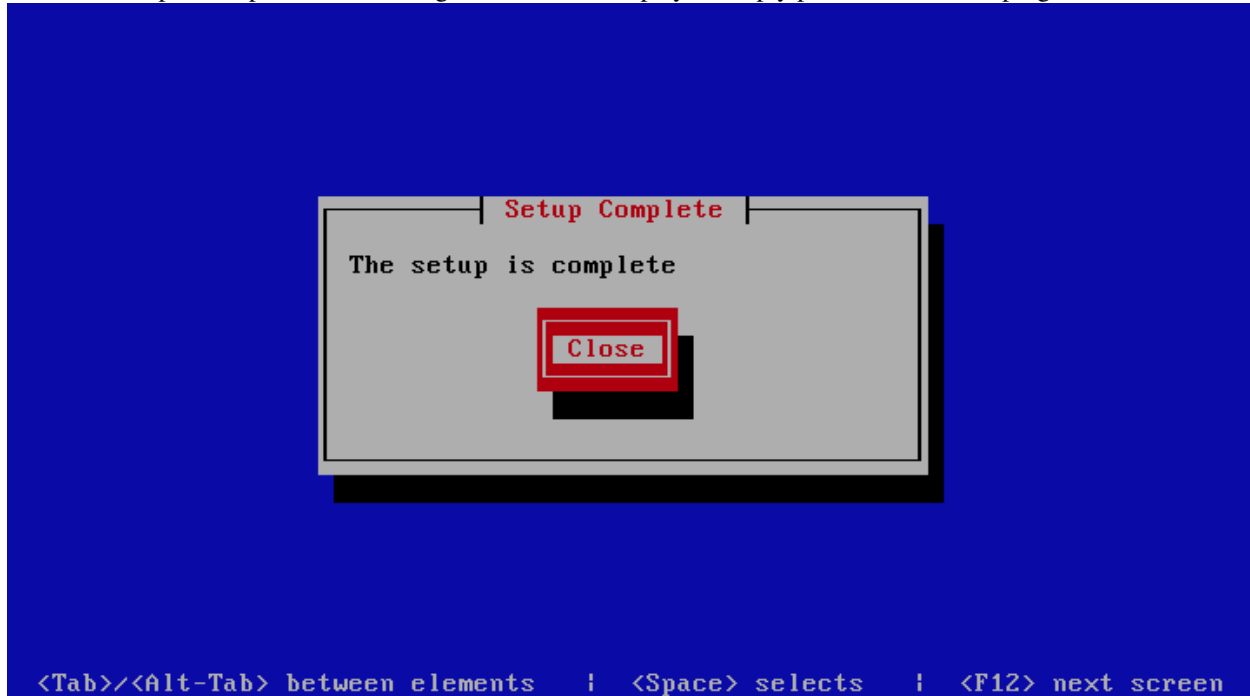
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.6 Web and Mail System

This is a frontend system it provides the mail and web interfaces, mail is delivered to the server and at the same time it serves as the web interface for both administration as well as end user access. This system requires a backend system or distributed backend systems. You can have several of these nodes scaling up or down as demand grows or drops.

### 7.6.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

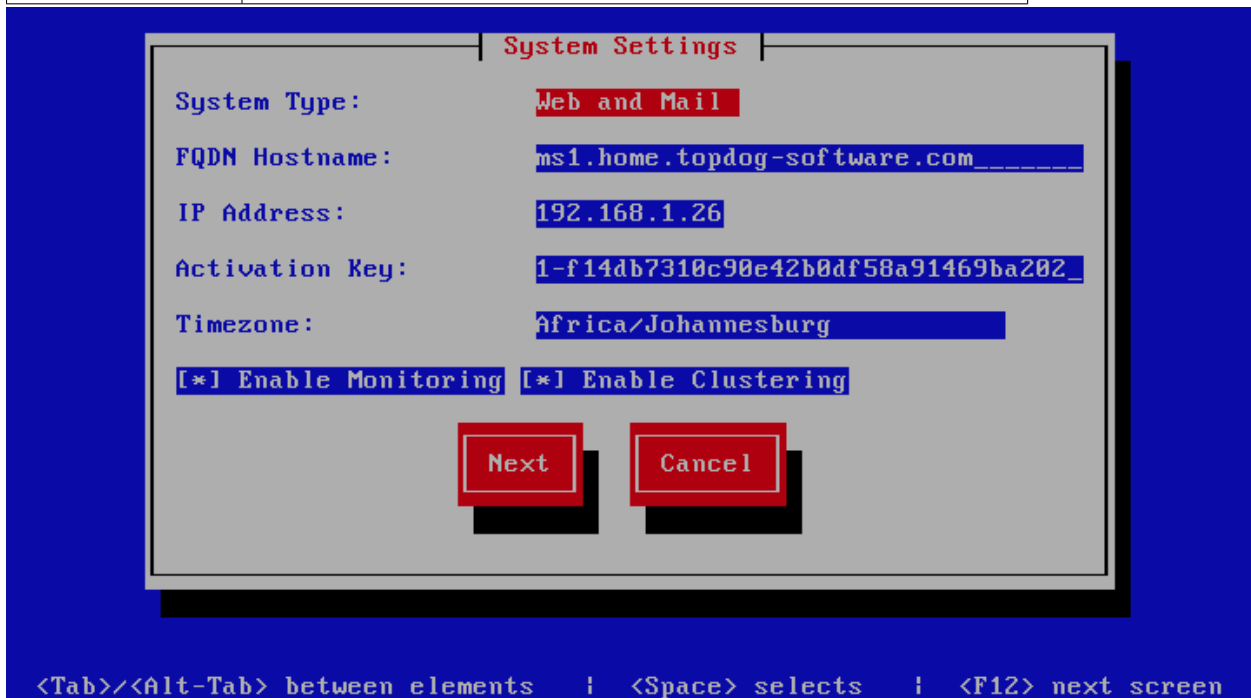
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

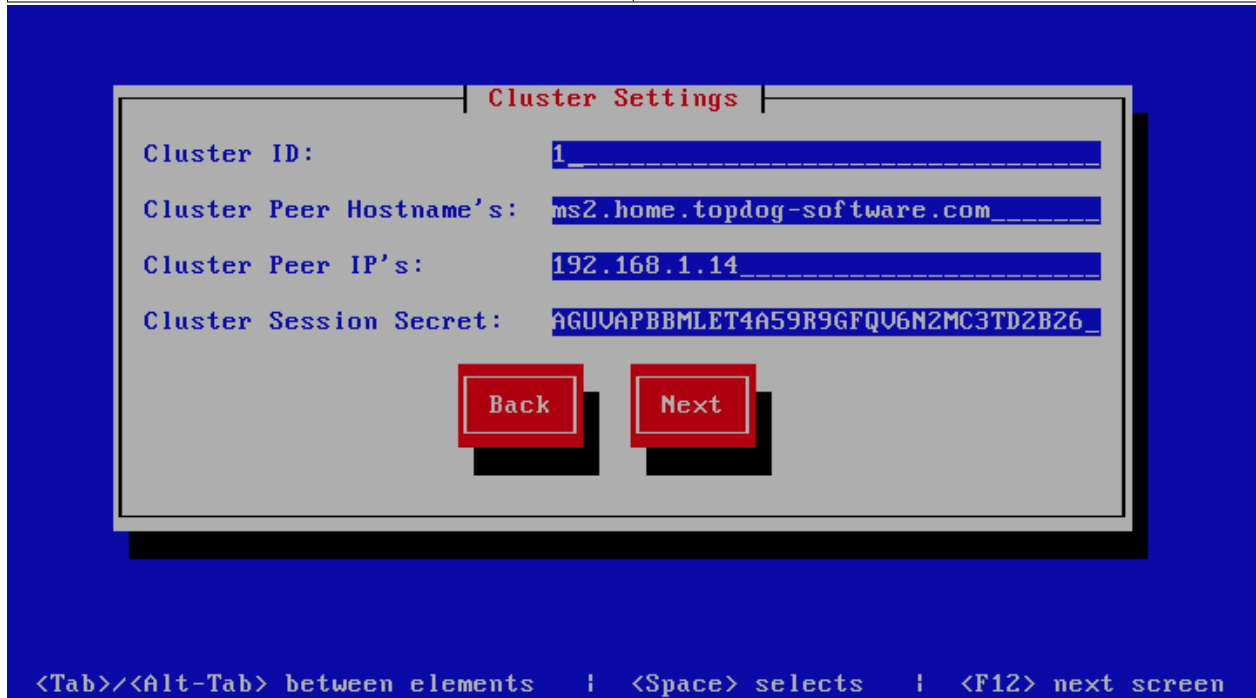
Option	Description
System Type	Set this to Web and Mail
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check this
Enable Monitoring	Check this to enable the NRPE service



### Cluster Settings

This screen configures the cluster settings. The description of the options is as follows:

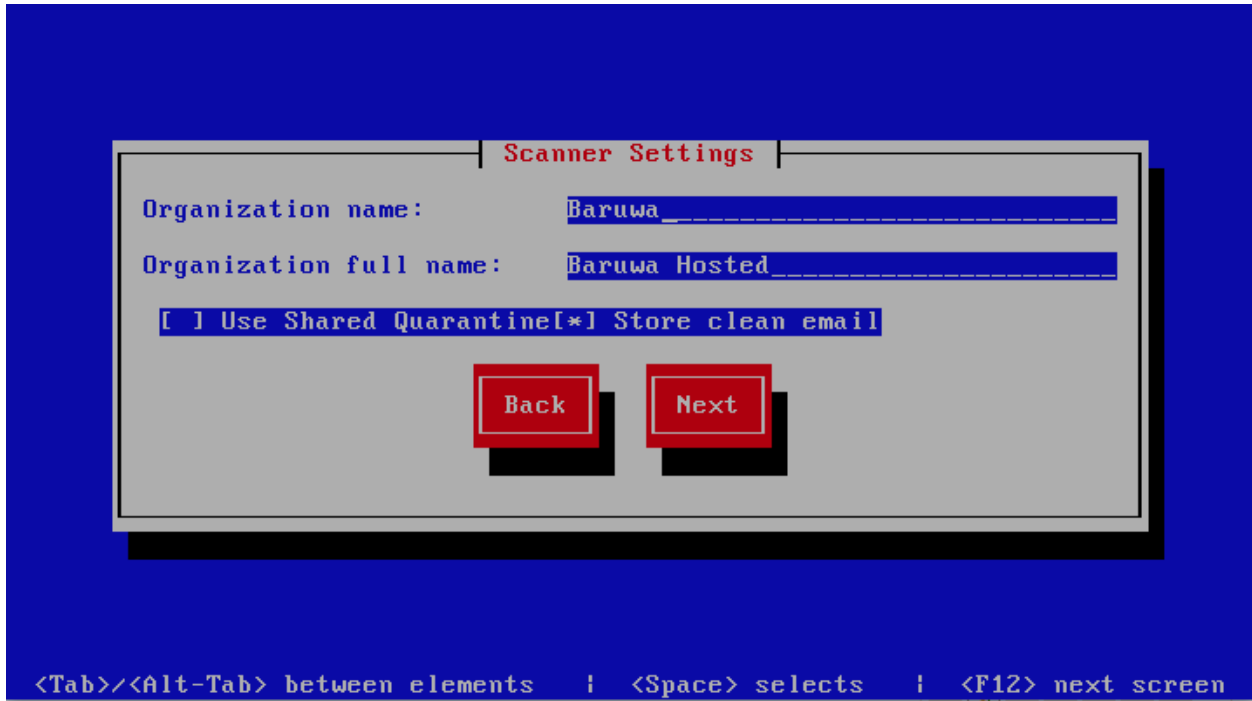
Option	Description
Cluster ID	An integer number unique to each node
Cluster Peer Hostname's	A space separated list of this nodes peers
Cluster Peer IP's	A space separated list of this nodes peers
Cluster Session Secret	This is used to encrypt session information a long password string over 35 characters, the same value should be used on all the cluster members. You can use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate it



### Scanner Settings

This screen sets the email scanner settings, The description of the options is as follows:

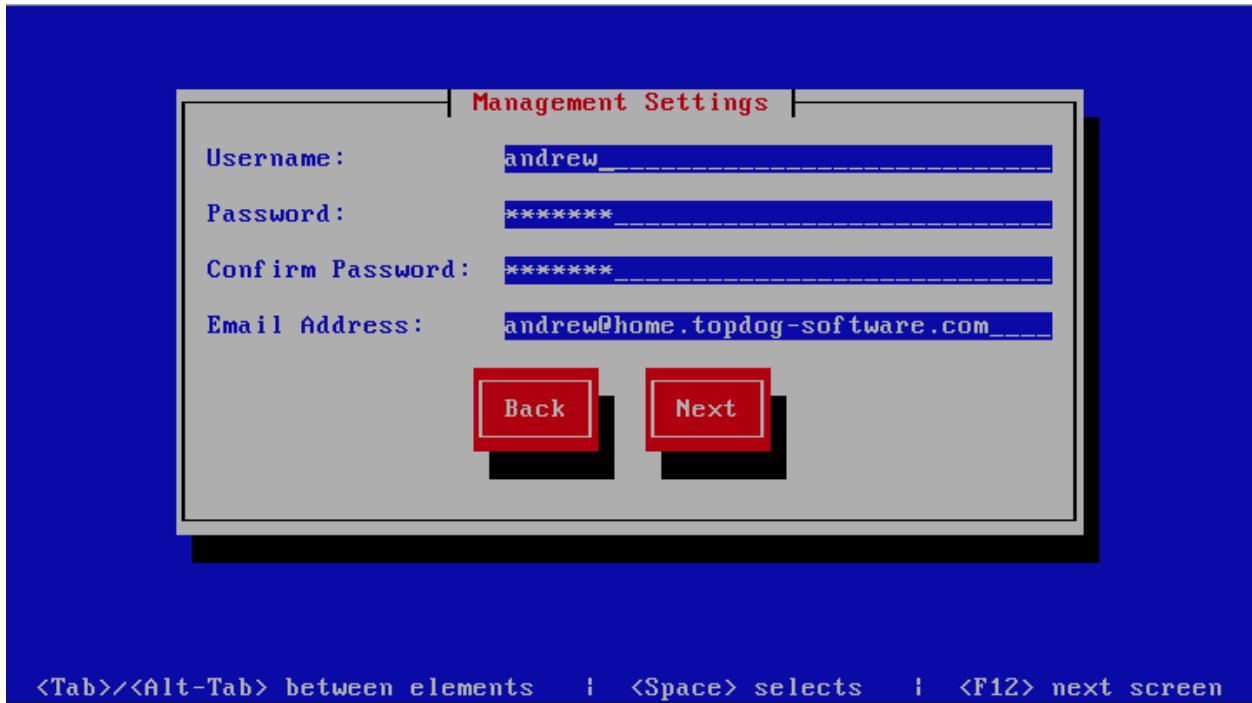
Option	Description
Organization name	Enter a short identifying name for your organisation this is used to make the X-Baruwa headers unique for your organisation Multiple servers within one site should use an identical value here. It must not contain any spaces.
Organization full name	Enter the full name of your organisation, this is used in the signature placed at the bottom of report messages sent by Baruwa. It can include pretty much any text you like. You can make the result span several lines by including “n” sequences in the text. These will be replaced by line-breaks.
Use Shared Quarantine	Check this only if you have setup a shared filesystem for the mail quarantine and configured the server to mount the <code>/var/spool/MailScanner/quarantine</code> directory to it
Store clean mail	Check this if you want to store messages not tagged as SPAM, Use this option only if it is legal in your country



## Management Settings

The screen sets the management account settings, The description of the options is as follows:

Option	Description
Username	Administrator username
Password	Administrator password, Only strong passwords will be accepted use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address

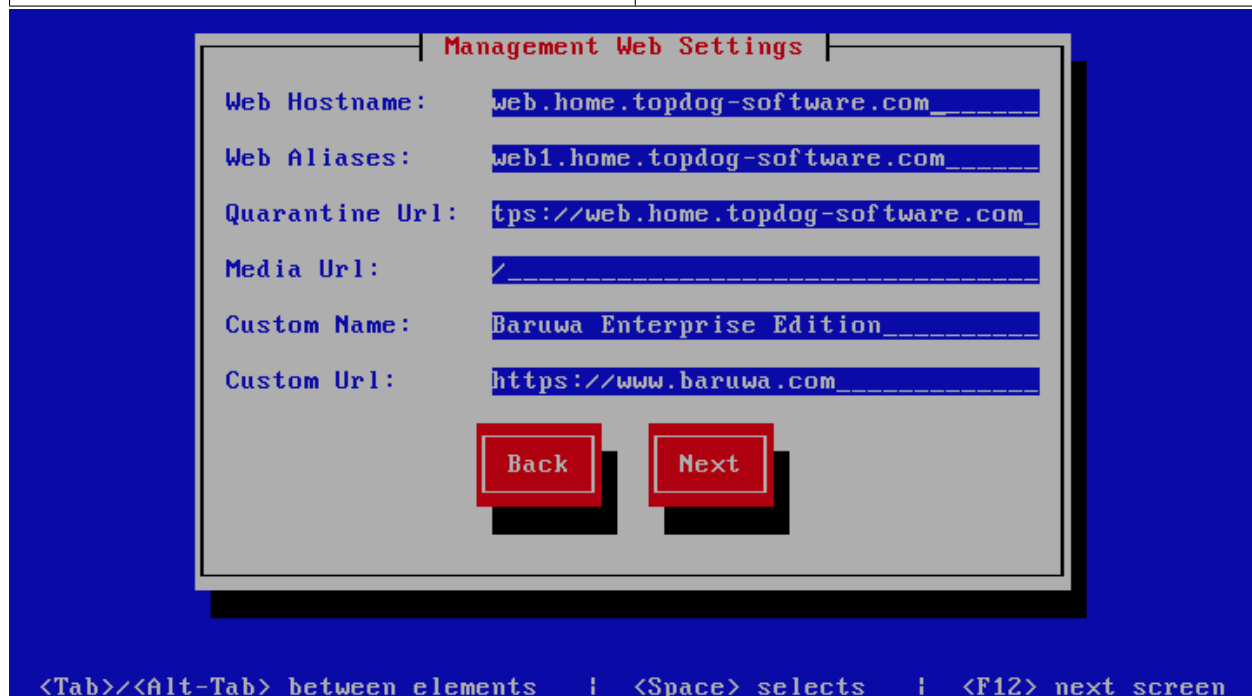


### Management Web Settings

The screen sets the management web interface settings, The description of the options is as follows:



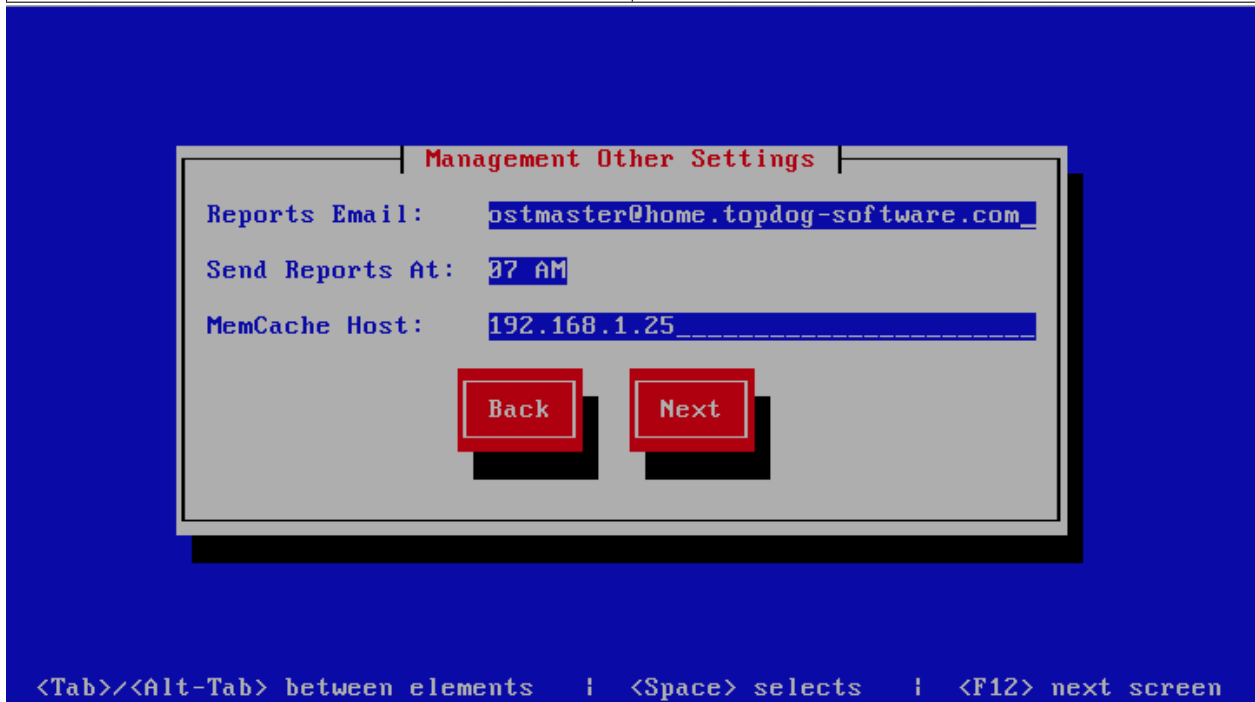
Option	Description
Web Hostname	The hostname to be used to access the web interface
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the web interface as well.
Custom URL	This creates links to your product page within the web interface and email reports that are sent out.



### Management Other Settings

The screen sets other management settings, The description of the options is as follows:

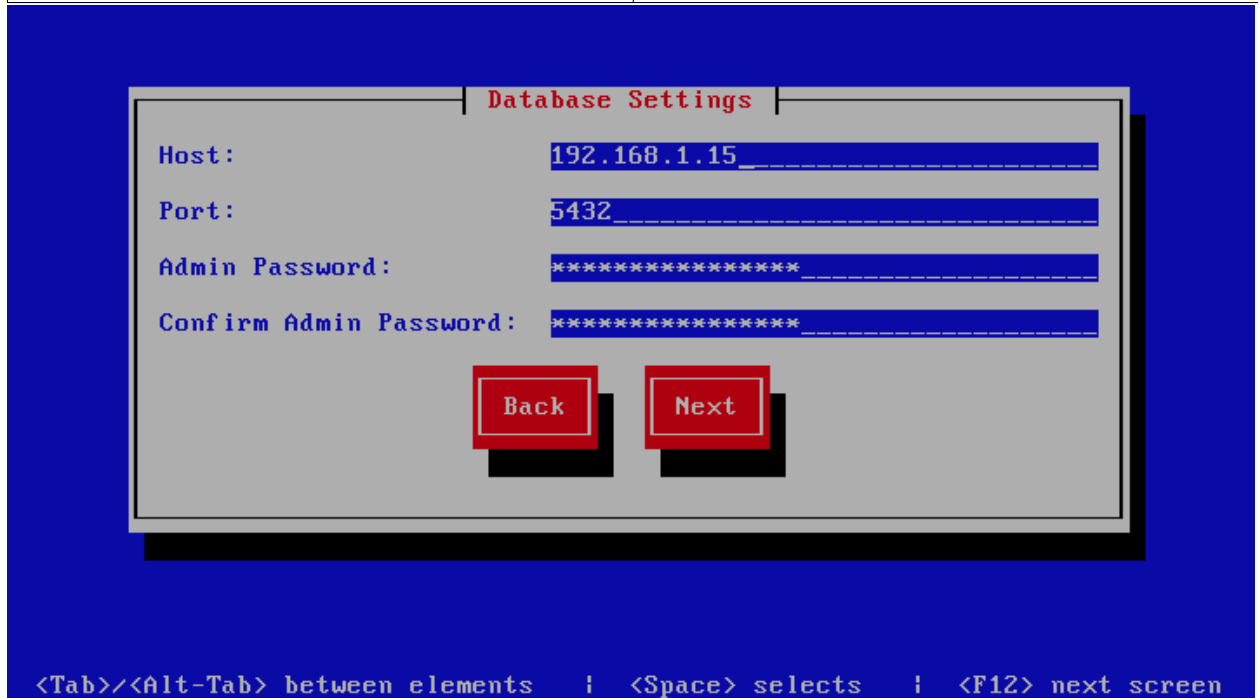
Option	Description
Reports Email	The email address used to send out email reports
Send Reports At	The hour at which to send reports, this is localized to the users location based on their timezone setting
MemCache Host	The IP address of the Memcache Server



### Database Settings

The screen sets database settings, The description of the options is as follows:

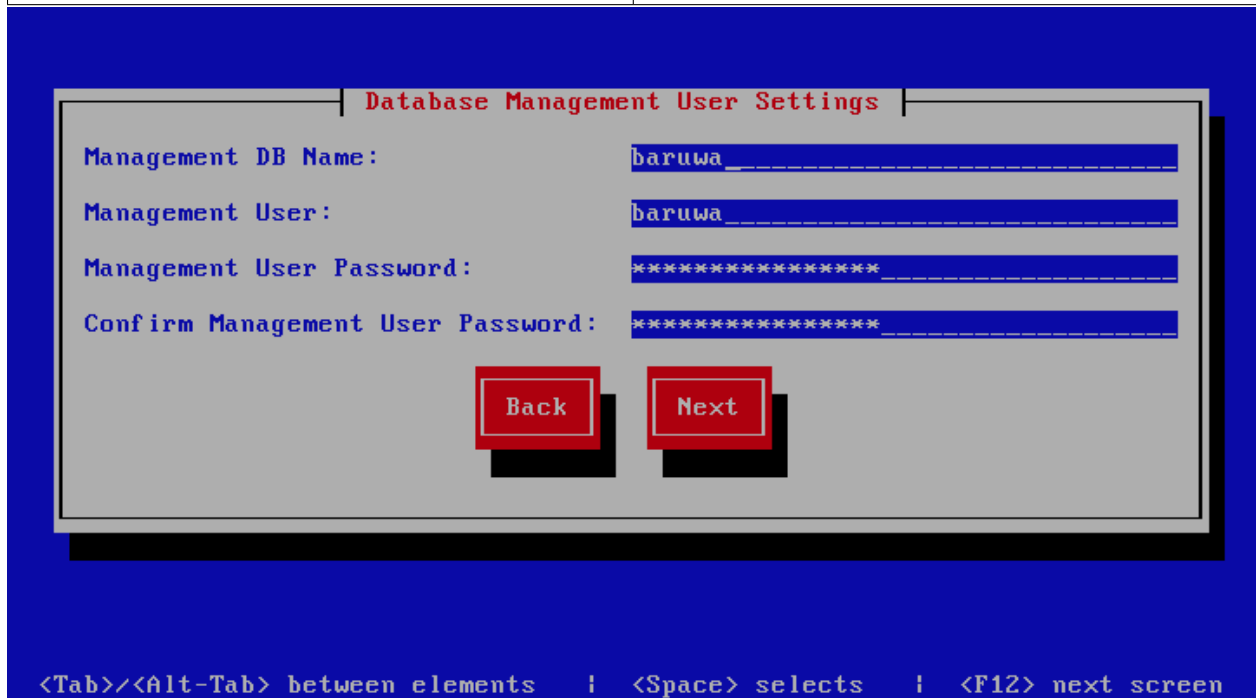
Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password



### Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:

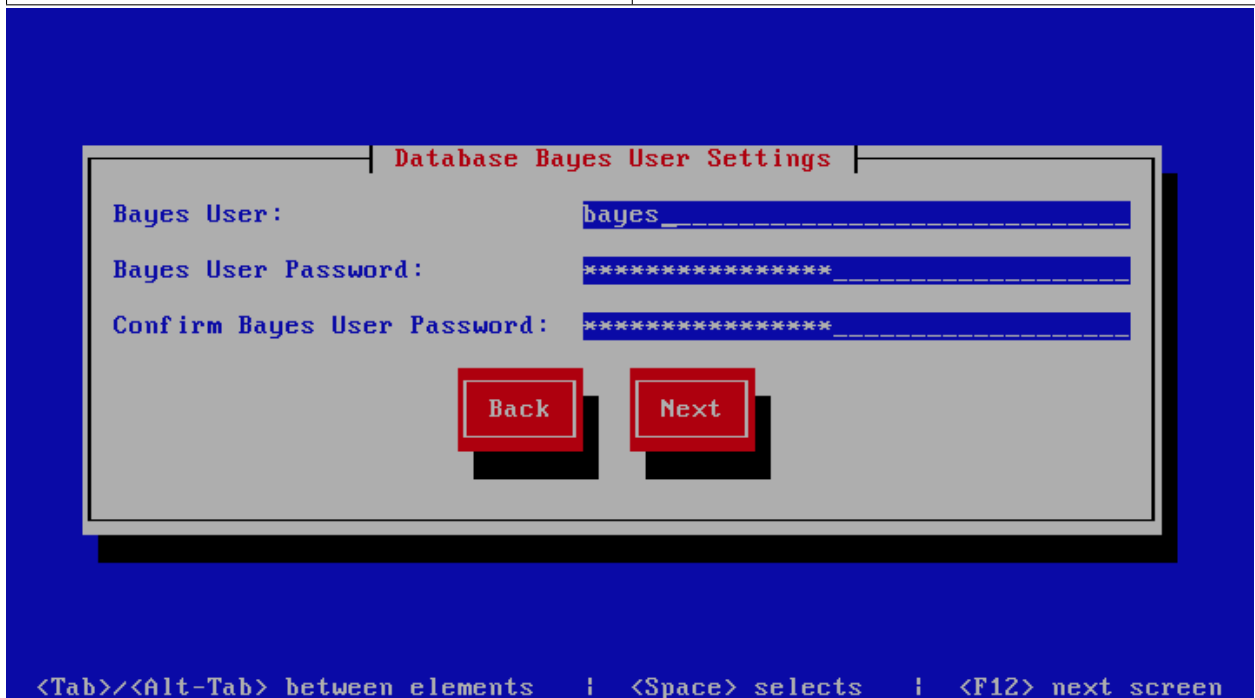
Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password



### Database Bayes User Settings

The screen sets database bayes user settings, The description of the options is as follows:

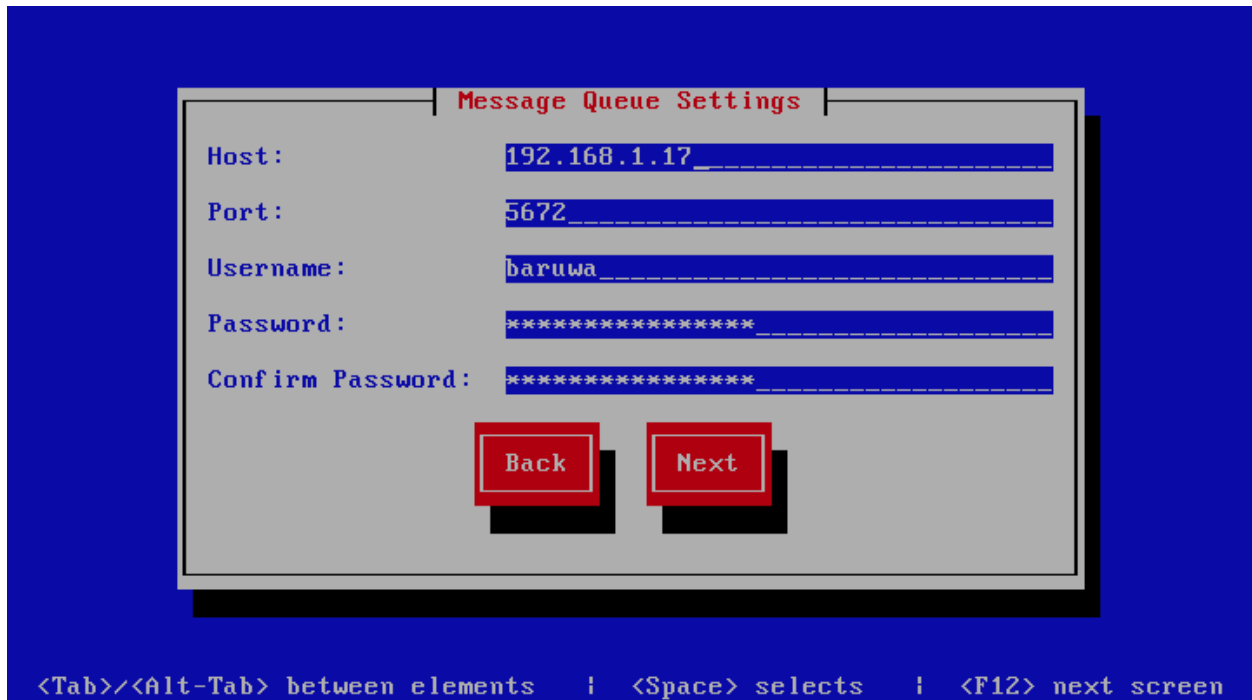
Option	Description
Bayes User	The bayes database username
Bayes User Password	The bayes database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Bayes User Password	Confirm the bayes database user password



### Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

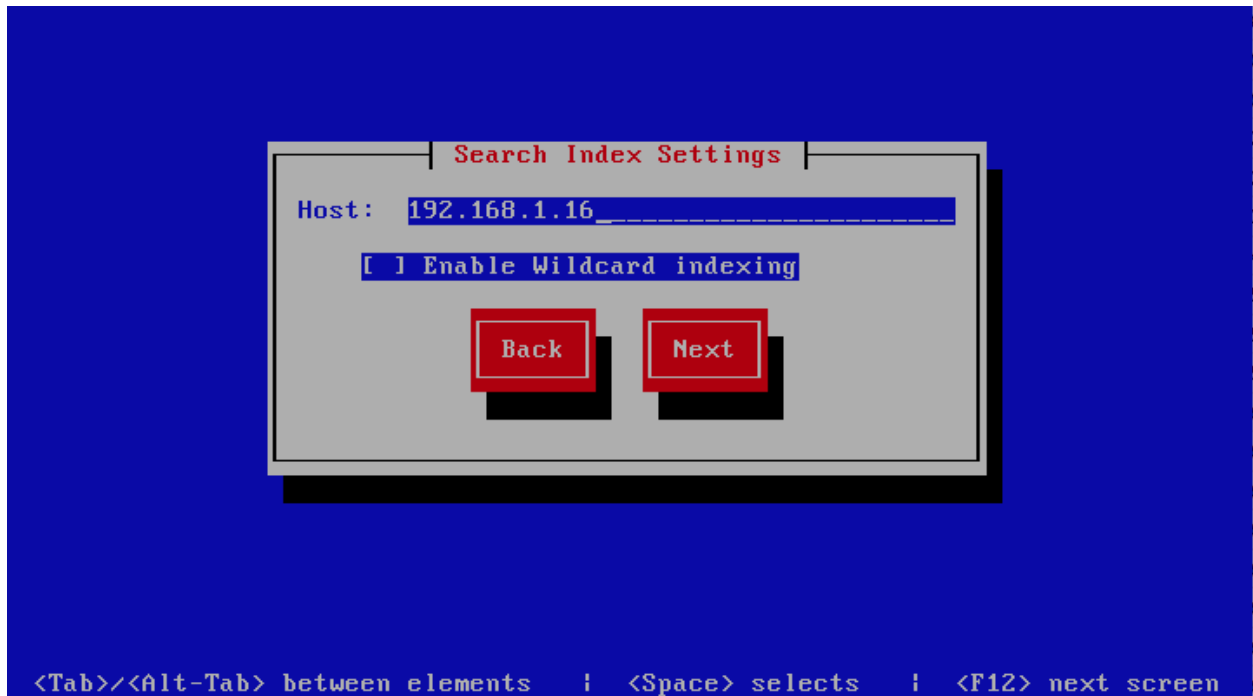
Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### Search Index Settings

The screen sets search index settings, The description of the options is as follows:

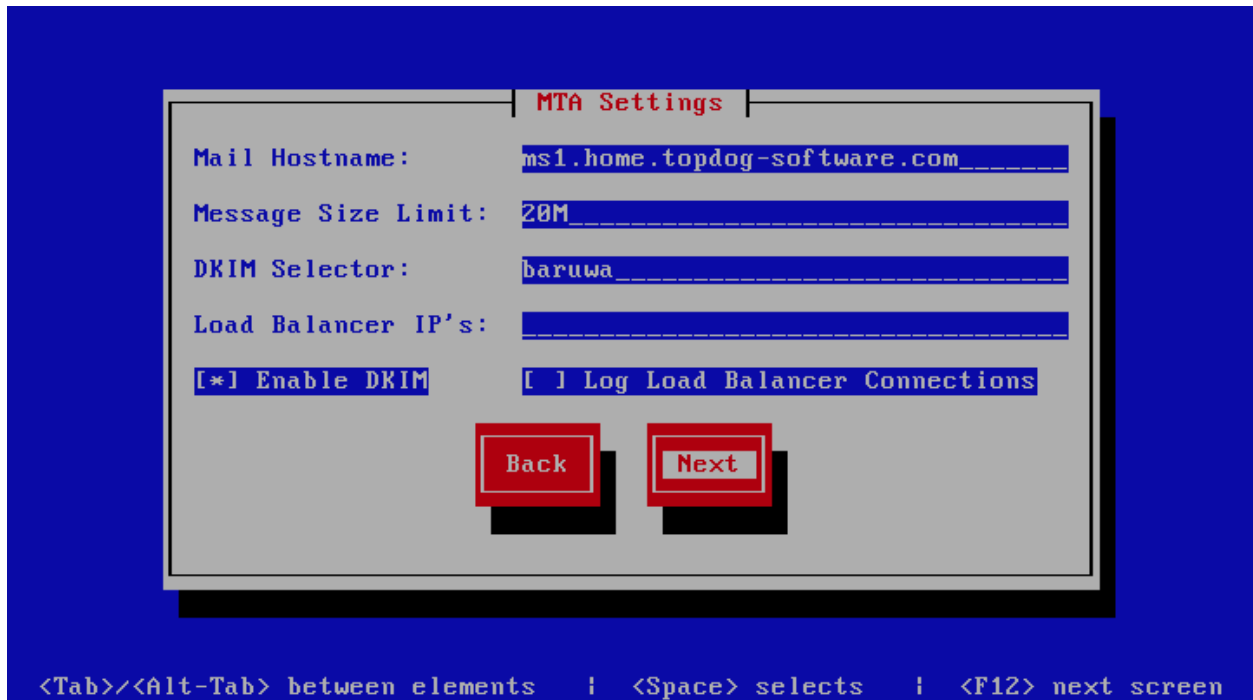
Option	Description
Host	Indexing server IP address
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



## MTA Settings

The screen sets mta settings, The description of the options is as follows:

Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable DKIM	Enable DKIM functionality
Log Load Balancer Connections	Log Load Balancer connections to the MTA log

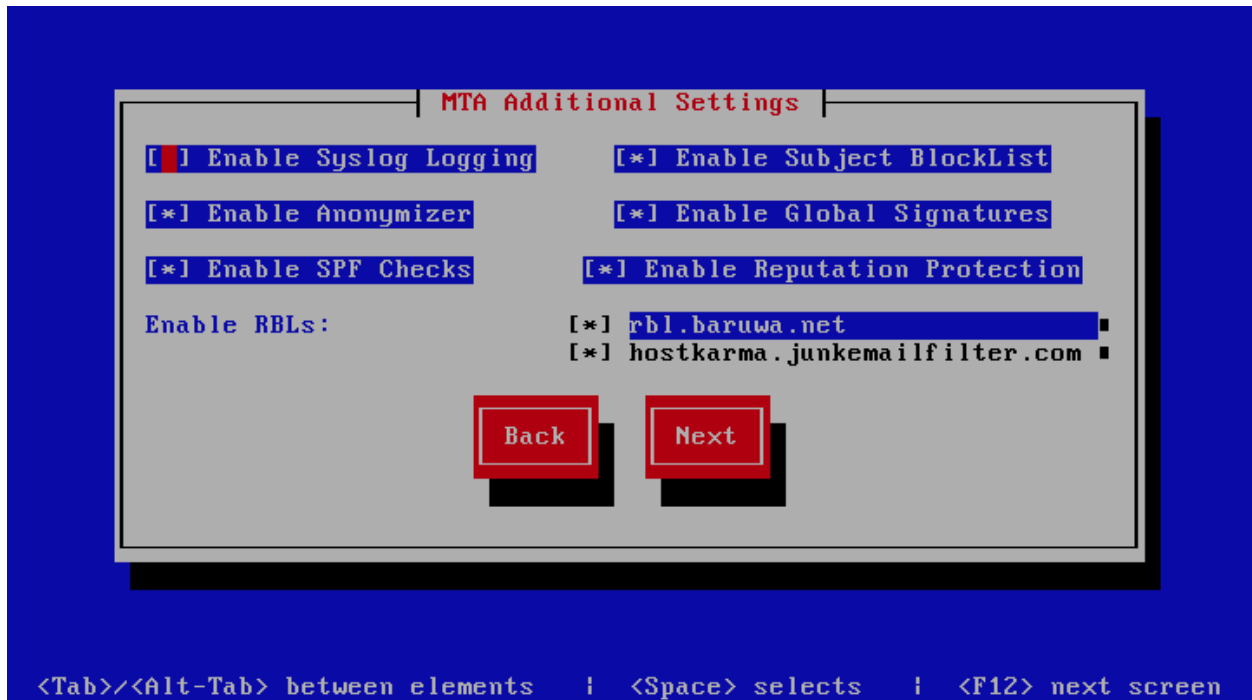


### MTA Additional Settings

The screen sets MTA additional settings, The description of the options is as follows:

Option	Description
Enable Syslog Logging	Turns on MTA logging to syslog
Enable Subject Blocklist	Enable the blocking by subject functionality
Enable Anonymizer	Enable the Anonymizer functionality
Enable Global Signatures	Enable Global Signatures
Enable SPF Checks	Enable SPF checking functionality
Enable Reputation Protection	Enables functionality to block abusive outbound SMTP requests
Enable RBLs	Select the SMTP time DNSBL's to enable

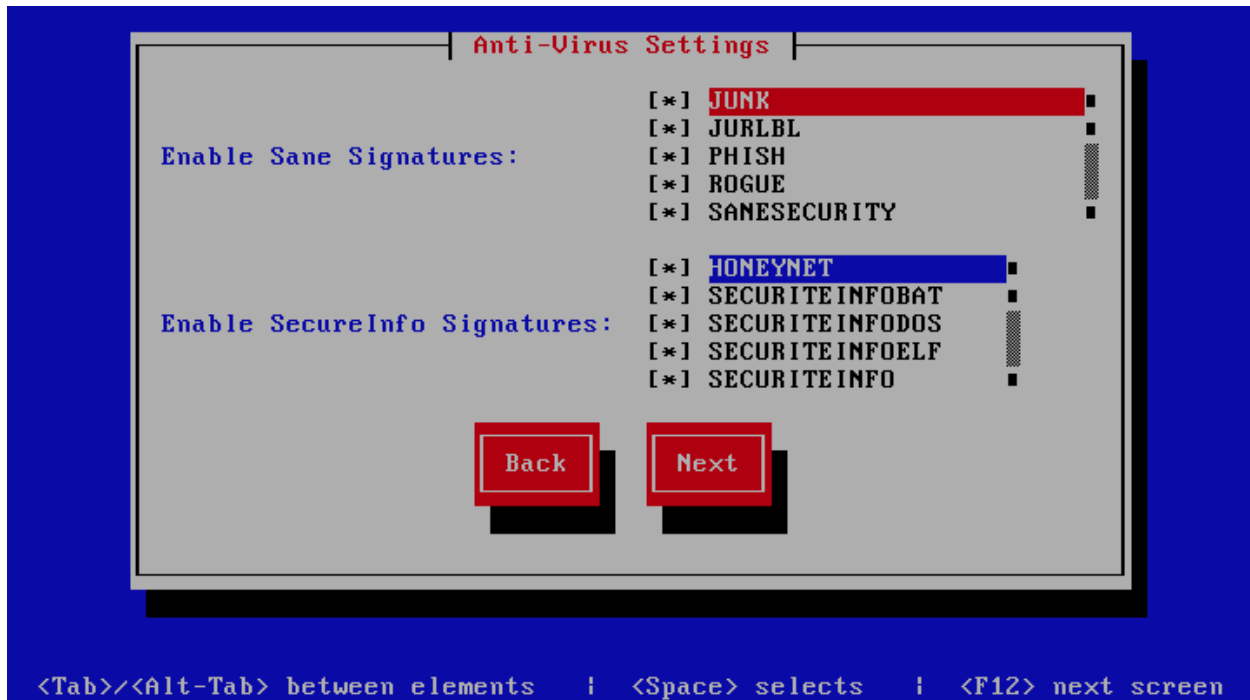




## Anti Virus Settings

The screen sets anti virus settings, The description of the options is as follows:

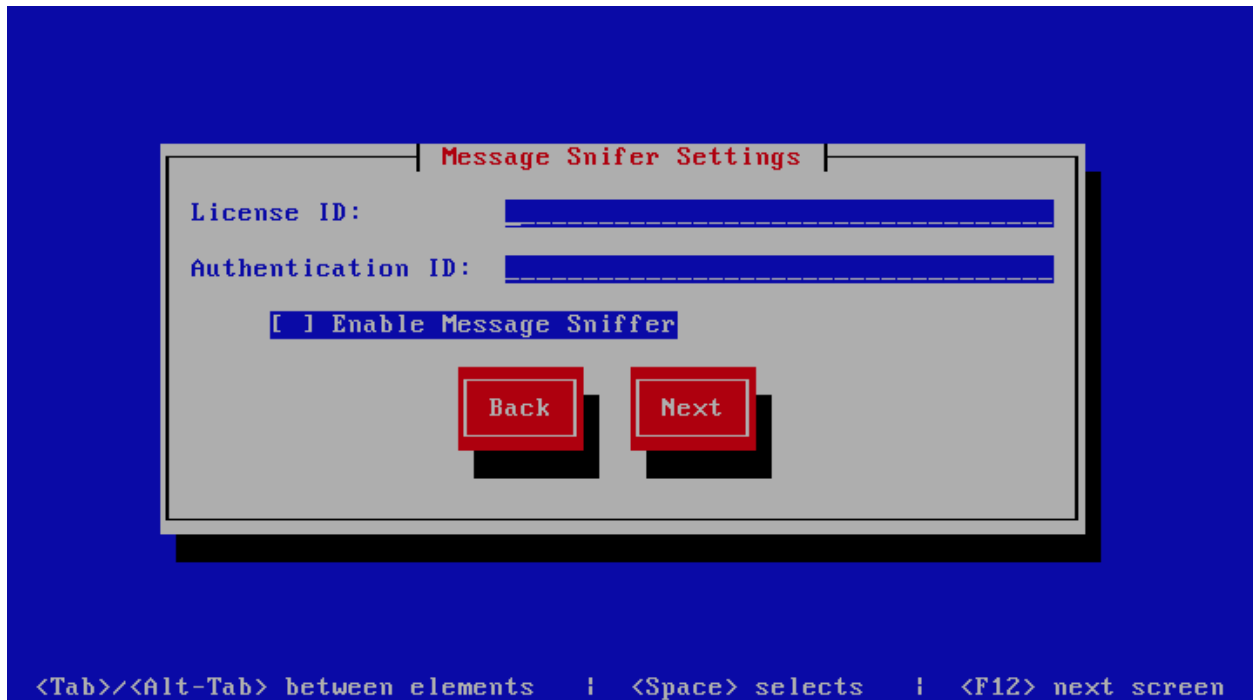
Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Enable SecureInfo Signatures	ClamAV Unofficial SecureInfo signatures to enable



### Message Sniffer Settings

The screen sets message sniffer settings, The description of the options is as follows:

Option	Description
License ID	Message Sniffer License ID This is emailed to you when you purchase a subscription
Authentication ID	Message Sniffer Authentication ID This is emailed to you when you purchase a subscription



## SSL/TLS Settings

The Baruwa web interface MUST run over SSL/TLS, other services such as SMTP AUTH only work over SSL/TLS as well. So you need to either purchase a valid SSL certificate or have `baruwa-setup` automatically generate one non recognised SSL certificate for you. If you do not have a CA issued certificate and do not intend on purchasing one the leave the `I have a CA issued Certificate` unchecked.

The certificate that `baruwa-setup` generates will cover the web hostname, web aliases, cluster members and the mail hostname. This means that you should copy this certificate to other cluster hosts that you specified and select `I have a CA issued Certificate` on those hosts when you set them up instead of generating new certificates for them.

---

**Note:** We have partnered with the SSLShop to bring you discounted SSL certificate pricing. RapidSSL CA signed certificates can be purchased at discounted pricing using the Discount coupon “BARUWA” from <http://www.sslshop.co.za>

---

If you have a SSL certificate that is issued by a recognised CA and would like Baruwa to use it, install it prior to running `baruwa-setup`. Please NOTE that you need certificates that cover the web hostname and aliases, and the mail hostname. Please check `I have a CA issued Certificate`.

The preferred location to install certificates and keys on the server is under `/etc/pki`. You need to create a directory structure under that and store your certificate under it.

The following example creates a baruwa directory under `/etc/pki` and stores the certificates and keys there:

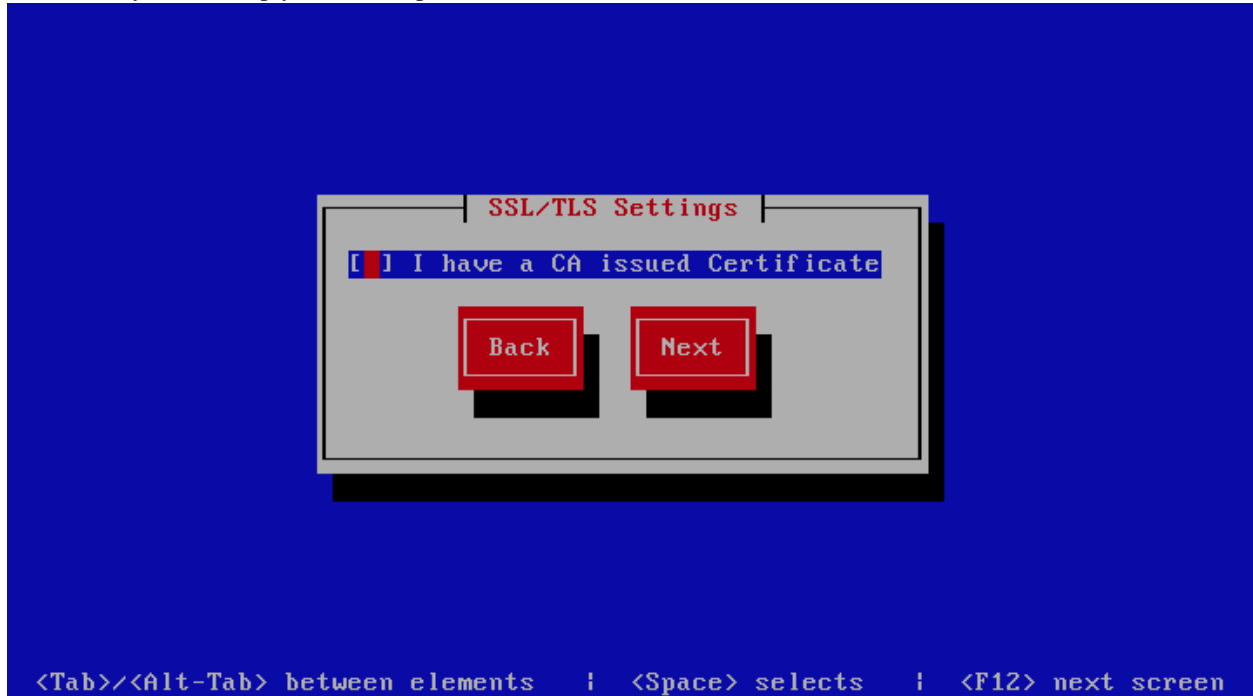
```
mkdir -p /etc/pki/baruwa/{certs,private}
```

Create the following files

- `/etc/pki/baruwa/certs/baruwa.pem` with the contents of your SSL certificate
- `/etc/pki/baruwa/private/baruwa.key` with the contents of your SSL private key

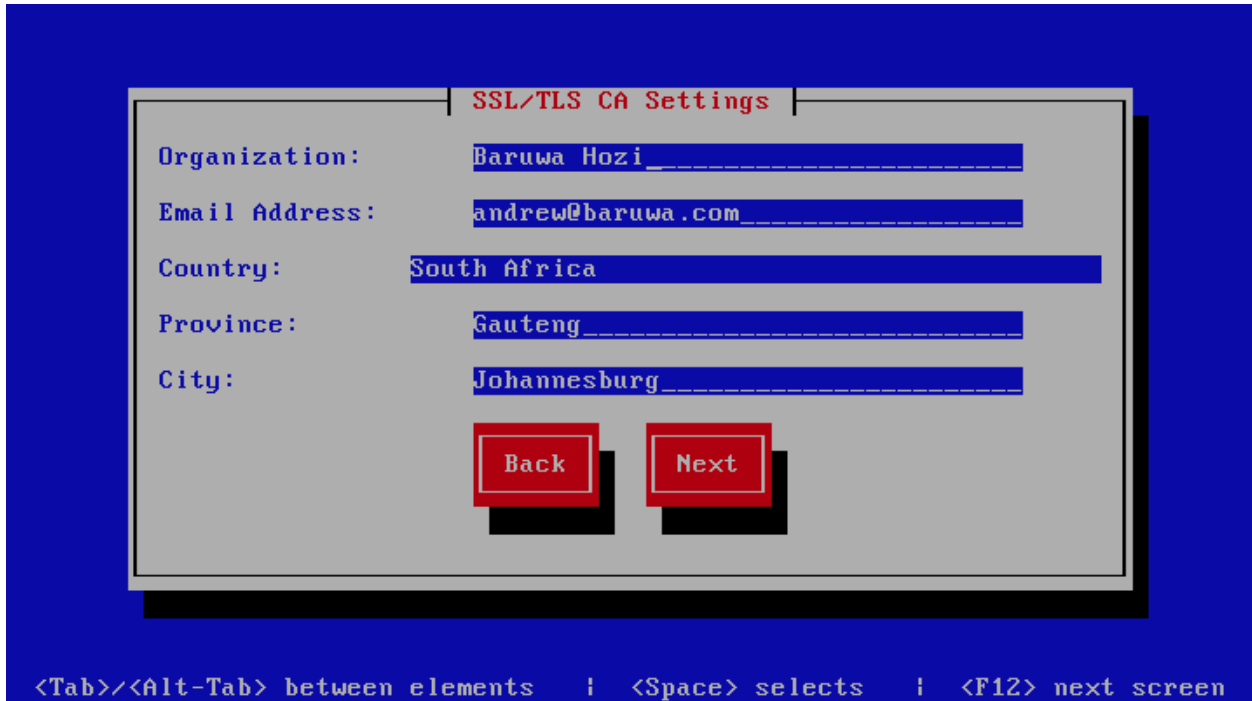
You need to create additional certificate pairs if your web hostname and mail hostname are not the same.

If you have a wildcard certificate with all your names being subdomains of that domain to which the certificate is issued then you can simply create one pair.



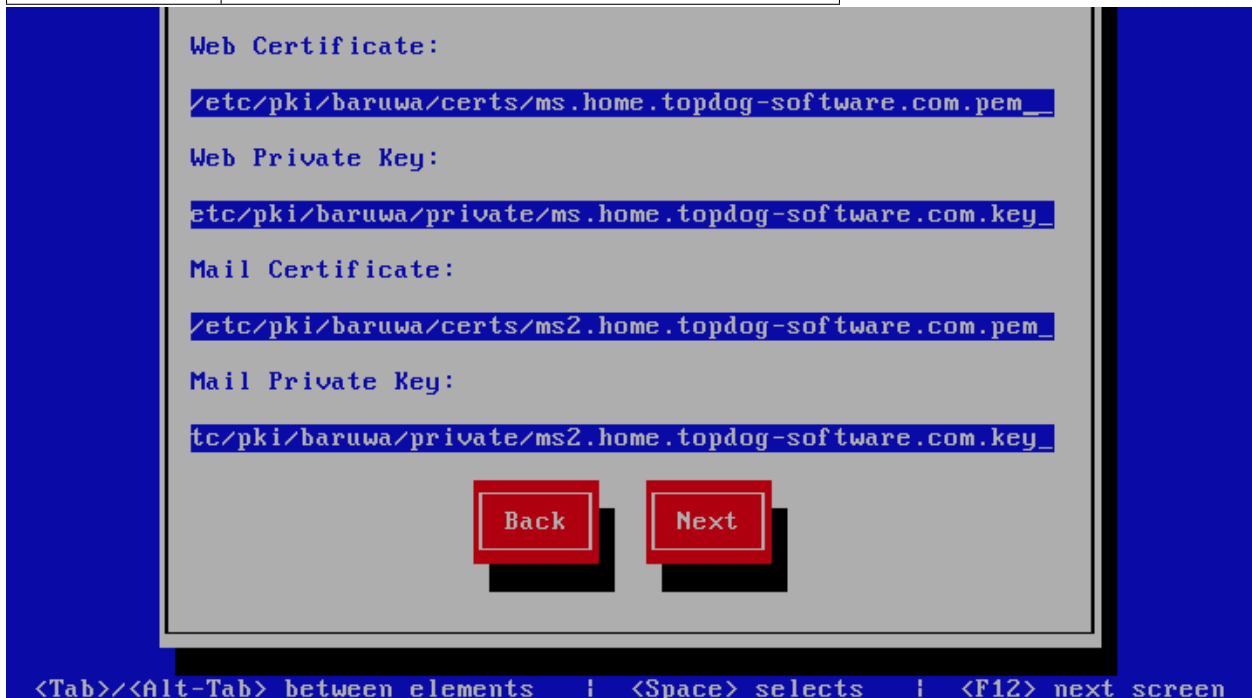
If you left I have a CA issued Certificate unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

Option	Description
Organization	OpenSSL CA Name
Email Address	OpenSSL email address
Country	OpenSSL country code
Province	OpenSSL province
City	OpenSSL city



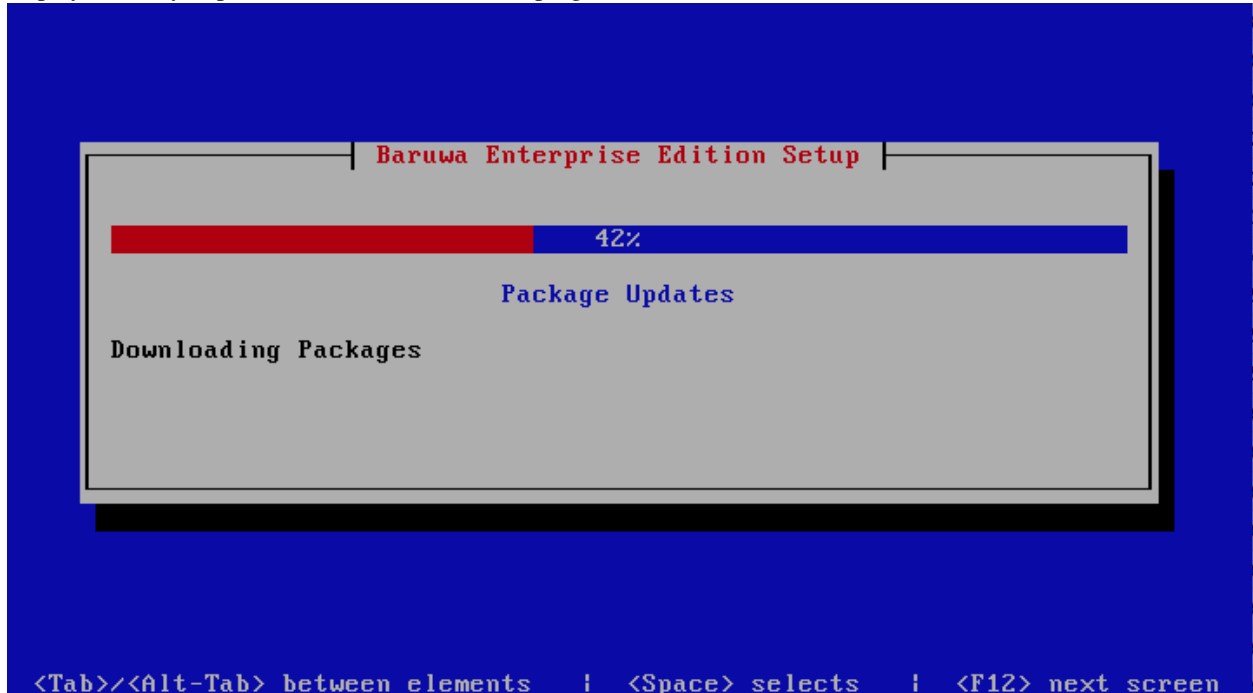
If you checked I have a CA issued Certificate you will be presented with the following screen, you need to specify the locations of your certificates and keys. The description of the options is as follows:

Option	Description
Web Certificate	The location of the web certificate file in PEM format
Web Private Key	The location of the web private key file in PEM format
Mail Certificate	The location of the mail certificate file in PEM format
Mail Private Key	The location of the mail private key file in PEM format



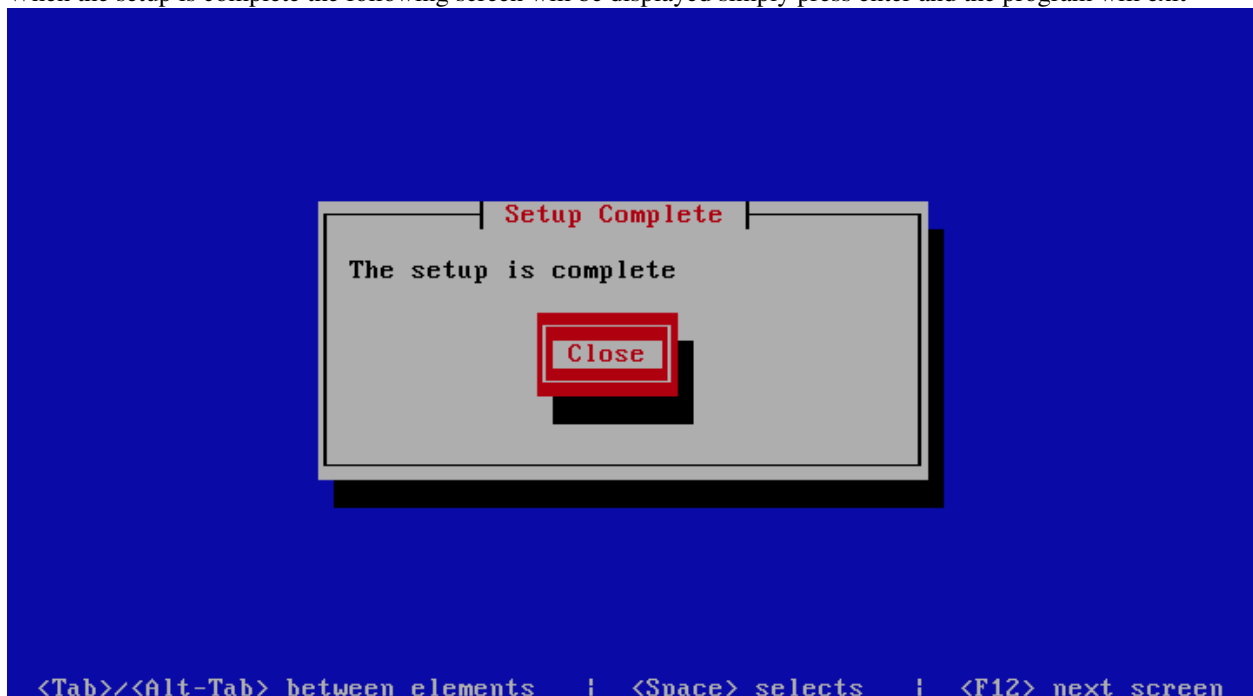
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.6.2 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a scanning Node*, *Add an Organization*, *Adding a Domain* and *Adding an Account*. This is done through the management web interface.

The exact sequence to follow is:

- Add the Node
- Add an Organization
- Add a Domain Administrator for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add a Domain to the Organization
- Add a delivery server for the Domain
- Add any user accounts to the Domain if not using external authentication

Review the *Administrators guide* and *Advanced configuration* for other configuration and setup options available.

## 7.7 Mail System

This is a front-end system that is dedicated to processing mail, it does not provide a web interface for administration as well as user access. You setup this kind of system if you want dedicated servers processing mail only. You can have several of these nodes scaling up or down as demand grows or drops.

### 7.7.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

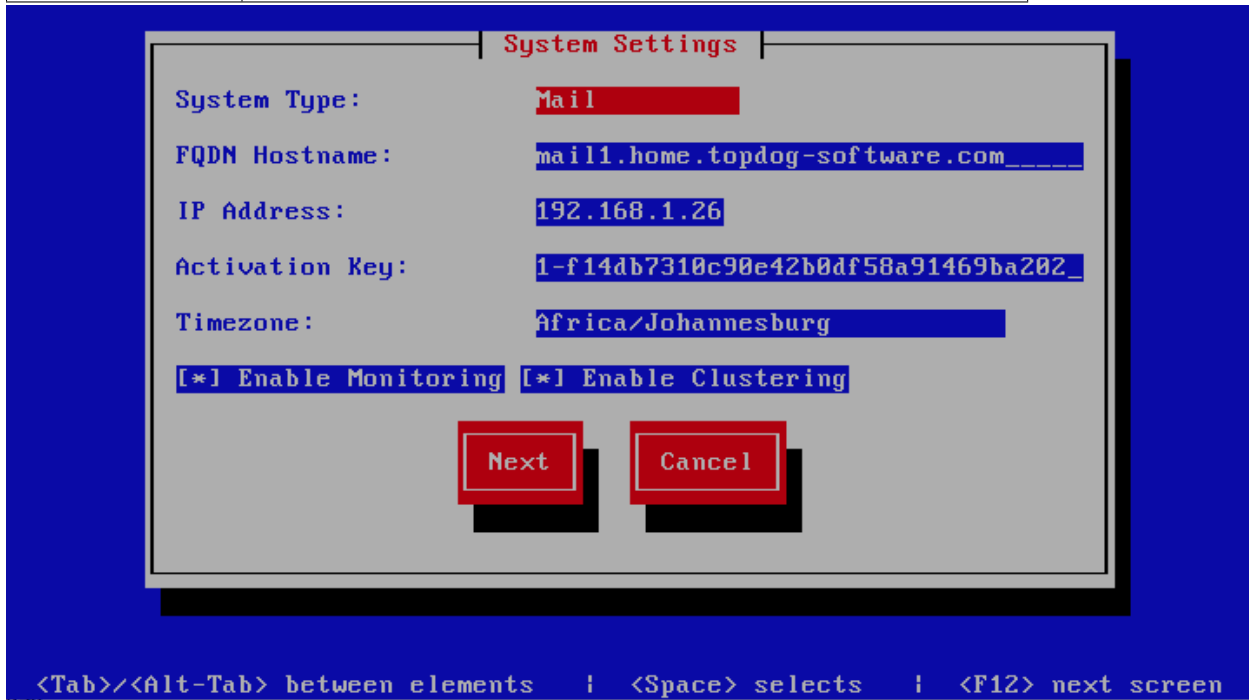
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

## System Settings

This screen configures the basic system settings. The description of the options is as follows:

Option	Description
System Type	Set this to Mail
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check this
Enable Monitoring	Check this to enable the NRPE service

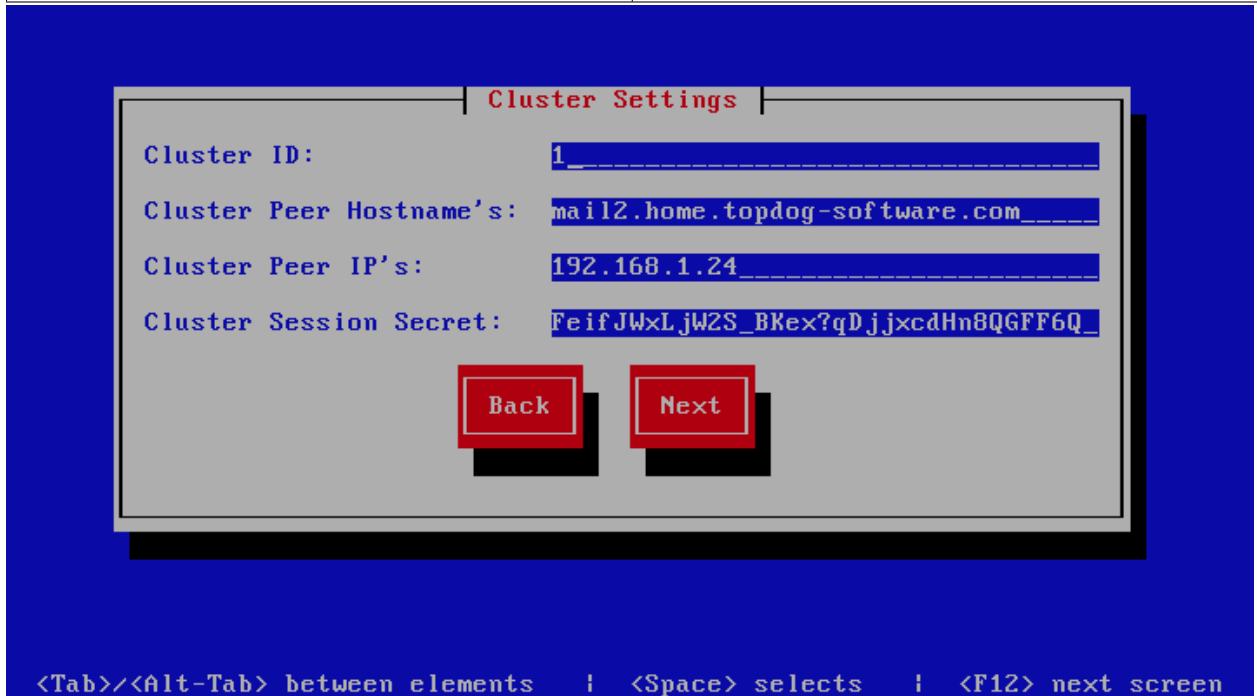


## Cluster Settings

This screen configures the cluster settings. The description of the options is as follows:



Option	Description
Cluster ID	An integer number unique to each node
Cluster Peer Hostname's	A space separated list of this nodes peers
Cluster Peer IP's	A space separated list of this nodes peers
Cluster Session Secret	This is used to encrypt session information a long password string over 35 characters, the same value should be used on all the cluster members. You can use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate it



### Scanner Settings

This screen sets the email scanner settings, The description of the options is as follows:

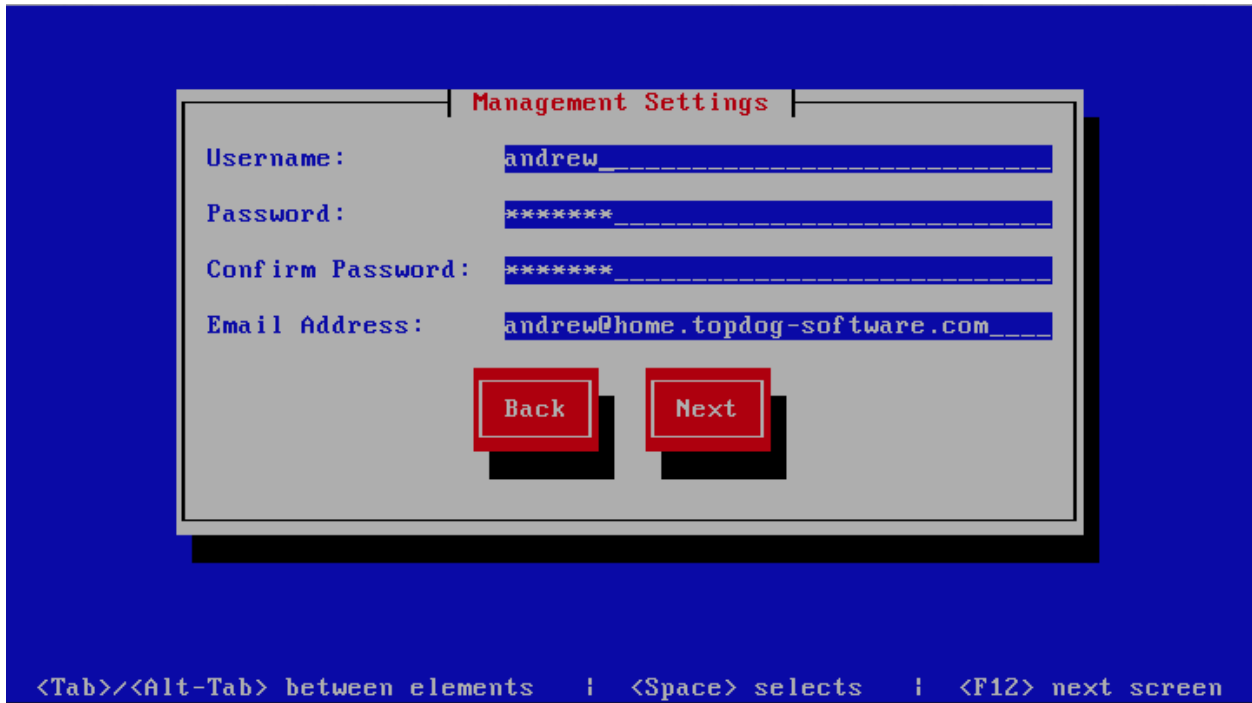
Option	Description
Organization name	Enter a short identifying name for your organisation this is used to make the X-Baruwa headers unique for your organisation Multiple servers within one site should use an identical value here. It must not contain any spaces.
Organization full name	Enter the full name of your organisation, this is used in the signature placed at the bottom of report messages sent by Baruwa. It can include pretty much any text you like. You can make the result span several lines by including “n” sequences in the text. These will be replaced by line-breaks.
Use Shared Quarantine	Check this only if you have setup a shared filesystem for the mail quarantine and configured the server to mount the <code>/var/spool/MailScanner/quarantine</code> directory to it
Store clean mail	Check this if you want to store messages not tagged as SPAM, Use this option only if it is legal in your country



## Management Settings

The screen sets the management account settings, The description of the options is as follows:

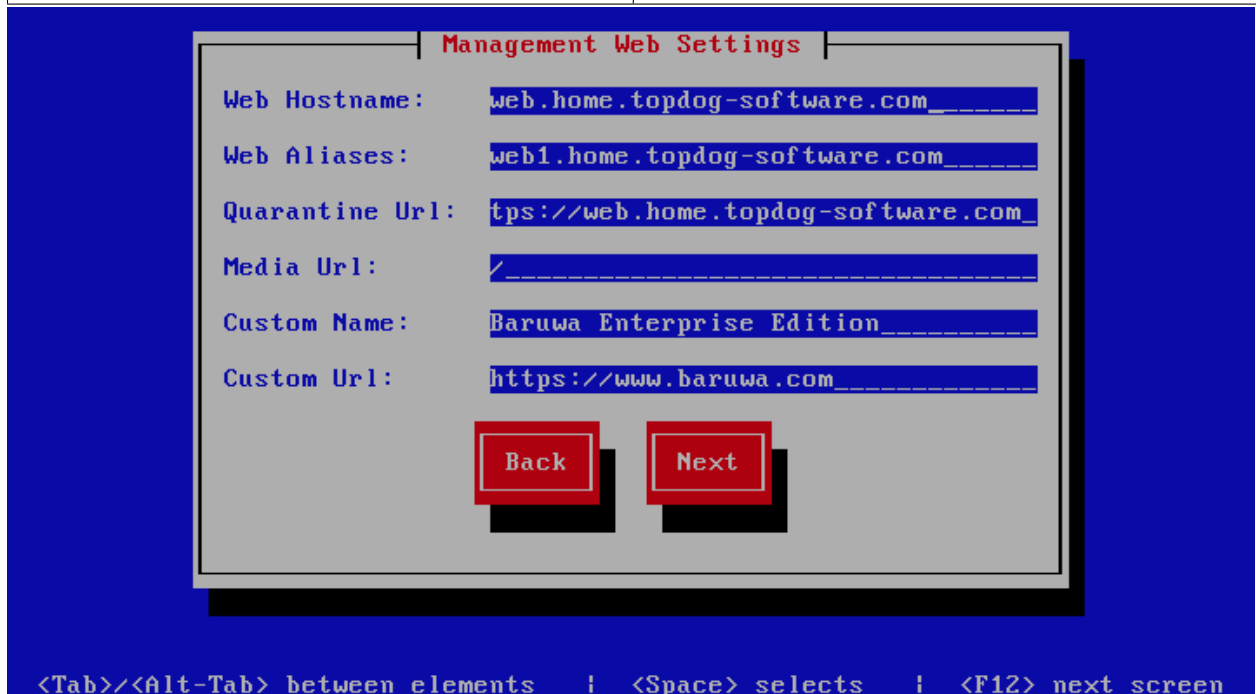
Option	Description
Username	Administrator username
Password	Administrator password, Only strong passwords will be accepted use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address



### Management Web Settings

The screen sets the management web interface settings, The description of the options is as follows:

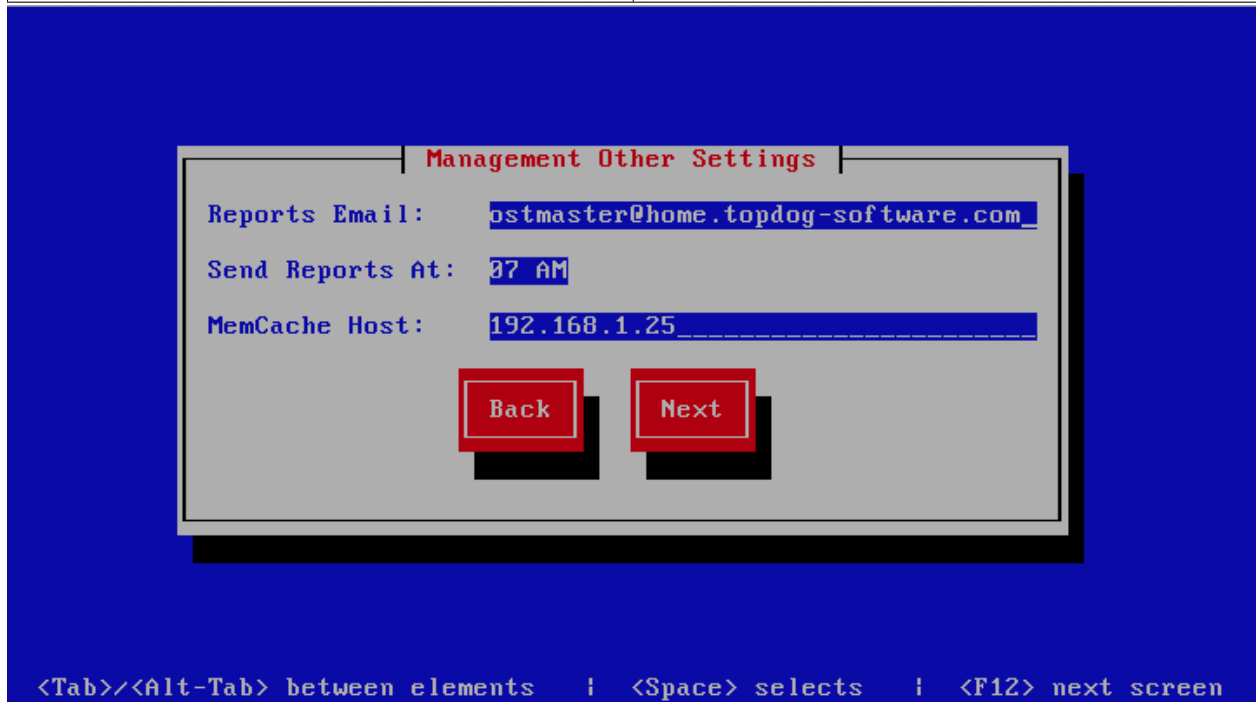
Option	Description
Web Hostname	The hostname to be used to access the web interface
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the web interface as well.
Custom URL	This creates links to your product page within the web interface and email reports that are sent out.



### Management Other Settings

The screen sets other management settings, The description of the options is as follows:

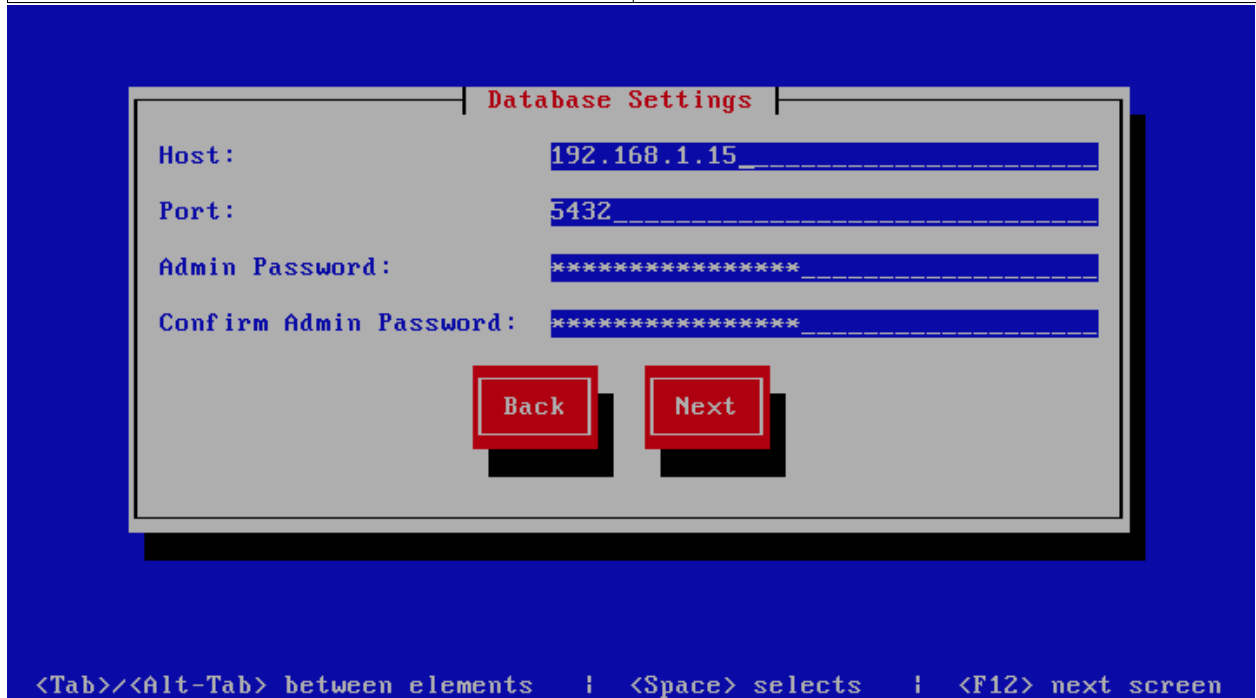
Option	Description
Reports Email	The email address used to send out email reports
Send Reports At	The hour at which to send reports, this is localized to the users location based on their timezone setting
MemCache Host	The IP address of the Memcache Server



### Database Settings

The screen sets database settings, The description of the options is as follows:

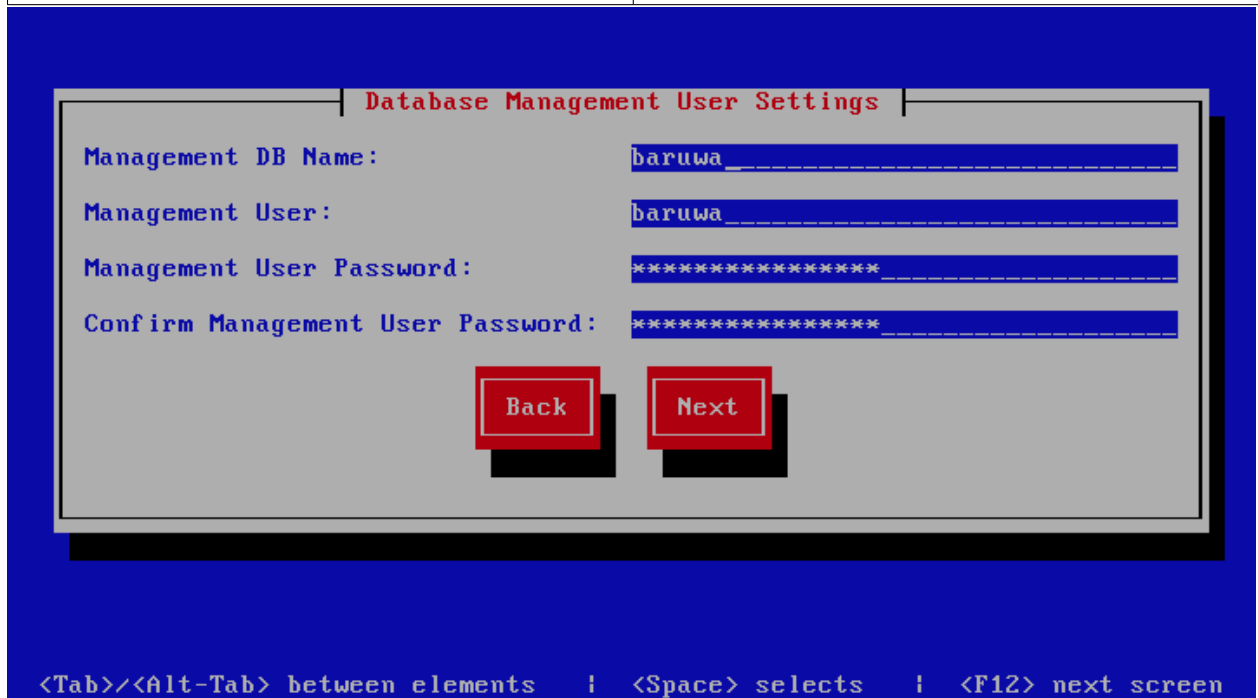
Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password



### Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:

Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password

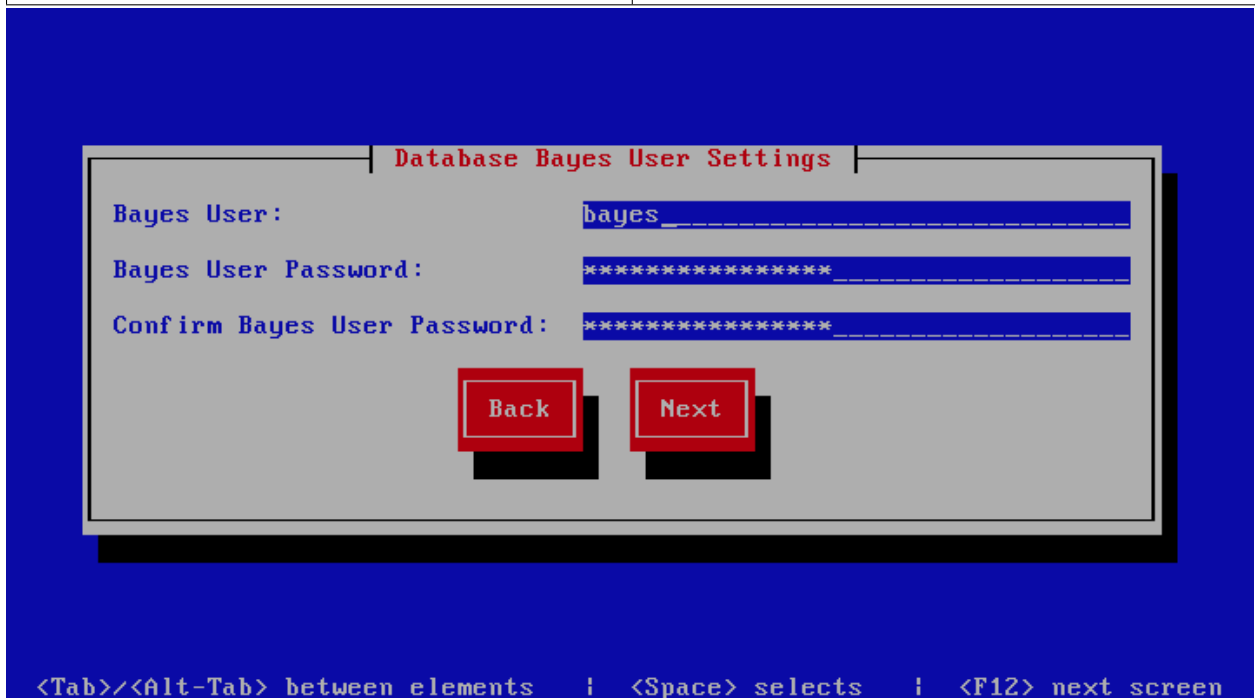


### Database Bayes User Settings

The screen sets database bayes user settings, The description of the options is as follows:



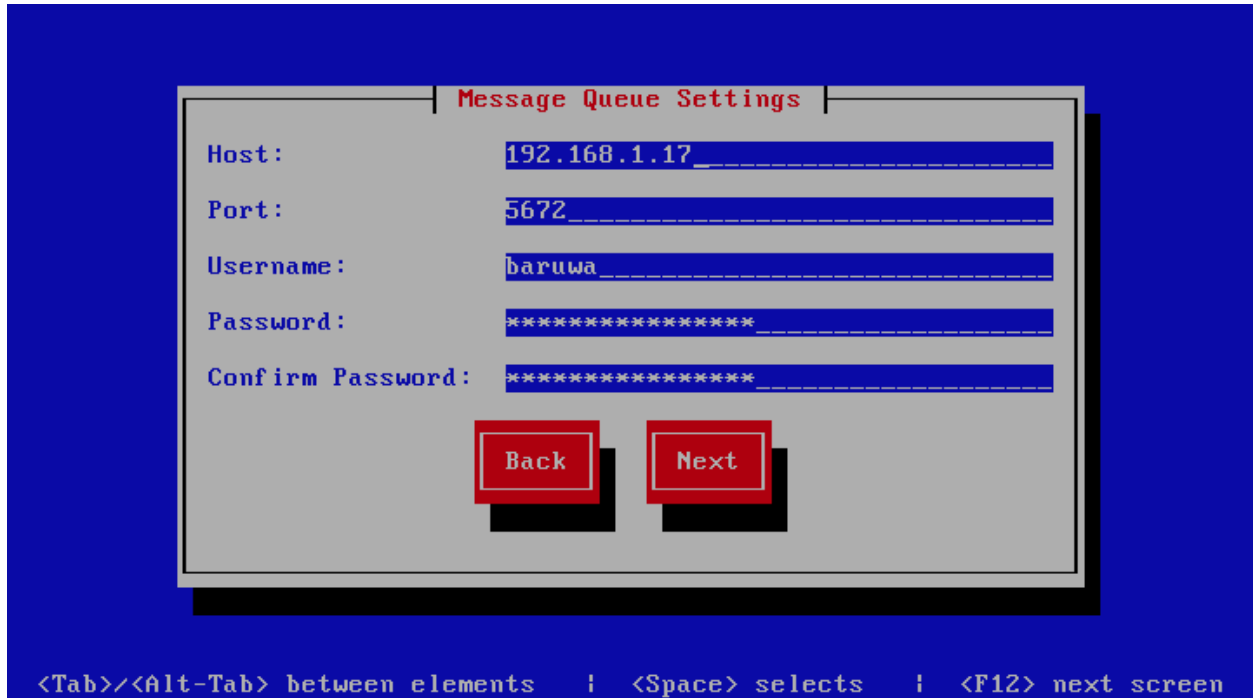
Option	Description
Bayes User	The bayes database username
Bayes User Password	The bayes database user password, Only strong passwords that do not contain the symbols ' , " , @ , # , \$ and : will be accepted.
Confirm Bayes User Password	Confirm the bayes database user password



### Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

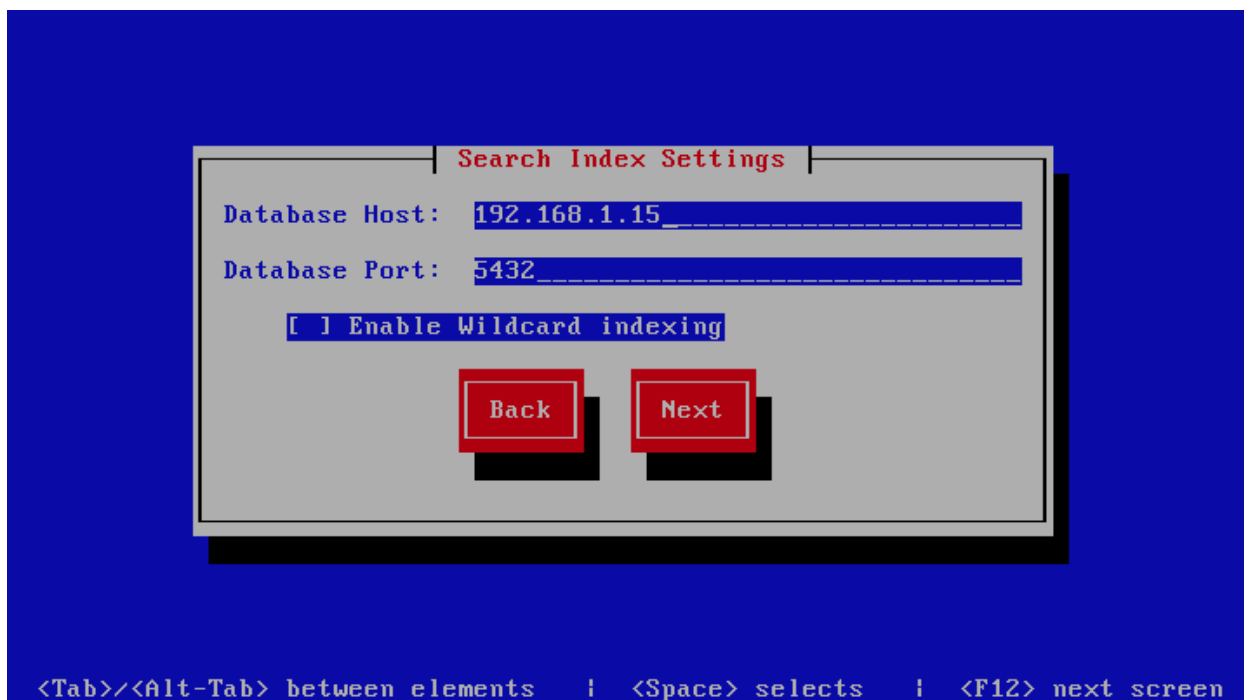
Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### Search Index Settings

The screen sets search index settings, The description of the options is as follows:

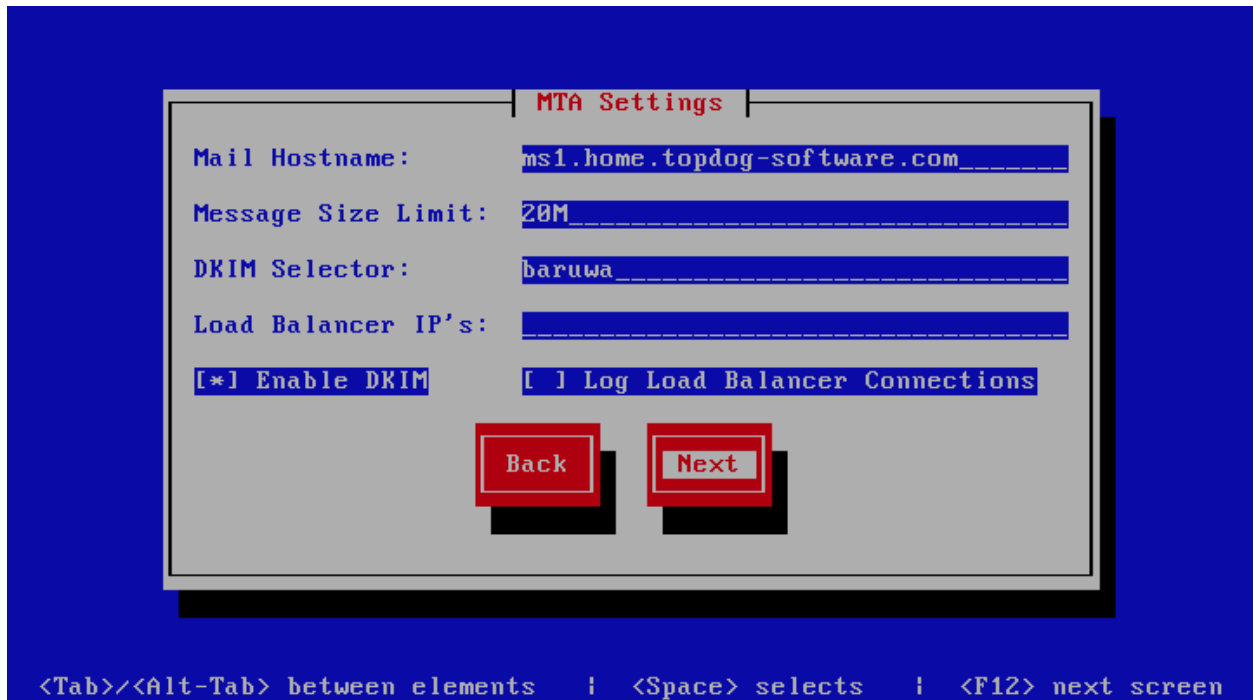
Option	Description
Database Host	Database server IP address
Database Port	Database server Port - leave as default
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



## MTA Settings

The screen sets mta settings, The description of the options is as follows:

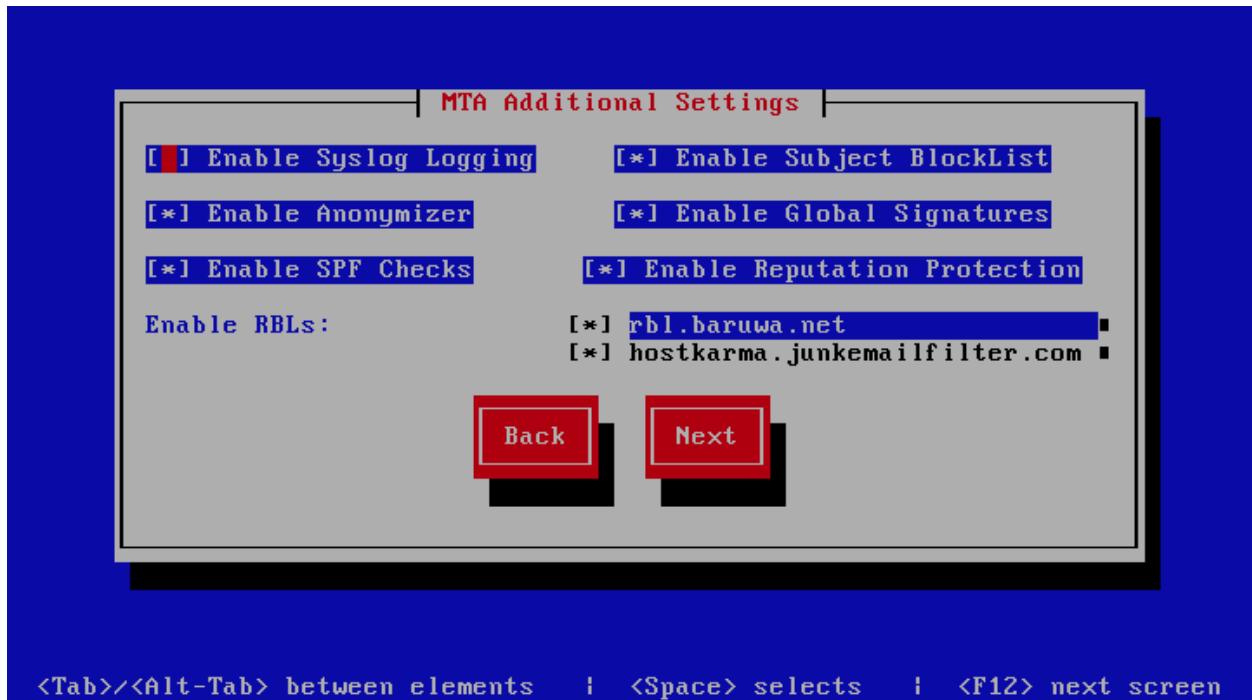
Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable DKIM	Enable DKIM functionality
Log Load Balancer Connections	Log Load Balancer connections to the MTA log



### MTA Additional Settings

The screen sets MTA additional settings, The description of the options is as follows:

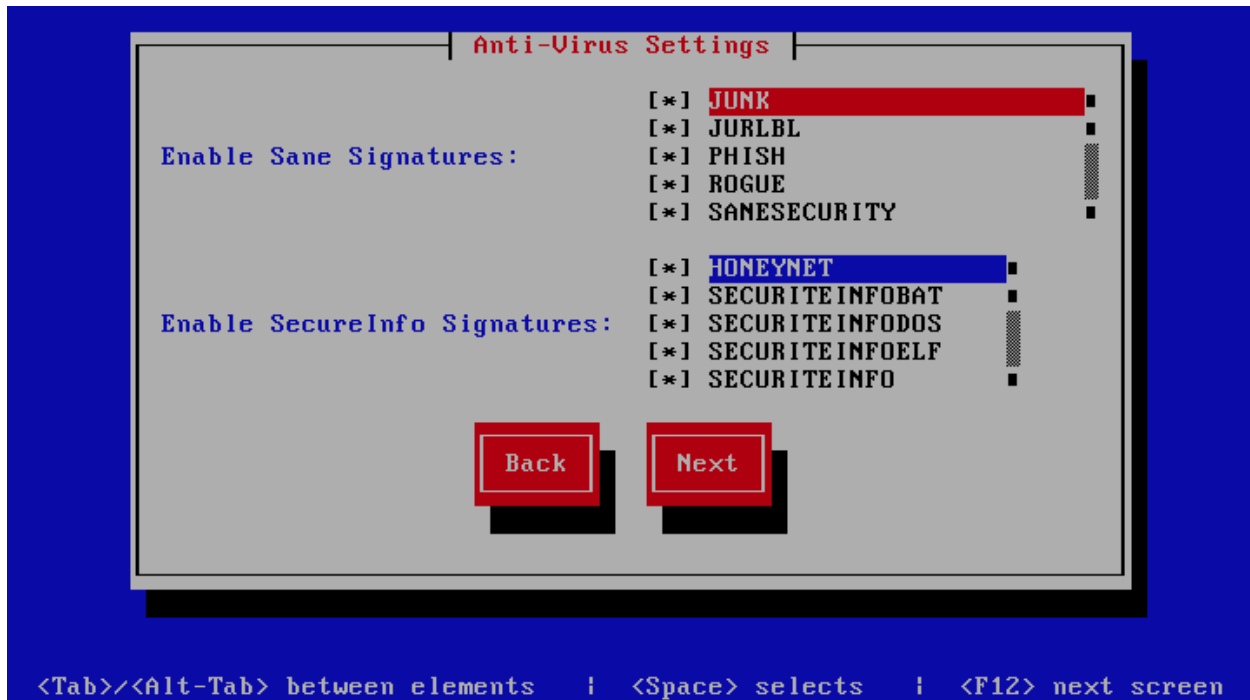
Option	Description
Enable Syslog Logging	Turns on MTA logging to syslog
Enable Subject Blocklist	Enable the blocking by subject functionality
Enable Anonymizer	Enable the Anonymizer functionality
Enable Global Signatures	Enable Global Signatures
Enable SPF Checks	Enable SPF checking functionality
Enable Reputation Protection	Enables functionality to block abusive outbound SMTP requests
Enable RBLs	Select the SMTP time DNSBL's to enable



### Anti Virus Settings

The screen sets anti virus settings, The description of the options is as follows:

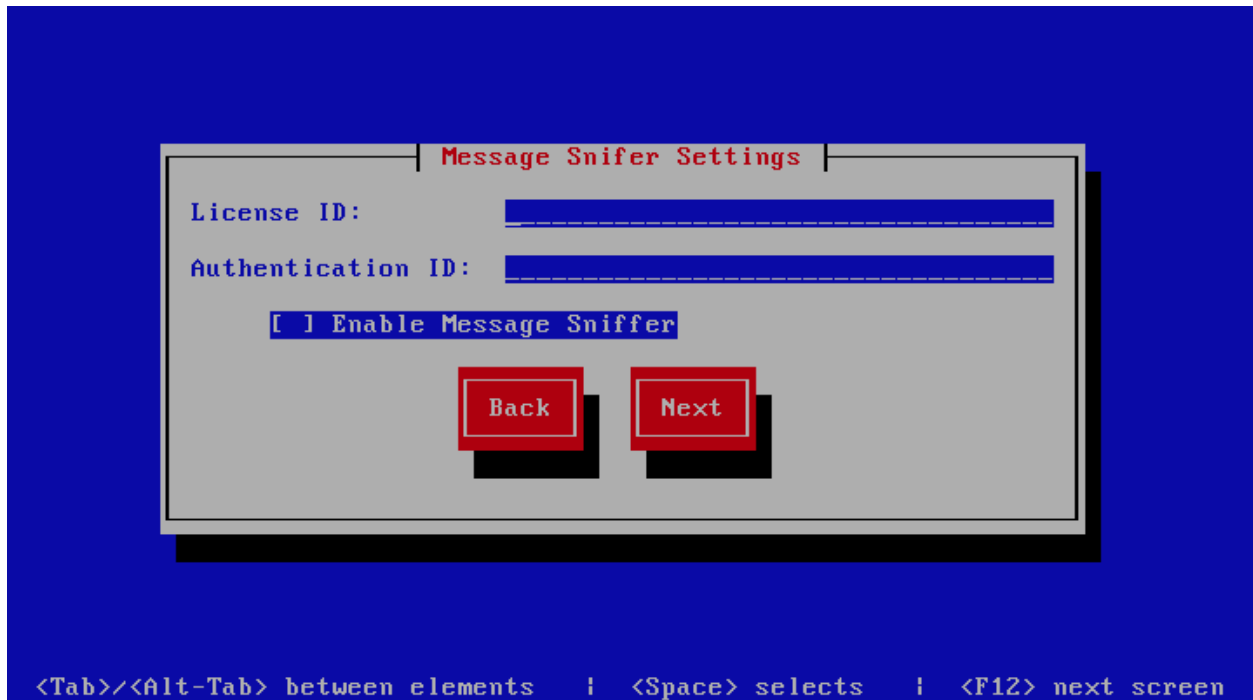
Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Enable SecureInfo Signatures	ClamAV Unofficial SecureInfo signatures to enable



### Message Sniffer Settings

The screen sets message sniffer settings, The description of the options is as follows:

Option	Description
License ID	Message Sniffer License ID This is emailed to you when you purchase a subscription
Authentication ID	Message Sniffer Authentication ID This is emailed to you when you purchase a subscription



## SSL/TLS Settings

The Baruwa web interface MUST run over SSL/TLS, other services such as SMTP AUTH only work over SSL/TLS as well. So you need to either purchase a valid SSL certificate or have `baruwa-setup` automatically generate one non recognised SSL certificate for you. If you do not have a CA issued certificate and do not intend on purchasing one the leave the `I have a CA issued Certificate` unchecked.

The certificate that `baruwa-setup` generates will cover the web hostname, web aliases, cluster members and the mail hostname. This means that you should copy this certificate to other cluster hosts that you specified and select `I have a CA issued Certificate` on those hosts when you set them up instead of generating new certificates for them.

---

**Note:** We have partnered with the SSLShop to bring you discounted SSL certificate pricing. RapidSSL CA signed certificates can be purchased at discounted pricing using the Discount coupon “BARUWA” from <http://www.sslshop.co.za>

---

If you have a SSL certificate that is issued by a recognised CA and would like Baruwa to use it, install it prior to running `baruwa-setup`. Please NOTE that you need certificates that cover the web hostname and aliases, and the mail hostname. Please check `I have a CA issued Certificate`.

The preferred location to install certificates and keys on the server is under `/etc/pki`. You need to create a directory structure under that and store your certificate under it.

The following example creates a baruwa directory under `/etc/pki` and stores the certificates and keys there:

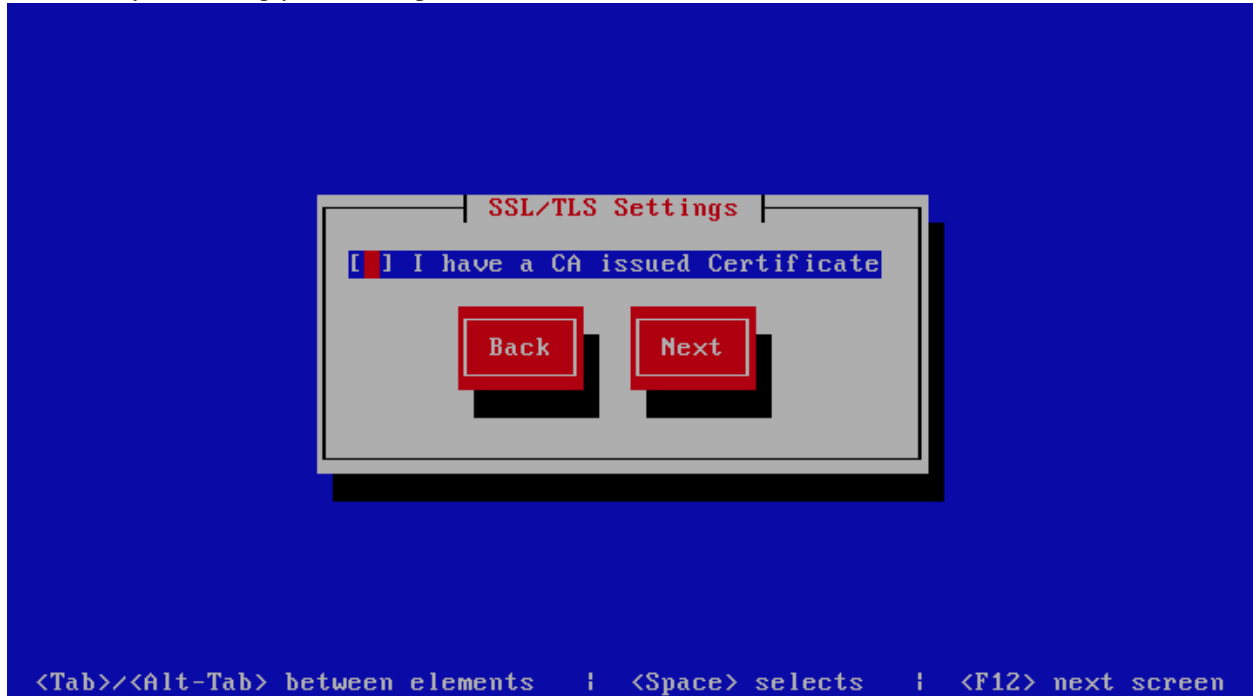
```
mkdir -p /etc/pki/baruwa/{certs,private}
```

Create the following files

- `/etc/pki/baruwa/certs/baruwa.pem` with the contents of your SSL certificate
- `/etc/pki/baruwa/private/baruwa.key` with the contents of your SSL private key

You need to create additional certificate pairs if your web hostname and mail hostname are not the same.

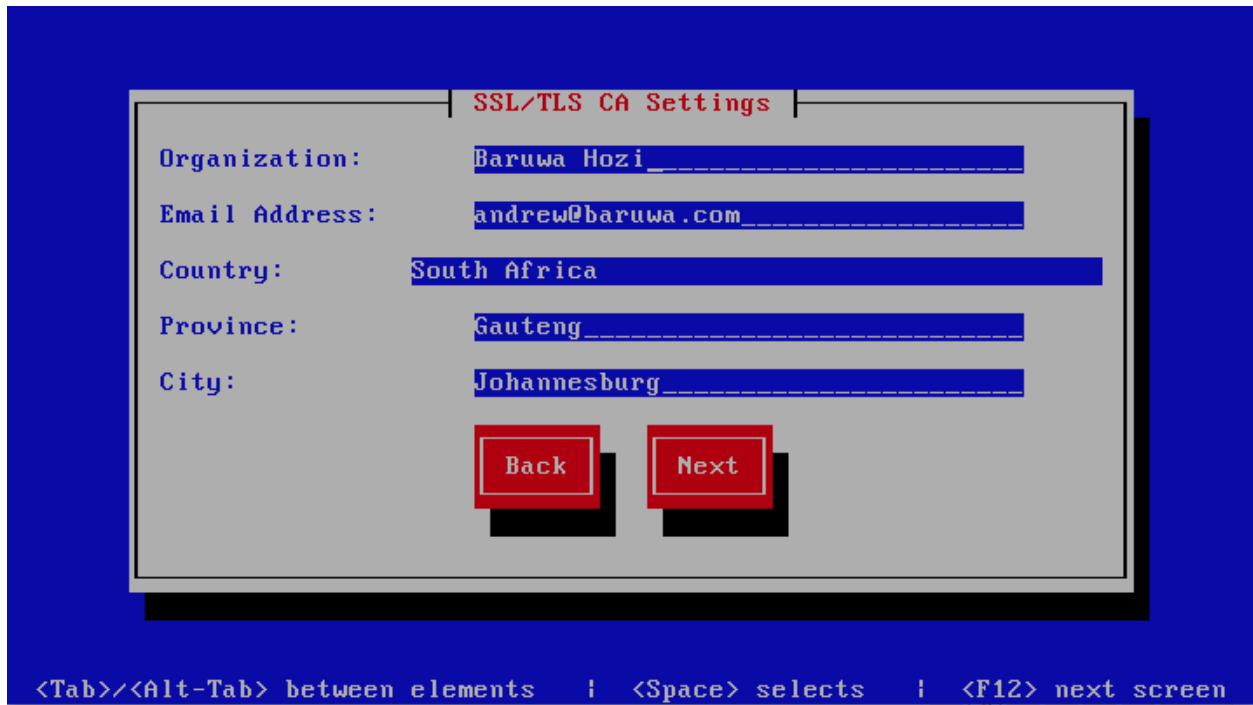
If you have a wildcard certificate with all your names being subdomains of that domain to which the certificate is issued then you can simply create one pair.



If you left I have a CA issued Certificate unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

Option	Description
Organization	OpenSSL CA Name
Email Address	OpenSSL email address
Country	OpenSSL country code
Province	OpenSSL province
City	OpenSSL city

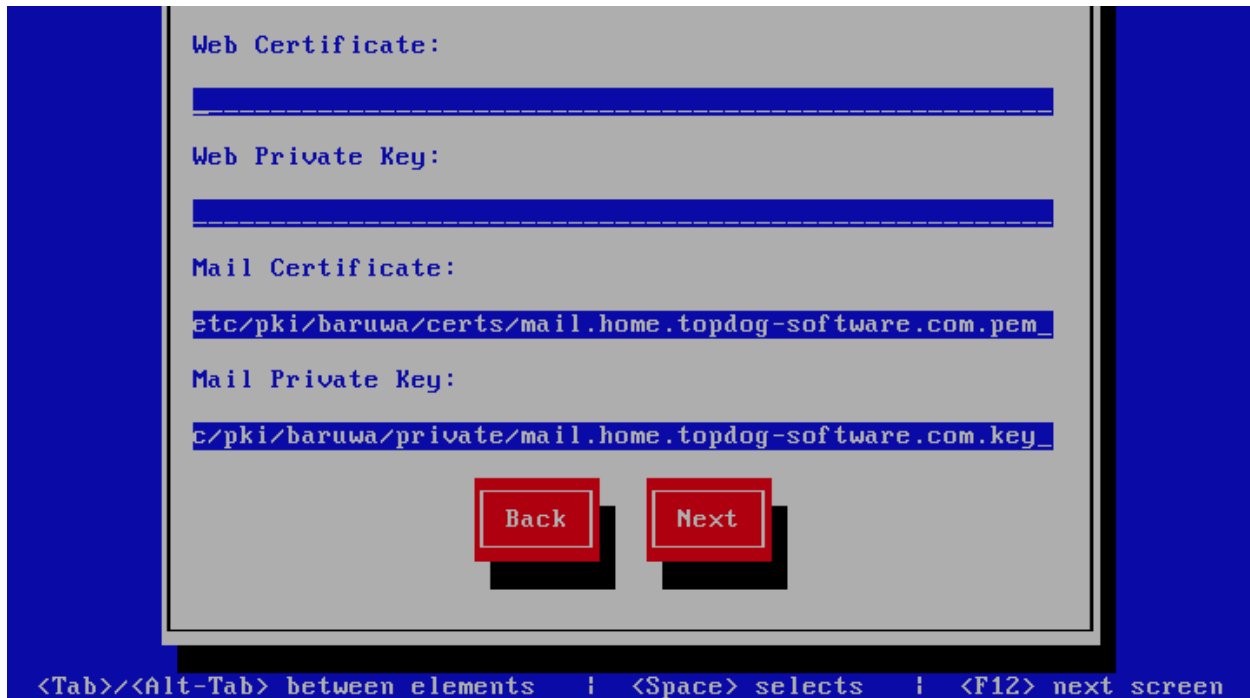




**Note:** You do not have to specify a web certificate and key pair for this profile

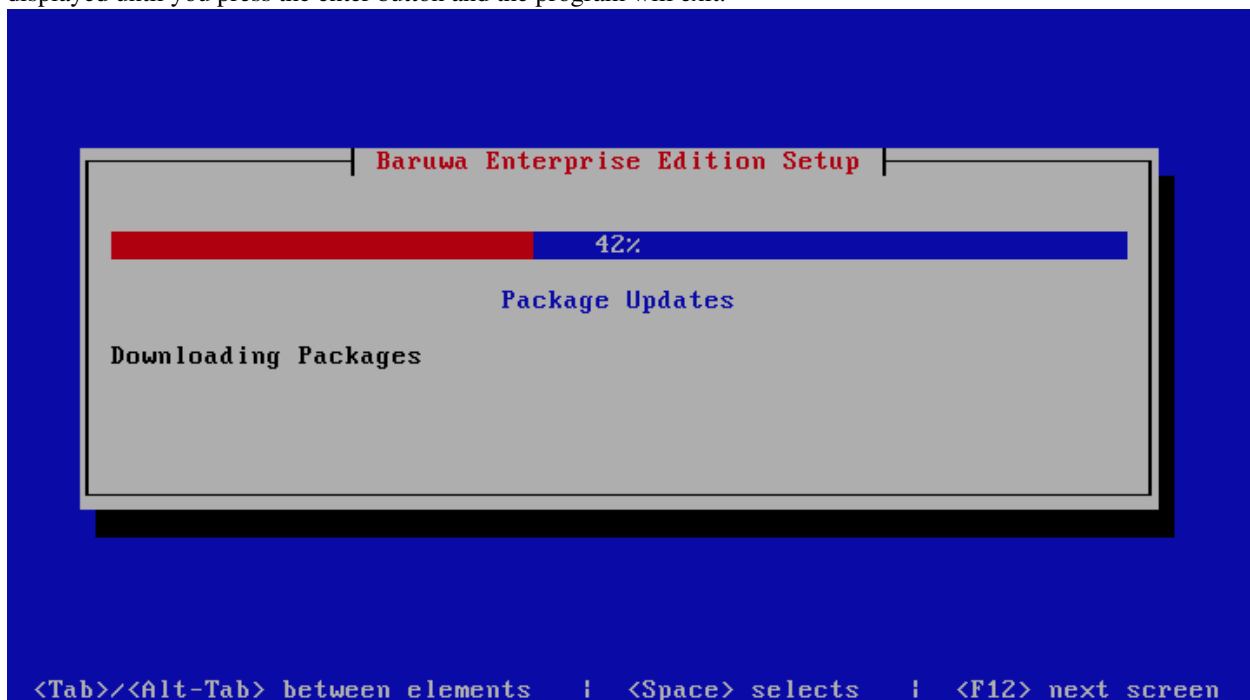
If you checked I have a CA issued Certificate you will be presented with the following screen, you need to specify the locations of your certificates and keys. The description of the options is as follows:

Option	Description
Web Certificate	The location of the web certificate file in PEM format
Web Private Key	The location of the web private key file in PEM format
Mail Certificate	The location of the mail certificate file in PEM format
Mail Private Key	The location of the mail private key file in PEM format



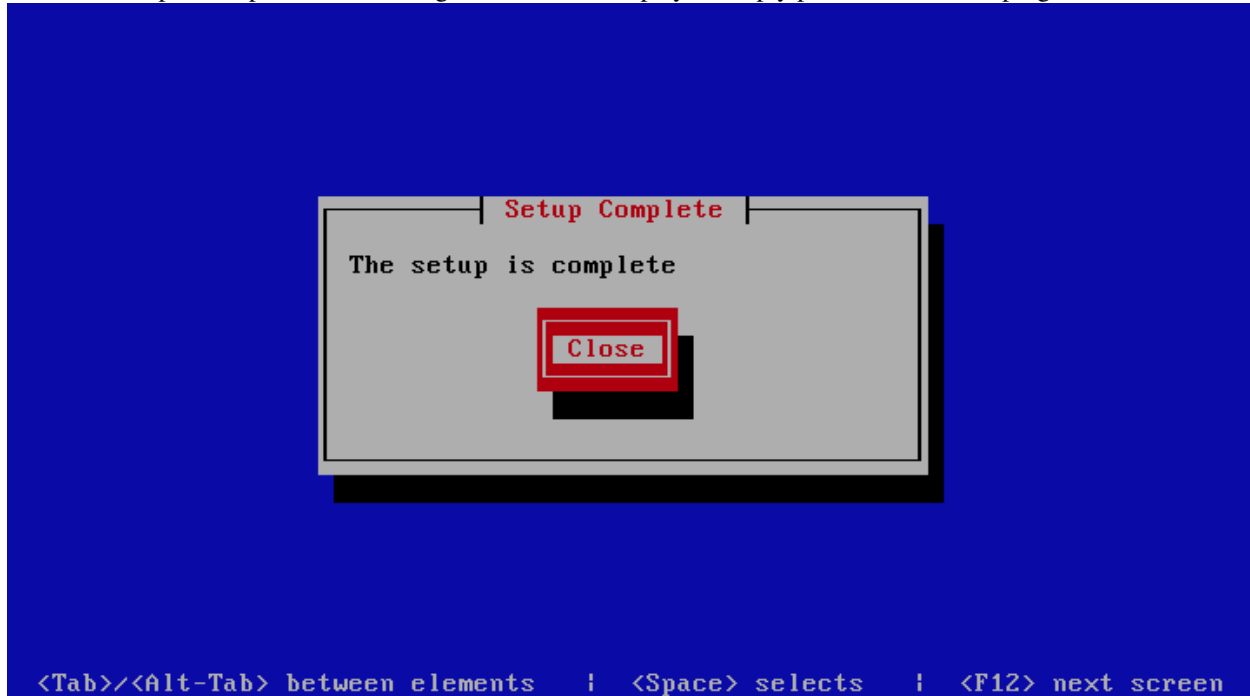
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.8 Web Interface System

This is a front-end system that is dedicated to providing web interface access for administration as well as user access. You setup this kind of system if you want dedicated servers providing only web access. You can have several of these nodes scaling up or down as demand grows or drops.

### 7.8.1 Automated Configuration

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

To start the configuration process login to the server with the username `root` and the password you set during installation.

Issue the `baruwa-setup` command at the command prompt:

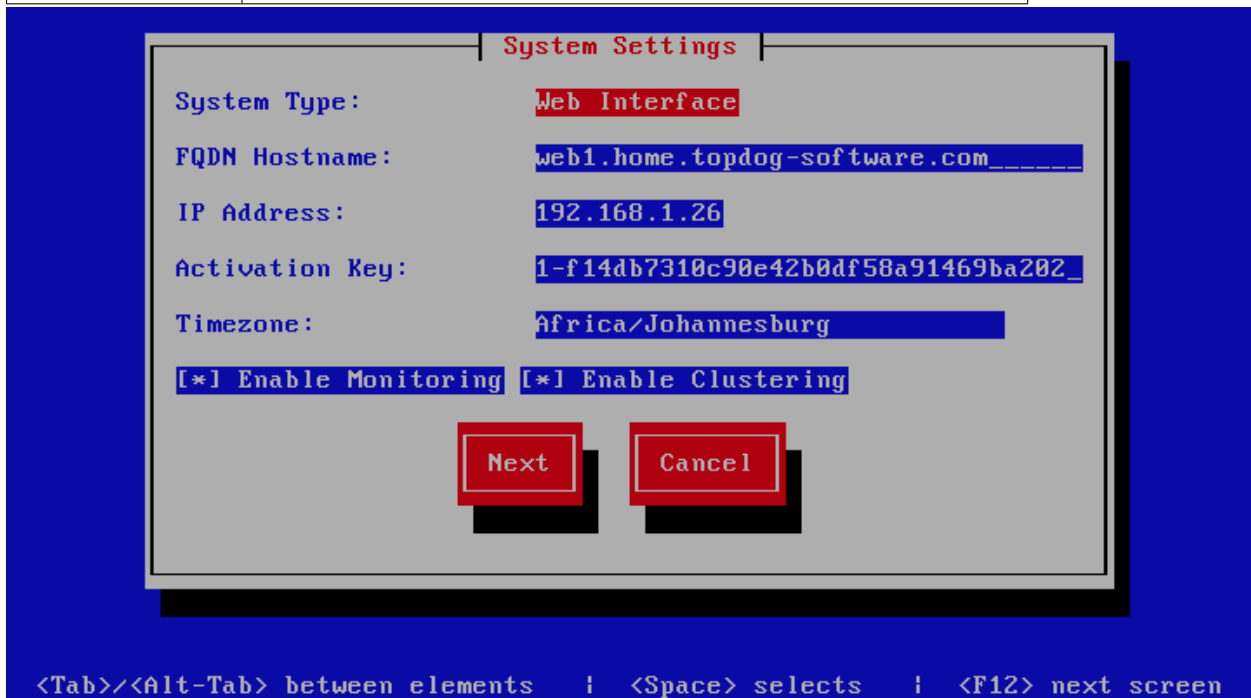
```
# baruwa-setup
```

The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

### System Settings

This screen configures the basic system settings. The description of the options is as follows:

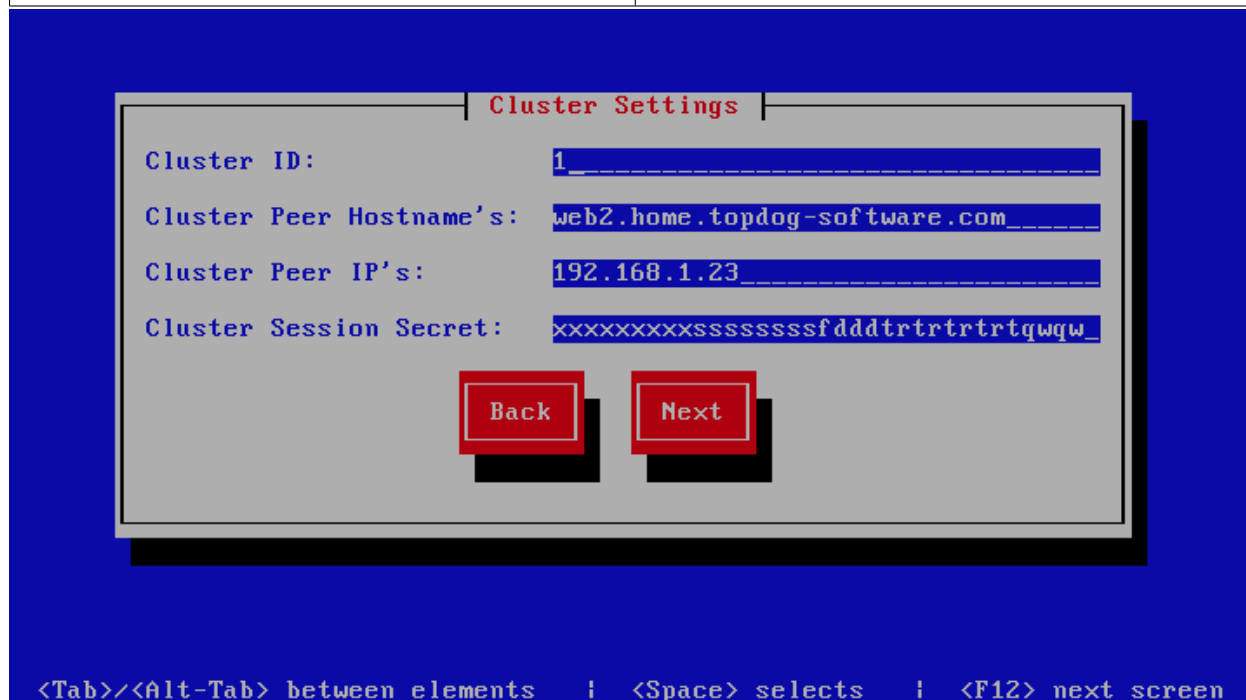
Option	Description
System Type	Set this to Web Interface
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check this
Enable Monitoring	Check this to enable the NRPE service



### Cluster Settings

This screen configures the cluster settings. The description of the options is as follows:

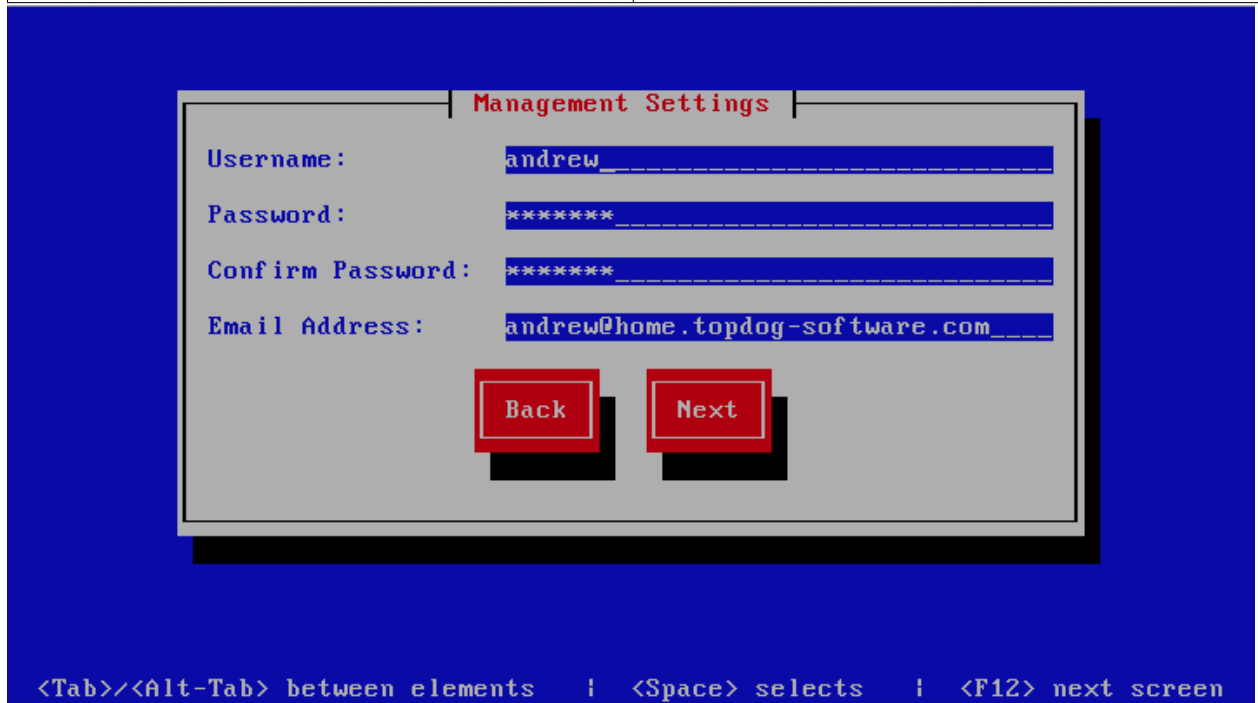
Option	Description
Cluster ID	An integer number unique to each node
Cluster Peer Hostname's	A space separated list of this nodes peers
Cluster Peer IP's	A space separated list of this nodes peers
Cluster Session Secret	This is used to encrypt session information a long password string over 35 characters, the same value should be used on all the cluster members. You can use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate it



## Management Settings

The screen sets the management account settings, The description of the options is as follows:

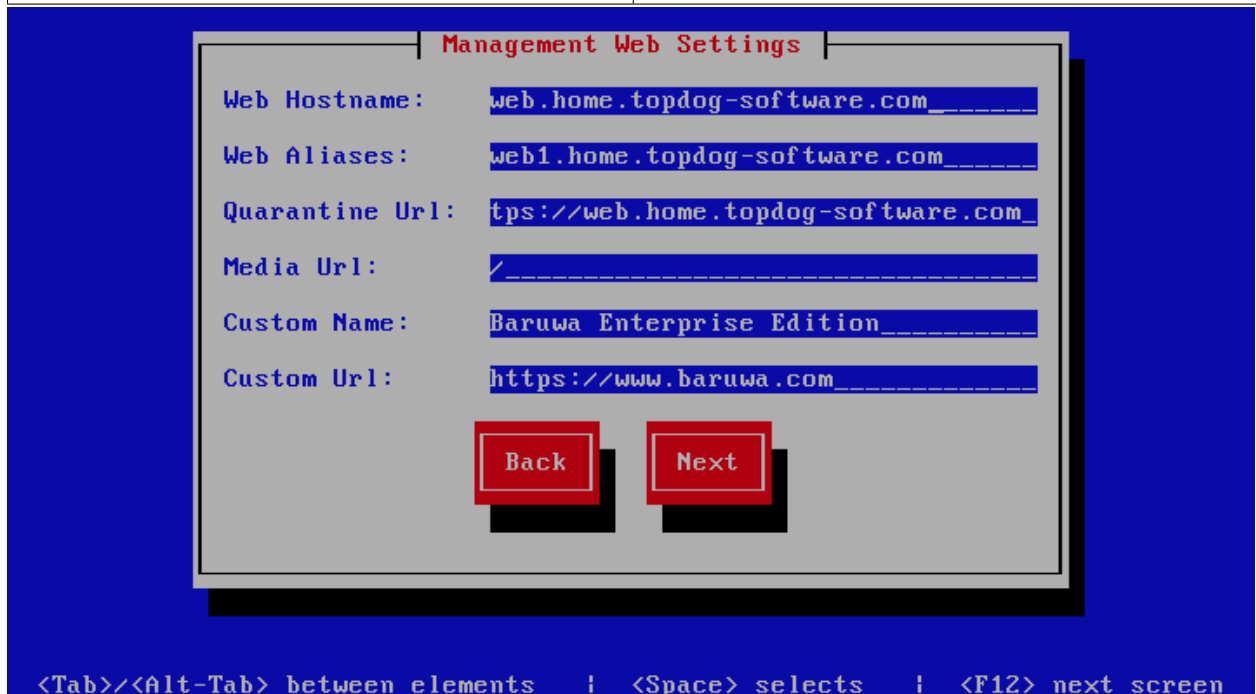
Option	Description
Username	Administrator username
Password	Administrator password, Only strong passwords will be accepted use a service such as <a href="http://passwordsgenerator.net">passwordsgenerator.net</a> to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address



### Management Web Settings

The screen sets the management web interface settings, The description of the options is as follows:

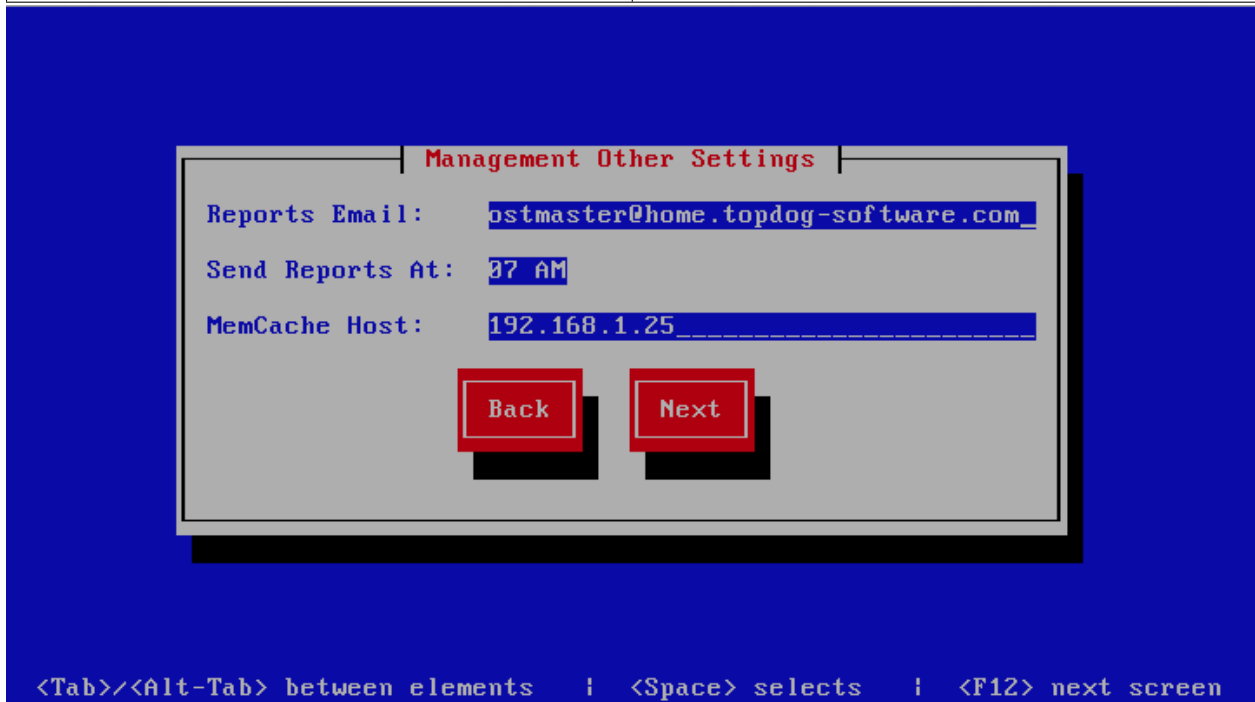
Option	Description
Web Hostname	The hostname to be used to access the web interface
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the web interface as well.
Custom URL	This creates links to your product page within the web interface and email reports that are sent out.



### Management Other Settings

The screen sets other management settings, The description of the options is as follows:

Option	Description
Reports Email	The email address used to send out email reports
Send Reports At	The hour at which to send reports, this is localized to the users location based on their timezone setting
MemCache Host	The IP address of the Memcache Server

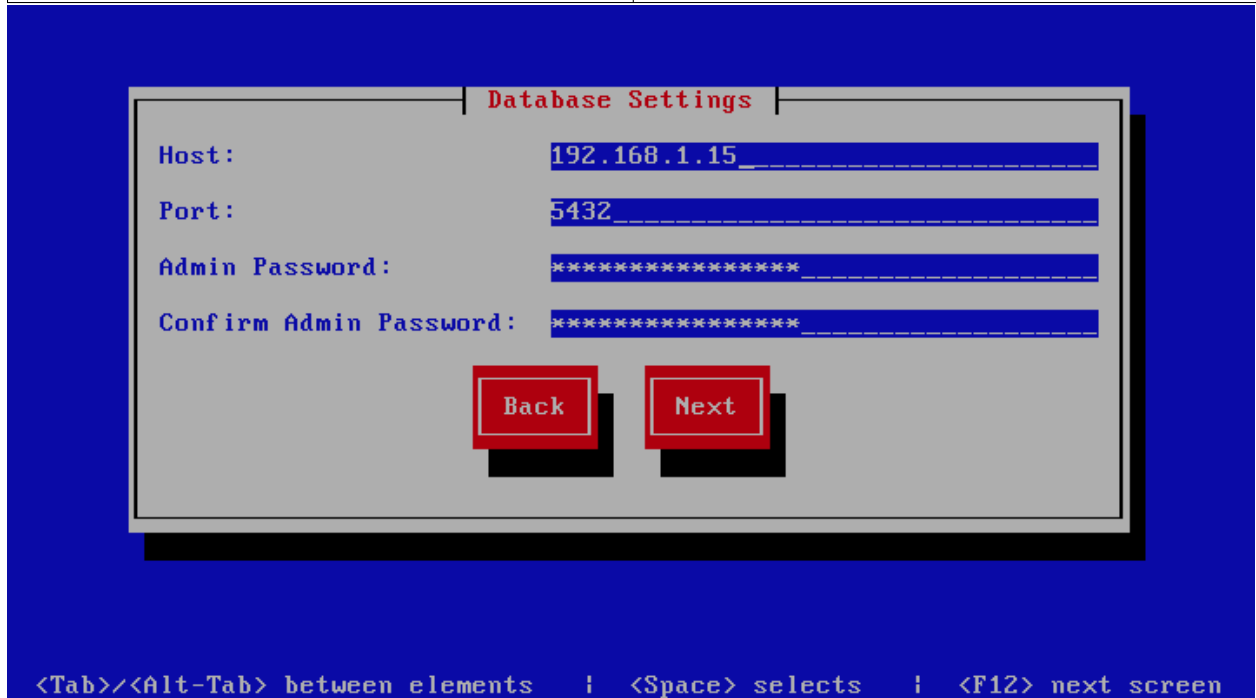


### Database Settings

The screen sets database settings, The description of the options is as follows:



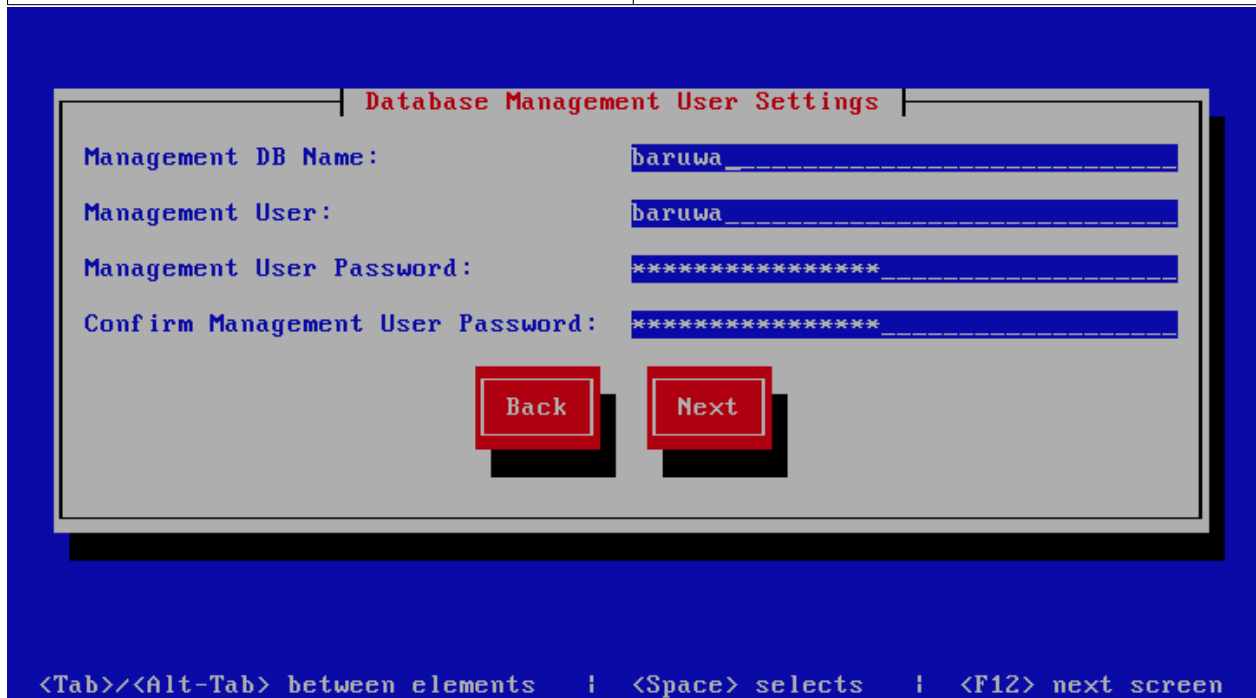
Option	Description
Host	The database server IP Address
Port	The database port
Admin Password	The database admin user password, Only strong passwords that do not contain the symbols ' , " , @ , \$ , # and : will be accepted.
Confirm Admin Password	Confirm the database admin user password



### Database Management User Settings

The screen sets database management user settings, The description of the options is as follows:

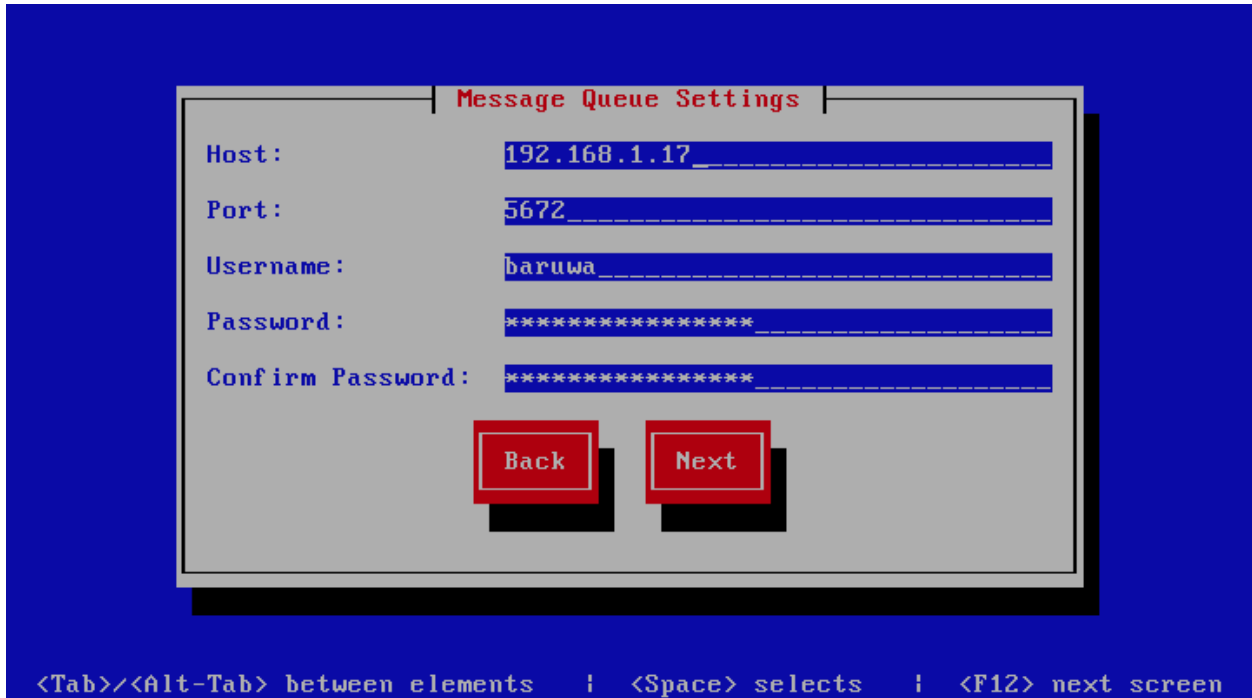
Option	Description
Management DB Name	The name of the management database
Management User	The management database username
Management User Password	The management database user password, Only strong passwords that do not contain the symbols ' , ", @, #, \$ and : will be accepted.
Confirm Management User Pass	Confirm the management database user password



### Message Queue Settings

The screen sets message queue settings, The description of the options is as follows:

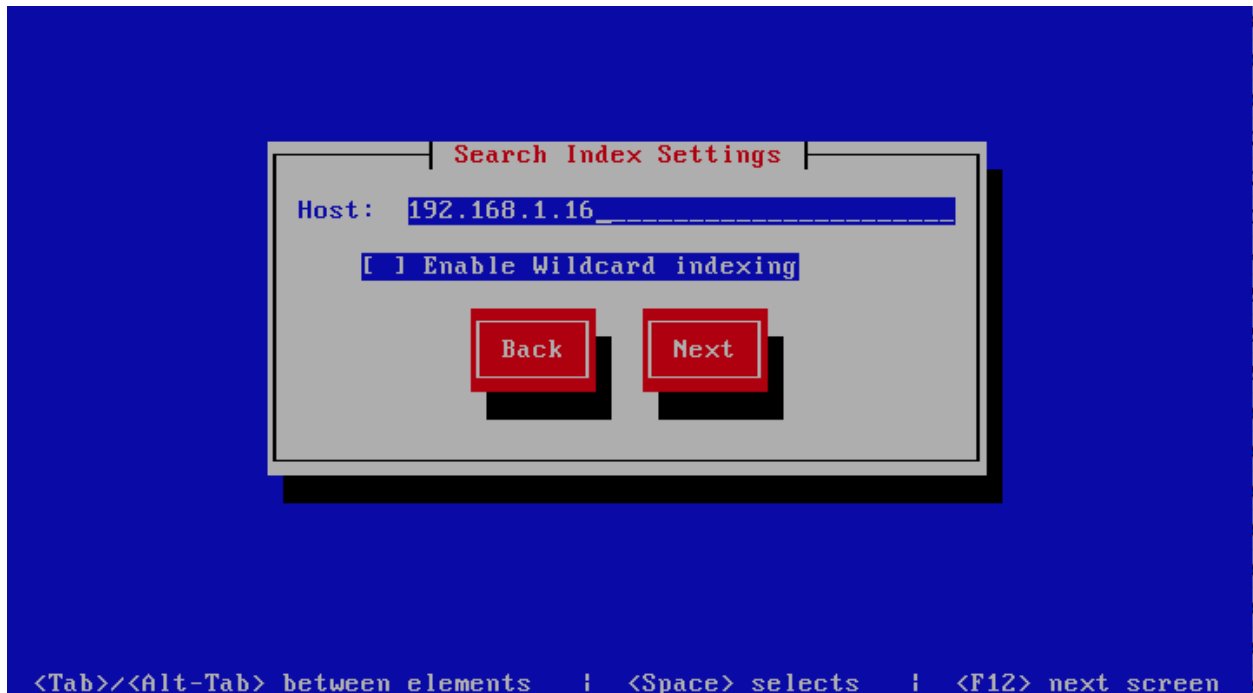
Option	Description
Host	The message queue server IP address
Port	The message queue server port
Username	The message queue server username
Password	The message queue server password
Confirm Password	Confirm the message queue server password



### Search Index Settings

The screen sets search index settings, The description of the options is as follows:

Option	Description
Host	Indexing server IP address
Enable wildcard indexing	Enables Sphinx wildcard indexing, Setting this to true will generate very large index files.



## SSL/TLS Settings

The Baruwa web interface MUST run over SSL/TLS, other services such as SMTP AUTH only work over SSL/TLS as well. So you need to either purchase a valid SSL certificate or have `baruwa-setup` automatically generate one non recognised SSL certificate for you. If you do not have a CA issued certificate and do not intend on purchasing one the leave the `I have a CA issued Certificate` unchecked.

The certificate that `baruwa-setup` generates will cover the web hostname, web aliases, cluster members and the mail hostname. This means that you should copy this certificate to other cluster hosts that you specified and select `I have a CA issued Certificate` on those hosts when you set them up instead of generating new certificates for them.

---

**Note:** We have partnered with the SSLShop to bring you discounted SSL certificate pricing. RapidSSL CA signed certificates can be purchased at discounted pricing using the Discount coupon “BARUWA” from <http://www.sslshop.co.za>

---

If you have a SSL certificate that is issued by a recognised CA and would like Baruwa to use it, install it prior to running `baruwa-setup`. Please NOTE that you need certificates that cover the web hostname and aliases, and the mail hostname. Please check `I have a CA issued Certificate`.

The preferred location to install certificates and keys on the server is under `/etc/pki`. You need to create a directory structure under that and store your certificate under it.

The following example creates a `baruwa` directory under `/etc/pki` and stores the certificates and keys there:

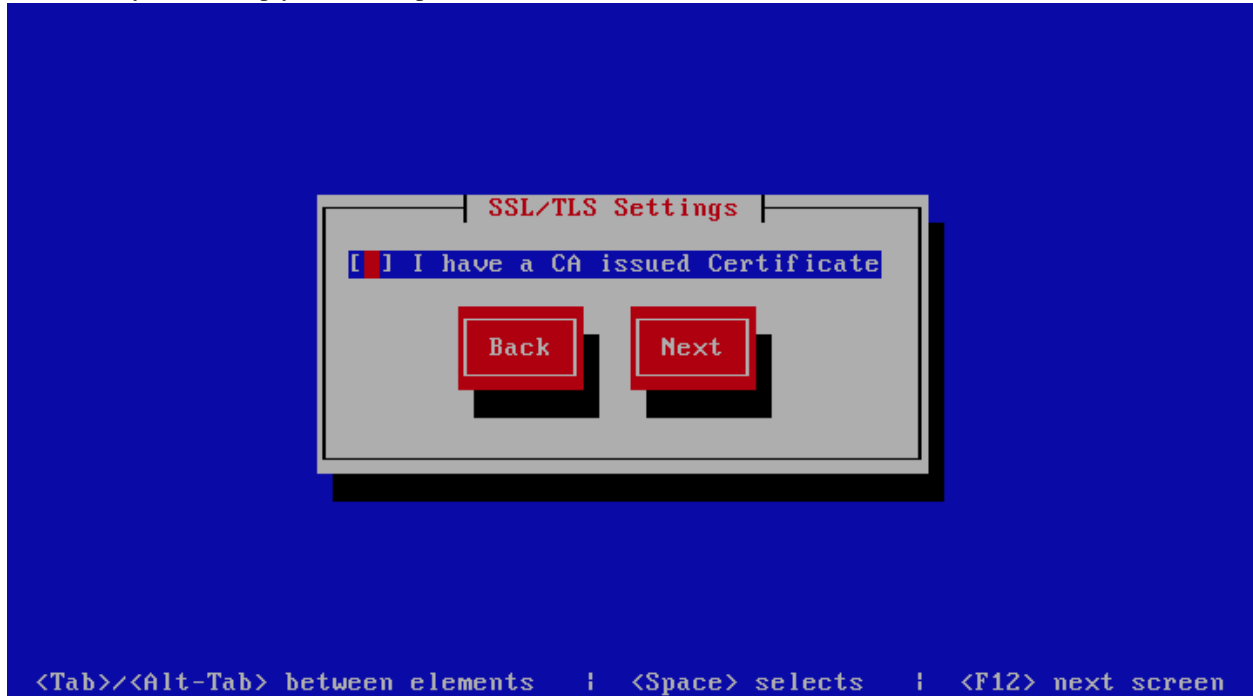
```
mkdir -p /etc/pki/baruwa/{certs,private}
```

Create the following files

- `/etc/pki/baruwa/certs/baruwa.pem` with the contents of your SSL certificate
- `/etc/pki/baruwa/private/baruwa.key` with the contents of your SSL private key

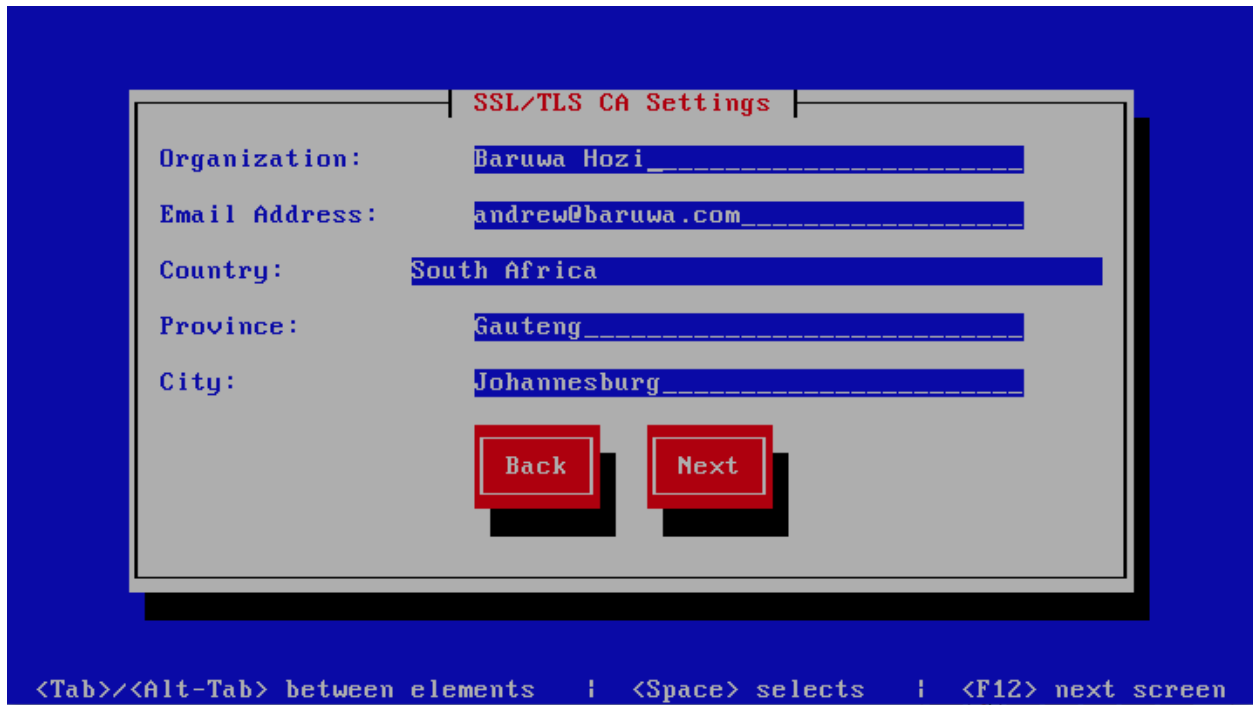
You need to create additional certificate pairs if your web hostname and mail hostname are not the same.

If you have a wildcard certificate with all your names being subdomains of that domain to which the certificate is issued then you can simply create one pair.



If you left I have a CA issued Certificate unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

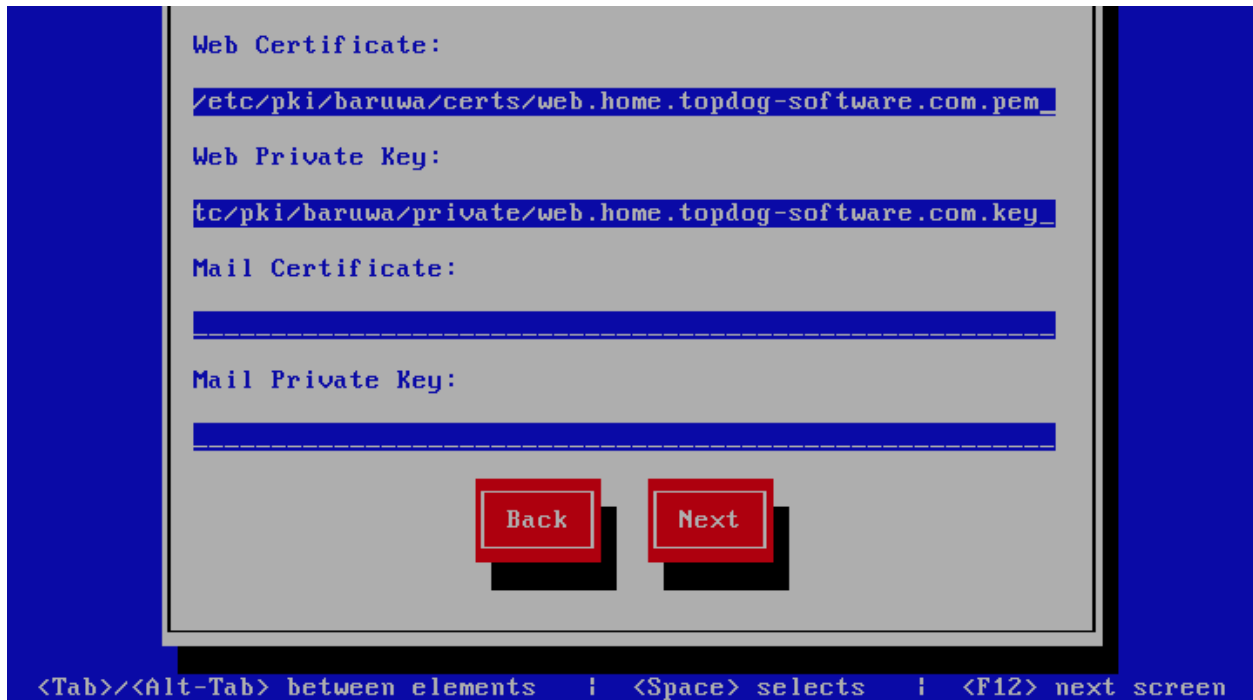
Option	Description
Organization	OpenSSL CA Name
Email Address	OpenSSL email address
Country	OpenSSL country code
Province	OpenSSL province
City	OpenSSL city



**Note:** You do not have to specify a mail certificate and key pair for this profile

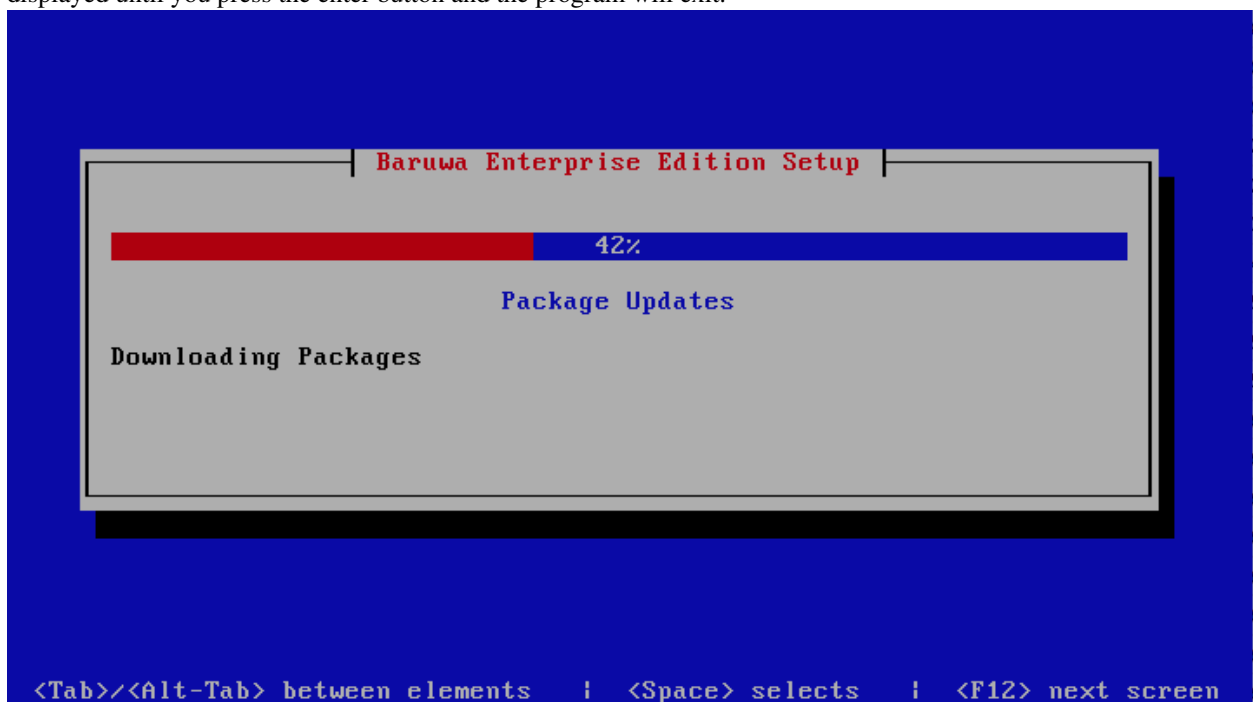
If you checked I have a CA issued Certificate you will be presented with the following screen, you need to specify the locations of your certificates and keys. The description of the options is as follows:

Option	Description
Web Certificate	The location of the web certificate file in PEM format
Web Private Key	The location of the web private key file in PEM format
Mail Certificate	The location of the mail certificate file in PEM format
Mail Private Key	The location of the mail private key file in PEM format



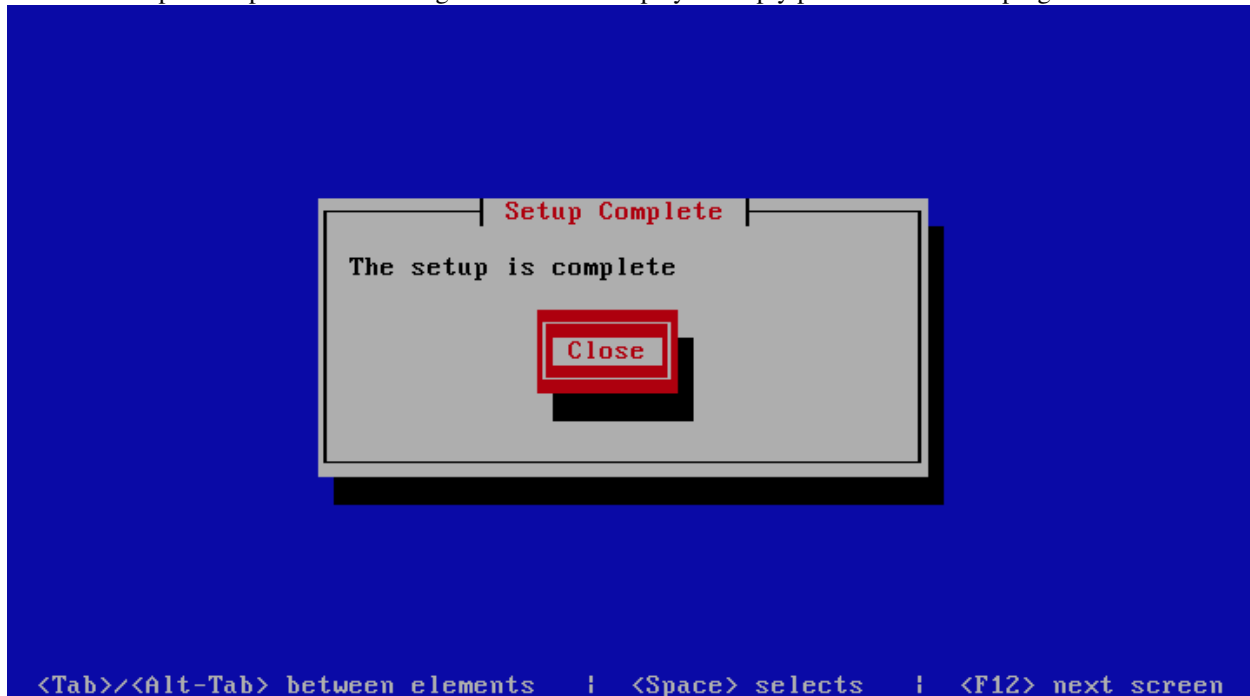
## Setup Running

At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.



## Setup Complete

When the setup is complete the following screen will be displayed simply press enter and the program will exit



## 7.8.2 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a scanning Node*, *Add an Organization*, *Adding a Domain* and *Adding an Account*. This is done through the management web interface.

The exact sequence to follow is:

- Add the Node
- Add an Organization
- Add a Domain Administrator for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add a Domain to the Organization
- Add a delivery server for the Domain
- Add any user accounts to the Domain if not using external authentication

Review the *Administrators guide* and *Advanced configuration* for other configuration and setup options available.



## ADVANCED CONFIGURATION

### 8.1 Content Protection

#### 8.1.1 Introduction

Content Protection in Baruwa is used to manage the types of email attachments that users are allowed to send and receive. It can be deployed to prevent malicious attachments from entering an organizations network or to prevent internal users for sending out organization data out of the organization network via email.

Baruwa allows you to perform certain actions based on the type or name of attachments attached to an email message that is being processed by it.

The actions that can be performed are:

- Allow - Allows the message through
- Deny - Denies the message
- Deny and Delete - Deletes the attachment from the message
- Email to addresses - Redirects the email to the specified addresses
- Rename - Renames the attachment to name.disarmed
- Rename To - Renames the attachment to the specified extension

The Rename and Rename To options are not available for archive attachments.

Baruwa uses policies to select messages to perform the above actions. Baruwa ships with default policies that usually work well with most setups. However in some cases users may want to customize or create their own specific policies.

#### 8.1.2 Policy Types

There are four(4) types of policies used by Baruwa:

- Archive File Name Policies - These are used to match the name of files inside archive attachments such as ZIP and TAR archives
- Archive Mime Policies - These are used to match the file type of files inside archive attachments such as ZIP and TAR archives. You can use this to identify files which have been renamed to a different extension so as to by pass filename checks. So attackers may rename executable files to different extensions to bypass checks this policy will be able to identify such files.
- File Name Policies - These are used to match files by name such as .doc
- File Mime Policies - These are used to match files by type such as executable

Policies contain rules, Rules are the actual statements used to match files. For a policy to be usable it should contain atleast one(1) enabled rule.

### 8.1.3 Creating Policies

Baruwa provides two options for creating policies:

- Clone - The policy is cloned from the built in policy. If you simply want to disable a few rules from the default policy, this is the best option to use. After cloning you can disable the rules you wish to disable then assign the policy.
- Create - This creates a blank policy to which you add rules.

After a policy has been created and customized, it is available to assign as either a global policy or as a domain policy. Global policies are the default policies that are applied to all messages that do not have a more specific domain policy. Domain policies only apply to messages addressed to or from the specific domain to which the policy is applied.

### 8.1.4 Policy Rules

Policy Rules are made up of the following parts:

- Action - Described above
- Expression - This is a regular expression used to match such as `\.ico$`
- Description - This is the message that will be logged and appear in warning messages that the email senders receive.
- Options - This part is used only by the `Email To` and `Rename To` actions. For the `Email To` action it contains a list of comma separated email addresses. For the `Rename To` actions it contains the rename to pattern.
- Enabled - This enables or disables a rule.

### 8.1.5 Configuration

The content protection system is configured using the Settings menu of the web interface. The instructions are available via [Content Protection](#)

## 8.2 External Authentication

Baruwa can be configured to authenticate to external authentication systems using authentication mechanisms such as LDAP, RADIUS, IMAP, POP3, SMTP, OAUTH. This is useful in cases where you have hundreds of users and cannot manually create all of them. The Baruwa user account will be automatically created the first time the user successfully authenticates to the external authentication system.

With LDAP authentication the users groups and email aliases will also be automatically added to the users Baruwa profile allowing them access to their aliased and group emails within Baruwa.

### 8.2.1 Supported Mechanisms

The following mechanisms are supported and can be fully configured via the web interface.

- LDAP

- RADIUS
- IMAP
- POP3
- SMTP

## 8.2.2 Configuration

Authentication mechanisms are setup on a per domain basis. The process is documented in the Domain management section of the admin guide under *Authentication Settings*

## 8.2.3 Planned Mechanisms

Future support is planned for the following

- YUBIKEY
- OAUTH

## 8.3 Clustering

### 8.3.1 Functionality available

Baruwa is capable of running in a cluster.

Full Baruwa functionality is available from any member within a Baruwa cluster and all cluster members have equal status. This allows you to provide round robin access either using *Load Balancers* or *DNS configuration*. This makes the running of a cluster totally transparent to the end users.

Cluster wide as well as node status information is visible via *Global status* and *Scanner node status*

### 8.3.2 Requirements

Baruwa stores client session information in Memcached, so all the nodes in the cluster should be configured to use the same Memcached server.

All nodes should be configured to either use a clustered MQ broker or use the same MQ broker as the other nodes. The nodes should be aware of the other nodes queues to enable them to submit tasks to those queues.

All the nodes with in a cluster should be configured to write to a single database and index data to a single or distributed sphinx server.

The full requirements are:

- Shared Memcached server
- Shared PostgreSQL server
- Shared MQ broker or clustered broker
- Shared Sphinx server or distributed sphinx servers

The recommended setup is to have Memcached, PostgreSQL, RabbitMQ, Sphinx running on a separate server. This called the *Distributed Backend Distributed Frontend* topology.

---

**Note:** If installed using the correct *System Profiles* the correct ports will be open on the host firewall. You may however wish to make the firewall more restrictive by allowing only your cluster machines to connect to the ports.

---

The firewall on the server hosting the above shared services needs to be configured to allow the following connections from the cluster nodes.

- TCP 9312, 9306 - Sphinx
- TCP 5432 - PostgreSQL or 6432 Pgouncer
- TCP 4369 - RabbitMQ EPMD
- TCP 11211 - Memcached

### 8.3.3 Shared quarantine

Since version 2.0.1 Baruwa supports shared quarantines using shared storage subsystems like NFS, GlusterFS, OCFS, etc. With a shared quarantine, message operations are still possible regardless of non availability of the node that processed the message. To use a shared quarantine you need to:

- Mount the quarantine directory `/var/spool/MailScanner/quarantine` to the shared file subsystem
- Check the `Use Shared Quarantine` checkbox of the `Scanner Setting` screen of `baruwa-setup`
- Set a unique `Cluster id` for each node in the `Cluster Settings` screen of `baruwa-setup`

### 8.3.4 Limitations

---

**Note:** This limitation is not present when using a shared quarantine.

---

Quarantines are node specific, so messages quarantined on a failed node will not be accessible until the node is restored.

### 8.3.5 Load Balancers

Baruwa Enterprise Edition can be setup to use load balancers that support the [Proxy-protocol](#), the most popular being Haproxy.

To use Baruwa Enterprise Edition SMTP servers with these load balancers you need to specify the load balancer IP addresses in the `Load Balancer IP's` field on the `MTA Settings` screen in `baruwa-setup`

A sample configuration for haproxy with both HTTP and SMTP being load balanced is below.

```
global
    log 127.0.0.1    local0
    log 127.0.0.1    local1 notice
    maxconn 4096
    chroot /var/lib/haproxy
    user haproxy
    group haproxy
    daemon

defaults
```

```
log      global
mode     http
option   httplog
option   dontlognull
option   redispatch
retries  3
maxconn  2000
timeout  connect      5000
timeout  client       50000
timeout  server       50000

listen http :80
    mode tcp
    option tcplog
    balance roundrobin
    server web1 192.168.1.20:80 check
    server web2 192.168.1.23:80 check

listen https :443
    mode tcp
    option tcplog
    balance roundrobin
    server web1 192.168.1.20:443 check
    server web2 192.168.1.23:443 check

listen smtp :25
    mode tcp
    no option http-server-close
    option tcplog
    timeout server 1m
    timeout connect 5s
    balance roundrobin
    server smtp1 192.168.1.22:25 send-proxy
    server smtp2 192.168.1.24:25 send-proxy
```

## 8.4 Themes

Themes, also known as skins, in the Baruwa Enterprise Edition are a combination of Mako Template, CSS and JS files that control the appearance of the Baruwa Web interface as well as reports and emails sent out by the system.

The theme system allows you to easily change the appearance of Baruwa, for example, to use the logo and colors of your company or institution.

There are two kinds of themes:

- Default theme
- Hostname/Domain linked themes

A `Default` theme can be used to override the built-in appearance for all hosts and domains on a server. A `Default` theme must be named `default` and only one default theme can be configured on a server.

`Hostname/Domain` Themes are linked to the hostname used to access the Baruwa server and the domain user accounts belong to, which means that you can virtual host various brands on the same server with different appearance and product name for each.

Using themes ensures that the changes you make survive upgrades as opposed to changes made to the built-in template and asset files shipped with Baruwa which get overwritten during an upgrade.

### 8.4.1 What can be customized

- Logos
- Web interface
- Emails
- Reports
- Product name
- Product url

### 8.4.2 Guidelines

Themes **MUST** retain the copyright notice at the bottom. If you would like to fully rebrand the interface please contact us to purchase a rebranding license.

---

**Note:** Themes that remove the copyright notices without a rebranding license will not render.

---

### 8.4.3 Configuration

The default configuration assumes that themes are stored under the following directory `/usr/share/baruwa/themes` with the following directory structure:

```
/templates/default/  
/templates/<hostname>/  
/templates/<domainname>/  
/assets/default/  
/assets/<hostname>/  
/assets/<domainname>/
```

Themes are configured by:

- Pointing the web server configuration for assets to the default and site's asset directory
- Setting the `baruwa.themes.base` to the directory containing the themes
- Setting the `baruwa.custom.name` to the custom product name
- Setting the `baruwa.custom.url` to the custom product web url

### 8.4.4 Creating a simple theme

To start off, you simply copy the built-in templates and assets into the a theme directory for the hostname you would like to customize for.

I will be using the hostname `spamfighter.example.com`:

```
BARUWA_PATH=$(python -c "from distutils.sysconfig import get_python_lib; print get_python_lib(1)")
mkdir -p /usr/share/baruwa/themes/assets/spamfighter.example.com/
mkdir -p /usr/share/baruwa/themes/templates/spamfighter.example.com/
cp -a $BARUWA_PATH/baruwa/templates/* /usr/share/baruwa/themes/templates/spamfighter.example.com/
cp -a $BARUWA_PATH/baruwa/public/* /usr/share/baruwa/themes/assets/spamfighter.example.com/
```

You can now modify the changes to the templates under `/usr/share/baruwa/themes/templates/spamfighter.example.com/` and the CSS, JS and image files under `/usr/share/baruwa/themes/assets/spamfighter.example.com/`

In order to brand other non web interfaces such as email you need to link the themes to the domain name you want to brand.

For example to theme the domain name `example.com`:

```
ln -s /usr/share/baruwa/themes/assets/spamfighter.example.com \
/usr/share/baruwa/themes/assets/example.com
ln -s /usr/share/baruwa/themes/templates/spamfighter.example.com \
/usr/share/baruwa/themes/templates/example.com
```

### 8.4.5 Default theme

A default theme allows you to customize all the domains on your system using one theme. To create a default theme, simply create templates and assets directories named `default`:

```
BARUWA_PATH=$(python -c "from distutils.sysconfig import get_python_lib; print get_python_lib(1)")
mkdir -p /usr/share/baruwa/themes/assets/default
mkdir -p /usr/share/baruwa/themes/templates/default
cp -a $BARUWA_PATH/baruwa/templates/* /usr/share/baruwa/themes/templates/default/
cp -a $BARUWA_PATH/baruwa/public/* /usr/share/baruwa/themes/assets/default/
```

You can now modify the changes to the templates under `/usr/share/baruwa/themes/templates/default/` and the CSS, JS and image files under `/usr/share/baruwa/themes/assets/default/`

### 8.4.6 Creating themes from scratch

It is possible to totally redesign the Baruwa interface using a theme, this requires an understanding of the data being sent into the template files by Baruwa as well as the Mako Template language.

We do provide theme customization services, contact us via the contact details on the [baruwa.com](http://baruwa.com) website.

### 8.4.7 Emails and Reports

Emails and Reports sent to non admin users will automatically use themes.

## 8.5 Baruwa API

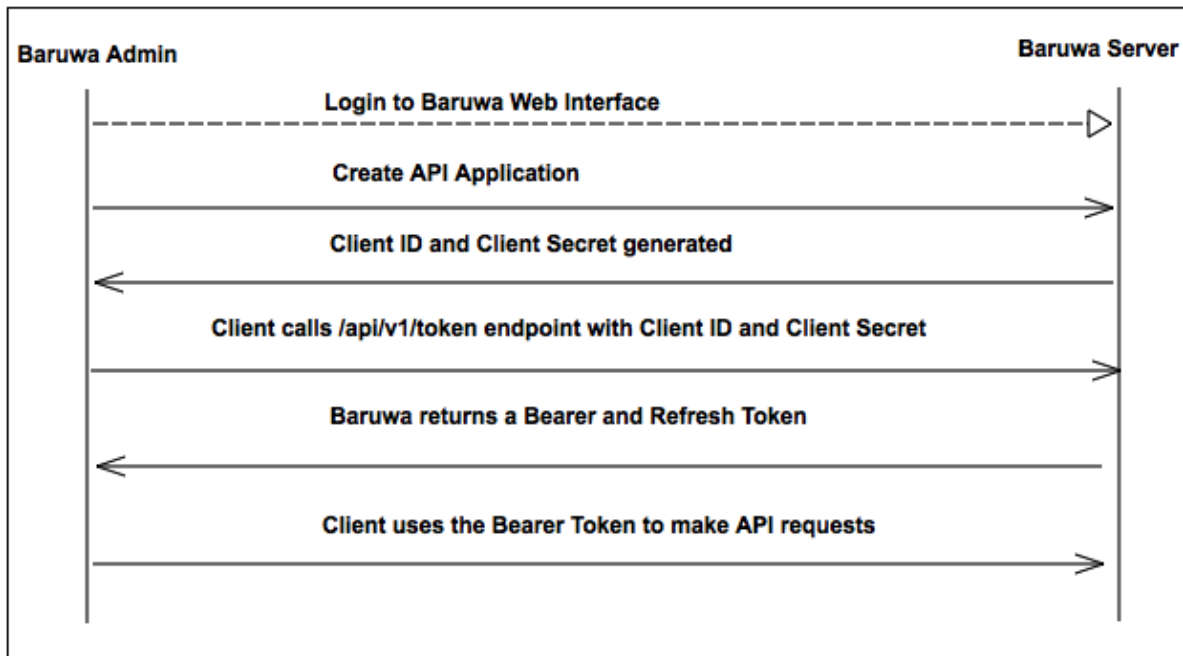
The Baruwa API allows you to manage a Baruwa Server, programmatic way using conventional HTTP requests. The endpoints are intuitive and powerful, allowing you to easily make calls to retrieve information or to execute actions. The Baruwa API is organized around **REST** and uses **OAuth 2.0** authentication. It is therefore possible to use off-the-shelf HTTP clients in any programming language.

Most of the functionality that you are familiar with in the Baruwa web interface is also available through the API, allowing you to script the complex actions that your situation requires.

### 8.5.1 How Baruwa uses OAuth 2.0

OAuth is an industry-standard open standard for authorization used by many companies to provide secure access to protected resources. The Baruwa API uses the OAuth 2.0 protocol to authorize requests.

Here is an overview of how the OAuth 2.0 auth flow works:



#### Application registration

Register your application by logging into the Baruwa web interface, and by going to the API & Applications menu under the user account.

When you create a new application, Baruwa generates a set of OAuth keys for the application (the keys consist of a `client_id` and `client_secret`).

#### Access token requests

You then obtain an access token for your application by sending a request to the `/api/v1/oauth/token` endpoint. You need to authenticate your access token request with your application credentials obtained as described above.

The Baruwa server, acting as the authorization server, verifies your application credentials and returns `Bearer` and `Refresh` access tokens.

#### API request authentication

When you make the API calls, make request by adding the access token in the `Authorization` header using the following syntax:



```
Authorization: {tokenType} {accessToken}
```

Example:

```
Authorization: Bearer XXXXXX...XXXXX9X2
```

## 8.5.2 Release Status

The API is still in Beta. Please note that during this period based on user feedback we may make some large changes which may break compatibility.

## 8.5.3 Documentation

The Baruwa API documentation is available [online](#).

## 8.6 Addons

### 8.6.1 Message Sniffer

The Message Sniffer software is designed to be installed on an email server or filtering appliance. Message Sniffer is driven by a professionally managed rulebase, available via subscription, that is continuously monitored and updated by intelligent machines and highly trained analysts. This teamwork between synthetic intelligence and extraordinary people reduces your administrative workload to a minimum and allows SNF to respond quickly (within minutes) to new threats while also predicting future hazards so they can be blocked before they arrive. Details on Message Sniffer can be found on their website at <http://www.armresearch.com/Products/aboutSNF.jsp>

Baruwa Enterprise Editions integrates with the Message Sniffer software.

### Purchase

Message Sniffer subscriptions are available for purchase from us at discounted list prices. To purchase a Message Sniffer subscription please contact us.

### Installation

The automated install system is capable of installing and configuring Message Sniffer software. In order to install Message Sniffer using the automated system, you need to contact us to purchase a subscription we will email you an AUTHENTICATION ID as well as a LICENSE ID.

You should then run the `baruwa-setup` utility and set the `Authentication ID` and the `License ID` in the `Message Sniffer Settings` screen and check the `Enable Message Sniffer` checkbox. The utility will setup your system to use Message Sniffer.

To install manually [Not recommended], you need to install the software by running the following command:

```
yum install spamassassin-plugin-snf snf snf-server -y
```

You then need to edit the following files and set the license id and authentication id.

- /etc/snf-server/identity.xml
- /etc/sysconfig/snf-server

After which you need to restart the server:

```
service snf-server restart
```

## ADMINISTRATORS GUIDE

### 9.1 Managing Organizations

---

**Note:** Organizations can be managed via the [API](#) as well.

---

Organizations enable easy management of large number of domains, Administrators are assigned to Organizations and can manage all the domains with in the organization.

You can create smaller organizations out of bigger organizations and add specific domains from a bigger organization to allow delegation of domain management.

#### 9.1.1 Add an Organization

1. Mouse over or Click Organizations
2. Click Add Organization
3. Enter the name in Organization name
4. Select domain in Domains list if they already exist
5. Select admins from Admins list if they already exist
6. Click the Add organization Button

#### 9.1.2 Update an Organization

1. Click Organizations
2. Select organization > Click Edit
3. Make changes
4. Click the Update organization Button

#### 9.1.3 Delete an Organization

1. Click Organizations
2. Select organization > Click Delete
3. Check Delete Organization domains if you want to delete domains belonging to the organization.
4. Click the Delete organization Button

### 9.1.4 Search for an Organization

If you have a large number of organizations you can search for an organization by name.

1. Click `Organizations`
2. Enter the organization name in the search box
3. Click the `Search Button`

### 9.1.5 List all domains that belong to an organization

To find all domains that belong to a specific organization.

1. Click `Organizations`
2. Select `organization > Click List domains`

### 9.1.6 List all accounts that belong to an organization

To find all accounts that belong to a specific organization.

1. Click `Organizations`
2. Select `organization > Click List accounts`

### 9.1.7 Add a new domain to an organization

1. Click `Organizations`
2. Select `organization > Click Add domain`
3. Enter the domain details
4. Click `Add domain`

### 9.1.8 Import domains in to an organization

Domains can be imported using a CSV formatted file. To import domains in to an organization.

1. Click `Organizations`
2. Select `organization > Click Import domains`
3. Browse for the CSV file by clicking `Browse` next to the `CSV file` field
4. Check `Skip first line` if your first line contains descriptions.
5. Click the `Import Button`

### 9.1.9 Export an Organization's user accounts

You can export all the user accounts with in an organization.

1. Click `Organizations`
2. Click the organization name
3. Click `Export accounts`

4. Click `Download` the `csv` file
5. Save the file to your computer

### 9.1.10 View Organization details

To view the details of an organization such as number of domains, admins, relay settings

1. Click `Organizations`
2. Click the organization name

### 9.1.11 Add Outbound SMTP relay settings

Relaying of outbound mail is authenticated on a per organization basis, to enable an organization to send outbound mail through Baruwa you need to add relay settings.

Two kinds of outbound relaying are supported.

- IP address
- SMTP AUTH

You can also set spam check thresholds and actions to outbound SMTP relays that have an IP address, this allows you to manage spam on outbound email. The spam thresholds and actions work the same way they do for domains and users but will in this case apply to email originating from the specified IP address.

#### Add Outbound SMTP IP Address settings

This allows the specific IP address to send outbound mail through Baruwa.

1. Click `Organizations`
2. Click the organization name
3. Click `Add relay setting`
4. Enter the IP address in the `Hostname` field
5. Ensure the `Enabled` checkbox is checked
6. Enter a description in the `Description` field
7. Enter `Probable spam score` and `Definite spam score` values if you do not want to use the defaults
8. Select the `What to do with probable spam` and `What to do with definite spam` actions
9. Click `Add settings`

#### Add Outbound SMTP AUTH settings

This allows any client that supplies these credentials to send outbound mail through Baruwa.

1. Click `Organizations`
2. Click the organization name
3. Click `Add relay setting`
4. Ensure the `Enabled` checkbox is checked

5. Enter the username in the SMTP-AUTH username field
6. Enter the password in the SMTP-AUTH password field
7. Reenter the password in the Retype Password field
8. Enter a description in the Description field
9. Click Add settings

## 9.2 Managing Domains

---

**Note:** Domains can be managed via the [API](#) as well.

---

### 9.2.1 Adding a Domain

Domains can be added by either importing them using a CSV file, via the [API](#) or by adding them using the Add domain form.

To add a domain by import refer to *Import domains in to an organization*. To add a domain via the API refer to the API documentation.

To add a domain using the Add domain form,

1. Mouse over or Click Domains
2. Click Add a domain
3. Enter the domain details
4. Click the Add domain Button

### 9.2.2 Updating a Domain

1. Click Domains
2. Select the domain > Click Edit under actions
3. Update the details you want to change
4. Click the Update Domain Button

### 9.2.3 Deleting a Domain

1. Click Domains
2. Select the domain > Click the Domain name
3. Click Delete domain
4. Click the Delete Domain Button

## 9.2.4 Exporting Domains

Domains can be exported to CSV, To export domains.

1. Click Domains
2. Click Export Domains
3. Click Download the csv file
4. Save the CSV file to your computer

## 9.2.5 Domain Settings

Each domain has a range of additional settings that you can configure. These include *Delivery Servers, Authentication Settings, Alias Domains, DKIM, Signatures*

### Delivery Servers

Delivery servers are the actual mail servers hosting the email accounts where messages processed by Baruwa need to be delivered.

Multiple servers per domain are supported and they can be configured to either load balance or fail over.

In load balance mode mail is sent to the group of servers in a round robin manner while in fail over mail is sent to the first in the list and only to the others if the first is not available.

### Adding a delivery server

1. Click Domains
2. Select the domain > Click the actions settings icon
3. Click Add delivery server
4. Enter server IP address or Hostname in the Server address field
5. Select the protocol in the Protocol drop down
6. Change the port in the Port field if your mail server does not use port 25
7. Ensure the Enabled checkbox is checked
8. Click the Add server button

### Editing a delivery server

1. Click Domains
2. Select the domain > Click the Domain name
3. Scroll to the bottom
4. Select the delivery server > Click Edit
5. Make changes
6. Click the Update server button

### Deleting a delivery server

1. Click `Domains`
2. Select the domain > Click the `Domain` name
3. Scroll to the bottom under `Delivery Servers`
4. Select the delivery server > Click `Delete`
5. Click the `Delete server` button

### Authentication Settings

Authentication settings allow users within a domain be be authenticated to an external authentication system.

This can be used for centralized user management and to allow users to use existing authentication credentials instead of creating duplicate accounts on the Baruwa system.

The supported external authentication mechanisms include:

- AD/LDAP
- SMTP
- POP3
- IMAP
- RADIUS

The following mechanisms are planned but have not been implemented yet:

- YUBIKEY
- OAUTH

The AD/LDAP mechanism allows for the user details in the directory to be automatically updated to the Baruwa account created for them. These details include:

- First name
- Last name
- Primary Email Address
- Alias Email Addresses

### Adding Authentication Settings

1. Click `Domains`
2. Select the domain > Click the `actions settings` icon
3. Click `Add Authentication settings`
4. Enter server IP address or Hostname in the `Server address` field
5. Select the Authentication protocol in the `Protocol` drop down
6. Enter the port in the `Port` field
7. Ensure the `Enabled` checkbox is checked
8. Check the `Split address` checkbox if the username does not contain the domain part



9. Enter a username map template if your usernames require translation e.g Webmin creates usernames like `domainowner.username` the template would be `domainowner.%(user)s` For available variables see *Username map template variables*

10. Click the Add button

The AD/LDAP and RADIUS mechanisms require additional settings which can be added by *Adding AD/LDAP Authentication additional settings* and *Adding RADIUS Authentication additional settings*.

### Username map template variables

Username map templates allow you to map Baruwa logins to complex user naming schemes such as those used by web hosting control panels for virtual accounts.

The following variables are available to your username map template:

- `%(user)s` - replaced by user part of the login
- `%(domain)s` - replaced by the domain part of the login

### Adding AD/LDAP Authentication additional settings

AD/LDAP authentication requires the following additional setting.

- Base DN - The LDAP Directory Base DN
- Username attribute - The username attribute, defaults to `uid`
- Email attribute - The email attribute, defaults to `mail`
- Bind DN - The BIND DN if Directory does not allow anonymous binds
- Bind password - The BIND password
- Use TLS - Use a TLS connection
- Search for UserDN - Find the UserDN then Bind to that
- Auth Search Filter - Filter used to find the UserDN, *LDAP Search Filter Variables* are supported
- Auth Search Scope - Search Scope, defaults to `subtree`
- Email Search Filter - Filter used to find email addresses, *LDAP Search Filter Variables* are supported
- Email Search Scope - Search Scope, defaults to `subtree`

To Add AD/LDAP Authentication additional settings:

1. Click Domains
2. Select the domain > Click the Domain name
3. Scroll to the bottom under Authentication Servers
4. Select the LDAP Authentication server > Click Settings
5. Enter the required settings
6. Click the Save settings button

### LDAP Search Filter Variables

The following variables are available for use in your LDAP search filters.

- %n - login (user@domain)
- %u - user (user part of the login)
- %d - domain (domain part of the login)
- %D - domainDN (domain DN)

Variable	Auth Search Filter	Email Search Filter
%n	<b>Available</b>	<b>Not Available</b>
%u	<b>Available</b>	<b>Available</b>
%d	<b>Available</b>	<b>Available</b>
%D	<b>Available</b>	<b>Not Available</b>

### Adding RADIUS Authentication additional settings

The RADIUS protocol requires a shared secret between the client and the server, the additional settings allows you to configure this.

To Add RADIUS Authentication additional settings:

1. Click Domains
2. Select the domain > Click the Domain name
3. Scroll to the bottom under Authentication Servers
4. Select the RADIUS Authentication server > Click Settings
5. Enter the shared secret in the Radius secret field
6. Click the Save settings button

### Alias Domains

Some organisations have email addressed to the same account using different domain names, Alias domains allow users access to all their messages regardless of the domain name under a single login.

By adding an alias to a domain name, Baruwa will accept and process email for that domain alias as well. This simplifies configuration in cases where an organisation owns multiple domains for example example.com, example.net and example.org. You can add example.com as a domain and then add the others as domain aliases of example.com.

### Adding an Alias Domain

1. Click Domains
2. Select the domain > Click the actions settings icon
3. Click Add Alias Domain
4. Enter Alias domain name in the Domain alias name field
5. Ensure the Enabled checkbox is checked
6. Click the Add button

## DKIM

*DomainKeys Identified Mail (DKIM) is a method for associating a domain name to an email message, thereby allowing a person, role, or organization to claim some responsibility for the message. The association is set up by means of a digital signature which can be validated by recipients.* [Wikipedia](#)

Baruwa allows you to manage the digital signatures within the interfaces and signs any outbound messages for which DKIM is enabled.

### Generate DKIM Keys

To generate DKIM keys for a domain,

1. Click Domains
2. Select the domain > Click the actions settings icon
3. Click DKIM > Generate DKIM keys
4. Select DNS record and add to you DNS zone

### Enable DKIM signing

1. Make sure your have followed the steps in *Generate DKIM Keys*
2. Click Domains
3. Select the domain > Click the actions settings icon
4. Click DKIM > Enable/Disable DKIM signing
5. Ensure the Enabled checkbox is checked
6. Click the Submit button

### Regenerate DKIM keys

1. Click Domains
2. Select the domain > Click the actions settings icon
3. Click DKIM > Regenerate DKIM keys
4. Select DNS record and update your DNS zone

## Signatures

Baruwa can manage email signatures / disclaimers that are added to messages that are sent outbound through it. Both HTML and Text signatures are supported. HTML signatures can contain a single embedded image.

### Adding Signatures/Disclaimers

1. Click Domains
2. Select the domain > Click the actions settings icon
3. Click Signatures > Add signature

4. Select `Signature` type from the drop down
5. Enter signature content
6. Ensure the `Enabled` checkbox is checked
7. Click the `Add signature` button

### Importing Accounts

Accounts can be imported into a domain using a CSV file.

1. Click `Domains`
2. Select the domain > Click the `actions settings` icon
3. Click `Import accounts`
4. Browse for the CSV file by clicking `Browse` next to the `CSV file` field
5. Check `Skip first line` if your first line contains descriptions.
6. Click the `Import Button`

### Exporting Accounts

Accounts can be exported from a domain to a CSV file.

1. Click `Domains`
2. Select the domain > Click the `actions settings` icon
3. Click `Export accounts`
4. Click `Download the csv file`
5. Save the file to your computer

### Rulesets

---

**Note:** Domain specific rule sets are not implemented yet.

---

## 9.2.6 Searching for Domains

If you have a large number of domains you can search for a domain by name.

1. Click `Domains`
2. Enter the `Domains` name in the search box
3. Click the `Search Button`

## 9.2.7 Bulk domain management

To enable, disable or delete multiple domains:

1. Click `Domains`
2. Use the checkbox to select the domains
3. Select `enable` or `disable` or `delete` at the top
4. Click the `Submit` button

## 9.3 Managing Accounts

---

**Note:** Accounts can be managed via the [API](#) as well.

---

### 9.3.1 Adding an Account

Accounts can be added by either importing them using a CSV file, via the [API](#) or by adding them using the `Add Account` form.

To add an Account by import refer to *Importing Accounts*. To add a Account using the `Add Account` form:

1. Mouse over or Click `Accounts`
2. Click `Add Account`
3. Enter the Account details
4. Click the `Create Account` button

### 9.3.2 Updating an Account

1. Click `Accounts`
2. Select the account > Click `Edit` under actions
3. Update the details you want to change
4. Click the `Update account` button

### 9.3.3 Deleting an Account

1. Click `Accounts`
2. Select the Account > Click the `Account name`
3. Click `Delete account`
4. Click the `Delete Account` button

### 9.3.4 Exporting Accounts

Accounts can be exported to CSV, To export accounts.

1. Click `Accounts`
2. Click `Export Accounts`
3. Click `Download the csv file`
4. Save the CSV file to your computer

### 9.3.5 Search for Accounts

If you have a large number of accounts you can search for an account or accounts by name.

1. Click `Accounts`
2. Enter the Accounts name in the search box
3. Click the `Search Button`

### 9.3.6 Add alias address

Alias addresses enable a user to view emails addressed to other addresses that belong to them apart from their primary email address.

`Address tags` are supported. The `+` and `-` separators are supported. It is possible to add addresses such as `username-*@domain.com` and `username+*@domain.com`. That will match `username-work@domain.com` and `username+work@domain.com`.

To add an Alias address.

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click then `Add alias address` menu option
4. Enter Email Address
5. Check the `Enabled` checkbox
6. Click the `Create` button

### 9.3.7 Update alias address

1. Click `Accounts`
2. Select the Account > Click the Username
3. Find the alias address under `Alias Addresses`
4. Click the `Edit` icon
5. Update the Email Address
6. Check or uncheck the `Enabled` checkbox
7. Click the `Update` button

### 9.3.8 Delete alias address

1. Click `Accounts`
2. Select the Account > Click the Username
3. Find the alias address under `Alias Addresses`
4. Click the `Delete` icon
5. Click the `Delete` button

### 9.3.9 Add account signatures

Baruwa can manage email signatures / disclaimers that are added to messages that are sent outbound through it. Both HTML and Text signatures are supported. HTML signatures support a single embedded image.

Account specific signatures/disclaimers can be setup.

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Add signature`
4. Select `Signature type` from the drop down
5. Enter signature content
6. Ensure the `Enabled` checkbox is checked
7. Click the `Add signature` button

### 9.3.10 Changing an Account password

Domain administrator and normal user account passwords can be changed using the web interface, administrator accounts can only be changed using the command line.

To change an account password:

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Change password`
4. Enter the password in the `New Password` field
5. Reenter the password in the `Retype Password` field
6. Click the `Change password` button

### 9.3.11 Bulk account management

To enable, disable or delete multiple accounts:

1. Click `Accounts`
2. Use the checkbox to select the accounts
3. Select `enable` or `disable` or `delete` at the top
4. Click the `Submit` button

## 9.4 Managing API Applications

API applications are used to setup credentials for API client applications, to see how this works refer to *How Baruwa uses OAuth 2.0*

API applications are only available on Administrator and Domain Administrator accounts.

### 9.4.1 Adding an Application

To add an Application:

1. Click `Accounts`
2. Select the user account or search for it and click it.
3. Click the `Apps & API` sub menu.
4. Click the `Register new Application` link.
5. Fill in the Application details and select the scopes required.
6. Click `Create`.
7. The application details will be displayed.

### 9.4.2 Updating an Application

To update an existing application.

1. Click `Accounts`
2. Select the user account or search for it and click it.
3. Click the `Apps & API` sub menu.
4. Find the application in the list and click the `Edit` link under actions
5. Make the required changes.
6. Click `Update`.
7. The application details will be displayed.

### 9.4.3 Deleting an Application

To delete an existing application.

1. Click `Accounts`
2. Select the user account or search for it and click it.
3. Click the `Apps & API` sub menu.
4. Find the application in the list and click the `Edit` link under actions
5. Click `Delete`.
6. You will be returned to the `Apps & API` page.



## 9.5 Managing Settings

### 9.5.1 Scanning Nodes

In order to manage the scanner settings as well as get status information on your Baruwa servers you need to add them as scanning nodes

#### Adding a scanning Node

To add a scanning node, you:

1. Mouse over or Click `Settings`
2. Click `Add scanning node`
3. Enter the `Hostname` in the `Hostname` field
4. Ensure the `Enabled` checkbox is checked
5. Click the `Add node` button

#### Customize Node scanner settings

You can customize scanner settings for a specific node.

1. Click `Settings`
2. Select the scanning node > Click `settings` under actions
3. Make the changes
4. Click the `Save settings` button

#### Customize the Global scanner settings

These settings apply to all scanners that are managed from within this interface.

1. Mouse over or Click `Settings`
2. Click `MailScanner settings`
3. Make the changes
4. Click the `Save settings` button

### 9.5.2 Content Protection

Content Protection in Baruwa is used to manage the types of email attachments that users are allowed to send and receive. A full description is available at [Content Protection](#)

#### Viewing the System Default Policy

Baruwa ships default policies which are used if none is configured by the user. To view the rules in these policies:

1. Mouse over or Click `Settings`
2. Click `Content Protection`

3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Click System Default

### **Cloning a Policy**

Cloning a policy creates a new policy populated with rules from the default system policy shipped with Baruwa. This is the preferred method of creating policies where you simply would like to keep the majority of the rules but disable a few rules.

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Click Create Policy
5. Enter the Policy Name, it is better to simply edit the name part of the supplied name
6. Click the Clone Policy button

### **Creating a Policy**

This will add a blank policy without any rules in it, you will have to add rules to the policy after it has been created.

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Click Create Policy
5. Enter the Policy Name, it is better to simply edit the name part of the supplied name
6. Click the Create Policy button

### **Edit a Policy**

This allows you to enable a policy after you have added rules or to update the name of the policy/disable a policy.

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Find the Policy in the list displayed, Click the edit icon.
5. Make the changes
6. Click the Update Policy button

## Delete a Policy

This will delete the policy along with all the rules as well as update the global and domain settings which were using this policy.

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Find the Policy in the list displayed, Click the delete icon.
5. Click the Delete Policy button

## View Policy Rules

To view the rules within a policy:

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Find the Policy in the list displayed, Click the name

## Reorder Policy Rules

Baruwa matches rules on a first hit basis so in some cases you will need to change the ordering of your rules. To do so:

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Find the Policy in the list displayed, Click the name
5. Use the up and down arrows to move the rule up or down.

## Add a Rule

To add a rule to a policy you:

1. Mouse over or Click Settings
2. Click Content Protection
3. Click the Policy Type (Archive File Policies, Archive Mime Policies, File Policies, Mime Policies)
4. Find the Policy in the list displayed, Click the name.
5. Click the Add rule option
6. File in the form

7. Click the `Create Rule` button

### **Edit a Rule**

To edit a rule to a policy you:

1. Mouse over or Click `Settings`
2. Click `Content Protection`
3. Click the `Policy Type` (`Archive File Policies`, `Archive Mime Policies`, `File Policies`, `Mime Policies`)
4. Find the Policy in the list displayed, Click the name
5. Find the rule in the list displayed, Click the edit icon
6. Make the changes
7. Click the `Update Rule` button

### **Delete a Rule**

To delete a rule to a policy you:

1. Mouse over or Click `Settings`
2. Click `Content Protection`
3. Click the `Policy Type` (`Archive File Policies`, `Archive Mime Policies`, `File Policies`, `Mime Policies`)
4. Find the Policy in the list displayed, Click the name
5. Find the rule in the list displayed, Click the delete icon
6. Make the changes
7. Click the `Delete Rule` button

### **Set Global Policies**

To set Global Policies you:

1. Mouse over or Click `Settings`
2. Click `Content Protection`
3. Click `Set Global Policies`
4. Select the Policies
5. Click the `Save` button

### **Set Domain Policies**

To set domain specific policies you:

1. Click `Domains`
2. Select the domain > Click the actions settings icon

3. Click `Content Protection`
4. Select the Policies
5. Click the `Save` button

### 9.5.3 MTA Settings

MTA Settings in Baruwa are used to Manage the following lists

- Empty Reply Checks Exemptions
- Subject Block List
- Anti-Virus Checks Exemptions
- System Signature Exemptions
- Ratelimit Exemptions
- TLS/SSL Exemptions
- Anonymizer List
- DKIM Checks Exemptions
- DNSBL Checks Exemptions
- SPF Checks Exemptions

#### Empty Reply Checks Exemptions List

The `Empty Reply Checks Exemptions` list is used to exempt an IP address from Empty Reply Checks, Empty Reply checks block email messages that have an `empty Reply-To :` header set.

#### Adding to the Empty Reply Checks Exemptions list

To add an IP address you want to by pass the checks you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `Empty Reply Checks Exemptions`
4. Click `Add Setting`
5. Enter the IP address in the `Address` field
6. Check the `Enabled` checkbox
7. Click the `Create Setting` button

#### Updating an Empty Reply Checks Exemptions list item

To edit an address in the `Empty Reply Checks Exemptions` list you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `Empty Reply Checks Exemptions`

4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### **Deleting an entry from the Reply Checks Exemptions list**

To delete an address in the Empty Reply Checks Exemptions list you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Empty Reply Checks Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### **Subject Block List**

The Subject Block list is used to reject obvious spam based on the subject at SMTP time. Regular expressions can be used in the form of `^\Nregex\N$`, e.g `^\N.*viagra.*\N` will match 'viagra', 'v1agra', 'v-i-a-g-r-a', etc.

### **Adding to the Subject Block List**

To add a Subject you want to block, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Subject Block List
4. Click Add Setting
5. Enter the Subject in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### **Updating a Subject Block List item**

To edit a subject in the Subject Block List you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Subject Block List
4. Find the item in the list
5. Click the Edit icon in the Actions column

6. Make the changes
7. Click the Update Setting button

### Deleting an entry from the Subject Block List

To delete a subject in the Subject Block list you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Subject Block List
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### Anti-Virus Checks Exemptions List

The Anti-Virus Checks Exemptions list is used to exempt IP Addresses from Anti-Virus checks, only use this for hosts you trust with your life.

### Adding to the Anti-Virus Checks Exemptions List

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Anti-Virus Checks Exemptions
4. Click Add Setting
5. Enter the IP Address in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### Updating a Anti-Virus Checks Exemptions List entry

To edit an entry in the Anti-Virus Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Anti-Virus Checks Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### **Deleting an entry from the Anti-Virus Checks Exemptions List**

To delete an entry in the Anti-Virus Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Subject Block List
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### **System Signature Exemptions List**

The System Signature Exemptions list is used to exempt Domains from global signature additions.

### **Adding to the System Signature Exemptions List**

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click System Signature Exemptions
4. Click Add Setting
5. Enter the Domain name in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### **Updating a System Signature Exemptions List entry**

To edit an entry in the System Signature Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click System Signature Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button



### Deleting an entry from the System Signature Exemptions List

To delete an entry in the System Signature Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Subject Block List
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### Ratelimit Exemptions List

The Ratelimit Exemptions list is used to exempt IP Addresses from rate limiting.

### Adding to the Ratelimit Exemptions List

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Ratelimit Exemptions
4. Click Add Setting
5. Enter the IP Address in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### Updating a Ratelimit Exemptions List entry

To edit an entry in the Ratelimit Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Ratelimit Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### **Deleting an entry from the Ratelimit Exemptions List**

To delete an entry in the Ratelimit Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Ratelimit Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### **TLS/SSL Exemptions List**

The TLS/SSL Exemptions list is used to exempt IP Addresses from the requirement to use TLS/SSL.

### **Adding to the TLS/SSL Exemptions List**

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click TLS/SSL Exemptions
4. Click Add Setting
5. Enter the IP Address in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### **Updating a TLS/SSL Exemptions List entry**

To edit an entry in the TLS/SSL Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click TLS/SSL Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### Deleting an entry from the TLS/SSL Exemptions List

To delete an entry in the TLS/SSL Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click TLS/SSL Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### Anonymizer List

The Anonymizer List is for domains whose email messages you would like to anonymize by removing the Received headers.

### Adding to the Anonymizer List

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Anonymizer List
4. Click Add Setting
5. Enter the IP Address in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### Updating a Anonymizer List entry

To edit an entry in the Anonymizer List, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click Anonymizer List
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### **Deleting an entry from the Anonymizer List**

To delete an entry in the `Anonymizer List`, you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `Anonymizer List`
4. Find the item in the list
5. Click the `Delete` icon in the `Actions` column
6. Click the `Delete Setting` button

### **DKIM Checks Exemptions List**

The `DKIM Checks Exemptions List` is for IP addresses you want to exempt from DKIM verification checks.

### **Adding to the DKIM Checks Exemptions List**

To add an entry, you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `DKIM Checks Exemptions`
4. Click `Add Setting`
5. Enter the `IP Address` in the `Address` field
6. Check the `Enabled` checkbox
7. Click the `Create Setting` button

### **Updating a DKIM Checks Exemptions List entry**

To edit an entry in the `DKIM Checks Exemptions` list, you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `DKIM Checks Exemptions`
4. Find the item in the list
5. Click the `Edit` icon in the `Actions` column
6. Make the changes
7. Click the `Update Setting` button

### Deleting an entry from the DKIM Checks Exemptions List

To delete an entry in the DKIM Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click DKIM Checks Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### DNSBL Checks Exemptions List

The DNSBL Checks Exemptions List is for IP addresses you want to exempt from DNSBL/RBL checks.

### Adding to the DNSBL Checks Exemptions List

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click DNSBL Checks Exemptions
4. Click Add Setting
5. Enter the IP Address in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### Updating a DNSBL Checks Exemptions List entry

To edit an entry in the DNSBL Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click DKIM Checks Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### **Deleting an entry from the DNSBL Checks Exemptions List**

To delete an entry in the DNSBL Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click DNSBL Checks Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

### **SPF Checks Exemptions List**

The SPF Checks Exemptions List is for Domain names you want to exempt from SPF checks.

### **Adding to the SPF Checks Exemptions List**

To add an entry, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click SPF Checks Exemptions
4. Click Add Setting
5. Enter the Domain name in the Address field
6. Check the Enabled checkbox
7. Click the Create Setting button

### **Updating a SPF Checks Exemptions List entry**

To edit an entry in the SPF Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click SPF Checks Exemptions
4. Find the item in the list
5. Click the Edit icon in the Actions column
6. Make the changes
7. Click the Update Setting button

### Deleting an entry from the SPF Checks Exemptions List

To delete an entry in the SPF Checks Exemptions list, you:

1. Mouse over or Click Settings
2. Click MTA Settings
3. Click SPF Checks Exemptions
4. Find the item in the list
5. Click the Delete icon in the Actions column
6. Click the Delete Setting button

## 9.5.4 Local Scores

Local scores override the default system spam scores.

### Adding a local score

Local scores can be added via two routes.

1. From the message detail page
2. From the list under Local Scores

To add via the message detail page:

1. Click Rule name
2. Enter the Local Score
3. Click the Update Local Score Button

To add via the Local Scores list:

1. Mouse over or Click Settings
2. Click Local scores
3. Find the Rule in the list
4. Click the Edit icon under the Actions column
5. Enter the Local Score
6. Click the Update Local Score Button

### Updating a local score

Follow the same steps as Adding a local score.

### Deleting a local score

Follow the same steps as Adding a local score. Set the local score to 0

## 9.6 System Status

System status gives you a dash board view of your Baruwa system or cluster.

The following information is provided:

- Global status
- Scanner node status
- Mail Queues
- Audit logs

### 9.6.1 Global status

The global status dashboard gives you the status information for the whole of your Baruwa system/cluster at a glance.

#### Day's processed message totals

- Number of messages processed
- Number of messages found to be clean
- Number of messages found to be High scoring spam
- Number of messages found to be Low scoring spam
- Number of messages found to be Virus infected
- Number of messages found to be Policy blocked
- Number of messages in the Inbound queues
- Number of messages in the Outbound queues

#### Graph of Day's processed message totals

A graphical view of the above information in a PIE chart graph.

#### Scanner node status

The status of all the scanning nodes in this Baruwa cluster.

### 9.6.2 Scanner node status

Provides the status of a specific scanning node, and allows you to pull additional information via select commands.

The following status information is provided.

- Day's stats for the specific node
- Node Hardware status (CPU, Memory, Disk, Network)
- System Network stats
- System software status (Scanners, MTA, Anti Virus engine)



### 9.6.3 Mail Queues

The status of both the `inbound` and `outbound` mail queues is provided. The following actions can be performed on messages that are in the queues:

- Delivery
- Bounce
- Hold
- Delete
- Preview

Details on how to carry out the above actions can be found in the user guide's *Processing queued messages* section.

### 9.6.4 Audit logs

Audit logs are provided for the interactions that users have with the system. The following information is recorded.

- Date and Time
- Username
- Interaction information
- Baruwa Node hostname or IP address
- Users IP address
- Category

Interactions are classified under the following categories

- Read
- Create
- Auth
- Update

The Audit logs can be exported in both PDF and CSV formats for offline usage.

The Audit logs are searchable, all full text search options are supported. Tips on searching are available on the *Baruwa Search Tips and Tricks* page.

## 9.7 Command line Reference

Custom paster commands are provided to enable scripting of house keeping tasks such as quarantine management and Database maintenance.

---

**Note:** This information is provided simply for reference and documentation purposes scheduled tasks are installed by default to perform these house keeping tasks for you, you do not have to create new cronjobs. For information on cronjobs that use these commands refer to *Scheduled commands*

---

### 9.7.1 Command options and help

These commands may take options to get details on the supported options run:

```
paster baruwa
paster COMMAND_NAME -h or paster help COMMAND_NAME
```

The paster command now has auto completions support meaning you can press tab to get the available options:

```
paster
camqadm                create                points                routes
celerybeat             create-admin-user    post                 send-pdf-reports
celeryd                exe                  prune-database       send-pdf-reports
celeryev               help                 prune-quarantine     send-quarantine-
change-user-password   make-config          request              send-quarantine-
```

### 9.7.2 Quarantine management

```
paster prune-quarantine /etc/baruwa/production.ini
```

Deletes quarantined files older than `ms.quarantine.days_to_keep`. This is set in the `/etc/baruwa/production.ini` file

### 9.7.3 Quarantine reports

```
paster send-quarantine-reports-ng /etc/baruwa/production.ini
```

Generates an email report of the quarantined messages. This command allows you to specify the number of days the report should cover as well as the maximum number of messages to return. The following switches allow you to specify periods.

- `-o NUM_DAYS, --newer-than=NUM_DAYS` Report on messages this number of days back
- `-m MAX_MSGS, --max-records=MAX_MSGS` Maximum number of messages to return
- `-i ORG_ID, --org-id=ORG_ID` Process only this organization's accounts
- `-e EXCLUDE_ORG, --excluded-org=EXCLUDE_ORG` Exclude this organization's accounts
- `-f, --force` Force sending of reports even if hour is not in user or domain set timezone

### 9.7.4 Database maintenance

```
paster prune-database /etc/baruwa/production.ini
```

Deletes records older than 30 days from the messages table of the database, and archives them to the archive table. It deletes records older than 90 days from the archives table. These defaults can be configured in the configuration file as the following options:

- `baruwa.messages.keep.days`
- `baruwa.archive.keep.days`

The following options allow you to specify the periods of the records that need to be processed.

- `-d --days` records older than this number are deleted from messages
- `-a --adays` records older than this number are deleted from archives

### 9.7.5 Spamassassin rule description updates

```
paster update-sa-rules /etc/baruwa/production.ini
```

Updates the Spamassassin rule descriptions in the database.

### 9.7.6 PDF reports

```
paster send-pdf-reports-ng /etc/baruwa/production.ini
```

Sends PDF reports by email. This command allows you to specify the report type [domain, user], report period [daily, weekly, monthly] and the number of days to report on. The following switches allow you to specify the options.

- `-t REPORT_TYPE, --report-type=REPORT_TYPE` Report type [user, domain]
- `-p REPORT_PERIOD, --report-period=REPORT_PERIOD` Report period [daily, weekly, monthly]
- `-d NUMBER_OF_DAYS, --number-of-days=NUMBER_OF_DAYS` Restrict to number of days
- `-i ORG_ID, --org-id=ORG_ID` Process only this organization's accounts
- `-e EXCLUDE_ORG, --excluded-org=EXCLUDE_ORG` Exclude this organization's accounts
- `-f, --force` Force sending of reports even if hour is not in user or domain set timezone

### 9.7.7 Mail queue Stats updates

```
paster update-queue-stats /etc/baruwa/production.ini
```

Query the inbound and outbound queues and write stats to the database.

### 9.7.8 Delta search index updates

```
paster update-delta-index --index messages --realtime /etc/baruwa/production.ini
paster update-delta-index --index archive /etc/baruwa/production.ini
```

The `messages` and `archive` index have deltas to ensure that indexing is efficient the above commands merge the delta index with the main index and remove id's from the realtime index that have been indexed to disk indexes.

The `messages` index has a real time index while `archive` does not.

### 9.7.9 Create an administrator account

```
paster create-admin-user -u USERNAME -p PASSWORD -e EMAIL -t TIMEZONE /etc/baruwa/production.ini
```

Create an administrator account

### 9.7.10 Change user password

```
paster change-user-password --username USERNAME [/etc/baruwa/production.ini]
```

Changes an accounts password, This is the only way to change an administrator account's password as it cannot be changed via the web interface.

### 9.7.11 Generate list of top spammers

```
paster send-top-spammer-list -e EMAIL [-m -s SPAMSCORE -p REPORT_PERIOD -d] [/etc/baruwa/production.
```

Generates a list of top spammers and emails or displays it.

- `-e EMAIL`, `--email=EMAIL` Email address to send data to
- `-m`, `--include-message-count` Include the number messages received
- `-d`, `--dry-run` Print to stdout do not send email
- `-n NUM`, `--messages-sent=NUM` Return senders with message counts equal to or greater than
- `-s SPAMSCORE`, `--spam-score-threshold=SPAMSCORE` Count messages with spam scores equal to or greater than
- `-p REPORT_PERIOD`, `--report-period=REPORT_PERIOD` Report period [daily, weekly, monthly]

### 9.7.12 Generate list of clean senders

```
paster send-whitelist-data -e EMAIL [-m -s SPAMSCORE -p REPORT_PERIOD -d] [/etc/baruwa/production.in
```

Generates a list of top ham senders for whitelisting.

- `-e EMAIL`, `--email=EMAIL` Email address to send data to
- `-m`, `--include-message-count` Include the number messages received
- `-d`, `--dry-run` Print to stdout do not send email
- `-n NUM`, `--messages-sent=NUM` Return senders with message counts equal to or greater than
- `-s SPAMSCORE`, `--spam-score-threshold=SPAMSCORE` Count messages with spam scores equal to or greater than
- `-p REPORT_PERIOD`, `--report-period=REPORT_PERIOD` Report period [daily, weekly, monthly]

### 9.7.13 Create Scanner rulesets

```
paster update-rulesets [/etc/baruwa/production.ini]
```

This will create or update the necessary Scanner rulesets.

### 9.7.14 Create MTA lookup files

```
paster update-mta-lookup [/etc/baruwa/production.ini]
```

This will create or update the MTA CDB lookup files.

### 9.7.15 Dump MTA lookup file

```
paster dump-mta-lookup-file [/etc/baruwa/production.ini] -f /var/lib/baruwa/data/db/routedata.cdb
```

This will display the contents of a CDB lookup file.

- `-f FILENAME, --filename=FILENAME` Lookup file to dump

## 9.8 Scheduled commands

Scheduled commands are configured as cronjobs to carry out house keeping and maintenance tasks on the system by default.

The following scheduled paster commands are installed and enabled by default.

### 9.8.1 /etc/cron.d/baruwa

This contains several commands which are run at different intervals.

Interval	Command	Description
3 Minutes	<code>paster update-queue-stats /etc/baruwa/production.ini</code>	Updates the mail queue statistics
@ 00H00	<code>paster update-sa-rules /etc/baruwa/production.ini</code>	Updates the Spam rules descriptions for the web interface
Hourly	<code>paster send-quarantine-reports /etc/baruwa/production.ini</code>	Sends out the quarantine reports in the users timezone
@ 01H00	<code>paster prune-database /etc/baruwa/production.ini</code>	Archives old records to the archive table and prunes old records from the archive table
@ 02H00	<code>paster prune-quarantine /etc/baruwa/production.ini</code>	Deletes old quarantined messages from disk
@ 10 mins every hour on the 1st	<code>paster send-pdf-reports /etc/baruwa/production.ini</code>	Sends out the PDF reports in the users timezone
@ 20 mins every hour every day	<code>paster send-pdf-reports -t domain -p daily -d 1 /etc/baruwa/production.ini</code>	Sends out the daily PDF reports in users timezone
@ 30 mins every hour on Monday	<code>paster send-pdf-reports -t domain -p weekly -d 7 /etc/baruwa/production.ini</code>	Sends out the weekly PDF reports in users

## 9.8.2 Other scheduled commands

You will find all the other schedules system commands in the cron directories in `/etc/cron.d` `/etc/cron.hourly` `/etc/cron.daily` `/etc/cron.weekly`

## 9.9 Baruwa Backups

### 9.9.1 Etckeeper

The configurations in the `/etc` directory are backed up using `etckeeper` into a git repository located in `/etc/.git`. You should be able to recover and restore any configuration files you change or delete.

### 9.9.2 Backup Ninja

Baruwa Enterprise Edition ships with and configures `backupninja` to backup the database, system configurations as well as the mail quarantine.

#### Database backups

A SQL dump of the database is created daily and is stored in the `/var/lib/pgsql/backups` directory.

#### Filesystem backups

These backups are created in the `rdiff` format and contain both the Database and Etckeeper backups.

The backups are stored under `/var/backups/hostname`.

#### Offsite Backups

You can setup your own offsite backups by placing a file in the `/etc/backups.d` directory. The supported remote backup formats are:

- `Rsync`
- `Rdiff`
- `Duplicity`
- `Wget`

### 9.9.3 Frequency

The backups are created once a day.

## 9.10 Monitoring

### 9.10.1 NRPE

It is possible to monitor Baruwa Enterprise Edition systems using the NRPE protocol from Nagios. To enable monitoring check the `Enable Monitoring` checkbox on the `System Settings` screen of the `baruwa-setup` utility.

#### Monitoring points

Depending on the system profile, the following points are available via NRPE.

- Disk space
- Uwsgi process
- Database process
- Database proxy process
- Indexer process
- Cache process
- Message Queue process
- Baruwa celery process
- Baruwa Logging process
- Mail Scanning process
- Anti Virus Engine process
- Message queue status
- System Load
- Security Updates

#### Adding your own monitoring points

You can add your own NRPE monitoring points by placing a `.cfg` file in `/etc/nrpe.d` then reload the `nrpe` service to activate the monitoring points.

#### Monitoring services

You can monitor the services by connecting to the actual port, most monitoring systems are able to do this.

#### Firewall

The firewall port 5666 inbound is open to all, you need to restrict this by allowing access only from your monitoring IP addresses.

## 9.11 Baruwa log files

Below are Baruwa Enterprise Edition log file locations, which may be useful for troubleshooting. The `baruwa-logs` command is also available and allows you to tail the necessary logs in colour. It will display the logs specific to the system profile.

To use the `baruwa-logs` command simply run:

```
baruwa-logs
```

### 9.11.1 Nginx

- `/var/log/nginx/[hostname].log`

### 9.11.2 Uwsgi

- `/var/log/uwsgi/uwsgi-baruwa.log`

### 9.11.3 Baruwa

- `/var/log/baruwa/celeryd.log`
- `/var/log/baruwa/what-who.log`

### 9.11.4 MailScanner

- `/var/log/maillog`

### 9.11.5 Exim

- `/var/log/exim/main.log`
- `/var/log/exim/reject.log`

### 9.11.6 RabbitMQ

- `/var/log/rabbitmq/[hostname].log`
- `/var/log/rabbitmq/shutdown_err`
- `/var/log/rabbitmq/shutdown_log`
- `/var/log/rabbitmq/startup_err`
- `/var/log/rabbitmq/startup_log`



### 9.11.7 ClamAV

- /var/log/clamav/clamd.log
- /var/log/clamav/freshclam.log
- /var/log/clamav-unofficial-sigs/clamav-unofficial-sigs.log

### 9.11.8 Sphinx

- /var/log/sphinx/query.log
- /var/log/sphinx/searchd.log

### 9.11.9 Pgbouncer

- /var/log/pgbouncer/pgbouncer.log

### 9.11.10 PostgreSQL

- /var/lib/pgsql/data/pg\_log/postgresql-[day].log

### 9.11.11 BackupNinja

- /var/log/backupninja.log

## 9.12 Languages supported

The following languages are currently supported. Adding a new language is a simple task which can be done using the online translation service: [Transifex](#) which is used to manage our translations.

- English
- French
- German
- Greek
- Catalan
- Chinese
- Dutch
- Bulgarian
- Czech
- Danish
- Hindi
- Indonesian
- Italian

- Norwegian
- Polish
- Portuguese
- Russian
- Spanish
- Swedish
- Thai
- Turkish
- Japanese
- Romanian
- Arabic
- Hebrew
- Finnish
- Korean
- Latvian
- Ukrainian
- Urdu
- Vietnamese
- Persian
- Afrikaans
- Burmese
- Hungarian
- Slovak
- Swahili

## 9.13 FAQ's

Answers to many common questions.

### 9.13.1 I think I've found a security problem! What should I do?

**Answer:** Email [security@baruwa.com](mailto:security@baruwa.com)

If you think you've found a security vulnerability with Baruwa, please send a message to [security@baruwa.com](mailto:security@baruwa.com). Do NOT post a bug report to our issue tracking system or disclose the issue on our mailing lists.

### 9.13.2 Can a user have multiple email addresses on a single account ?

**Answer:** Yes

You can add alias addresses to a users account. Domains using Active Directory authentication will have these auto populated from the groups and addresses in active directory.

Alias domain addresses are also auto created the first time a user logs in.

### 9.13.3 Can users use their current mail password to login to Baruwa ?

**Answer:** Yes

Setup external authentication with either POP3, IMAP, SMTP, LDAP and RADIUS / RSA SecurID.

### 9.13.4 Are there any restrictions on username format ?

**Answer:** No

However users that authenticate to external systems will have their email address automatically configured as their username locally.

### 9.13.5 Which MTA does Baruwa Enterprise use ?

**Answer:** Exim

Baruwa Enterprise uses a customized version of the Exim MTA

### 9.13.6 How do the Baruwa Enterprise Edition subscriptions work ?

In order to run Baruwa Enterprise Edition you have to purchase a subscription. This gives you access to the BaruwaOS, Baruwa Network, Baruwa Datafeeds and Email Support.

You get access to any new upgrades and updates are available via the Baruwa Network.

If you cancel you **MUST** uninstall and stop using the software.

Should you choose to return on to support, you will have to pay for the period when your system did not have support before you can be returned on to support.

### 9.13.7 Are there limitations on the number of users or domains ?

**Answer:** No

Unlike our competitors we do not restrict the number of users or domains you can configure on your systems.

## 9.14 Upgrading

### 9.14.1 2.0.8

- Enhancement
- Bug fix

## Backward compatibility

### New dependencies

None

### New configuration options

None

### Template changes

The following template files have been changed.

- settings/mta.html
- messages/detail.html

## Upgrading

Review the changelog for version *2.0.8* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, perform *Run OS Upgrade* first.

## Change Management

Ensure you follow your organization change management policy and schedule downtime as well as plan how to revert.

Backup your entire system before you proceed.

### Run setup utility

To perform the upgrade you run the `baruwa-setup` command as follows:

```
baruwa-setup
paster update-mta-lookup
```

### Monitor logs for issues

You can monitor the relevant logs using the `baruwa-logs` utility:

```
baruwa-logs
```

If you run into any issues please contact *Support*

Thats it.

## 9.14.2 2.0.7

### Upgrade Type

- Enhancement
- Bug fix

### Backward compatibility

This release introduces backwards incompatible database schema changes.

The `relaysettings` table has been modified to support the relay settings `ratelimit` option.

The `messages` and `archive` table have been updated to include a `msgfiles` column which stores the message on disk location.

### New dependencies

- arrow
- python-cdb

### New configuration options

- `baruwa.send.reports.at` - Sets the hour at which reports are sent out, this is translated to a users specific timezone.

### Upgrading

Review the changelog for version *2.0.7* and read the updated documentation before you proceed with the upgrade.

---

**Note:** Please note that Baruwa Enterprise Edition 2.0.7 uses a custom OS known as BaruwaOS this is based on CentOS so it will upgrade in place on any RHEL clone.

---

### Change Management

Ensure you follow your organization change management policy and schedule downtime as well as plan how to revert.

Backup your entire system before you proceed.

### Activation Key

Make sure you have your activation key, before you proceed. If you have misplaced your key please contact *Support*.

### Known issues

If the script detects that you are using weak database passwords it will automatically generate new passwords. If you are running in a cluster and require these new passwords they will be stored in `/root/.cluster-pws.txt`. The passwords are only stored if the configuration being upgraded is a clustered configuration. In standalone mode the passwords will be stored only in the encrypted database.

After you have finished the upgrade it is important that you delete this file.

### Run OS Upgrade

Download the OS upgrade script from the Baruwa Enterprise Edition website:

```
cd /usr/local/src
curl -O https://www.baruwa.com/downloads/upgradeos.py
```

Run the upgrade script to convert your OS to BaruwaOS:

```
chmod +x upgradeos.py
./upgradeos.py
```

The script will execute and convert your system to BaruwaOS

### Run setup utility

Baruwa Enterprise Edition  $\geq$  2.0.7 uses an automated wizard based utility called `baruwa-setup` to configure the system. This utility collects configuration information from the user, performs any required software updates and then configures the system based on the profile selected and the configuration data collected. This simplifies the whole setup process in that the user does not have to edit any files.

The `baruwa-setup` utility is a wizard that asks a series of questions and then configures the system based on the answers provided.

A pass phrase is required to secure the authentication information that is collected.

Make sure you choose a strong pass phrase which is easy for you to remember but difficult to guess for others, a long sentence describing a personal experience is a good pass phrase.

**Warning:** The `baruwa-setup` utility will automatically detect your existing certificates based on the hostname, if this is successful it will set the `I have a CA issued certificate to checked`. Do NOT uncheck this if you intend on creating a self signed certificate with the same details. If you do a certificate with the same serial number will be generated and it will be rejected by your client machines.

The `baruwa-setup` utility will import settings from your existing puppet manifest and prompt you for any new configuration settings. It will then upgrade your system.:

```
baruwa-setup -p /usr/local/src/${hostname}.pp
```

### Monitor logs for issues

You can monitor the relevant logs using the `baruwa-logs` utility:

```
baruwa-logs
```

If you run into any issues please contact *Support*

Thats it.

### 9.14.3 2.0.6

#### Upgrade Type

- Enhancement
- Bug fix

#### Backward compatibility

This release introduces backwards incompatible database schema changes.

#### New dependencies

- tinycss
- oauthlib

#### New configuration options

- `baruwa.languages` - Sets the languages that should be enabled and available. This limits the languages available to only the configured languages.
- `baruwa.default.language` - Sets the default system language.

#### Updated configuration options

- `challenge_decider` - Has been changed to a Baruwa function, the old one was a repoze function. The new option is `baruwa.lib.auth.middleware:baruwa_challenge_decider`
- `celery.queues` - The fanout queue is not named just `fanout` without the FQDN

#### Upgrading

Review the changelog for version *2.0.6* and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
```

## Automated installs

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Perform the upgrade:

```
yum upgrade -y
yum install rpmconf
rpmconf -a -c
export CCFG=/etc/puppet/manifests/toasters/baruwa/${hostname}.pp
export BCFG=/etc/puppet/manifests/toasters/baruwa/${hostname}.pp.orig
export NCFG=/etc/puppet/manifests/toasters/baruwa/init.pp
cp ${CCFG} ${BCFG}
/etc/puppet/bin/update-puppet-config.pl -oldconfig ${BCFG} -newconfig ${NCFG} > ${CCFG}
puppet apply ${CCFG}
rm -rf /var/lib/baruwa/data/templates/*
service mailscanner restart
service uwsgi restart
service baruwa restart
```

## Manual installs

Update the database schema:

```
psql -Ubaruwa baruwa
baruwa=> ALTER TABLE maildomains ADD column virus_actions smallint;
baruwa=> ALTER TABLE maildomains ADD column virus_checks_at_smtp boolean;
baruwa=> UPDATE maildomains SET virus_actions=2 WHERE virus_actions IS NULL;
baruwa=> UPDATE maildomains SET virus_checks_at_smtp='t' WHERE virus_checks_at_smtp IS NULL;
baruwa=> ALTER TABLE relaysettings ADD COLUMN low_score double precision;
baruwa=> ALTER TABLE relaysettings ADD COLUMN high_score double precision;
baruwa=> ALTER TABLE relaysettings ADD COLUMN spam_actions smallint;
baruwa=> ALTER TABLE relaysettings ADD COLUMN highspam_actions smallint;
baruwa=> UPDATE relaysettings SET low_score=0.0 WHERE low_score IS NULL;
baruwa=> UPDATE relaysettings SET high_score=0.0 WHERE high_score IS NULL;
baruwa=> UPDATE relaysettings SET spam_actions=2 WHERE spam_actions IS NULL;
baruwa=> UPDATE relaysettings SET highspam_actions=2 WHERE highspam_actions IS NULL;
```

Update the configuration files by referring to the configuration file section. The following files will require updating.

- /etc/exim/exim.conf
- /etc/exim/macros.conf
- /etc/MailScanner/MailScanner.conf

You can generate a new Baruwa configuration by running:

```
paster make-config baruwa /etc/baruwa/production.ini
```

Create additional database tables:



```
paster setup-app /etc/baruwa/production.ini
```

Generate the required MailScanner rulesets:

```
paster update-rulesets /etc/baruwa/production.ini
```

Clean up and restart the required services:

```
yum install rpmconf -y
rpmconf -a -c
rm -rf /var/lib/baruwa/data/templates/*
service mailscanner restart
service uwsgi restart
service baruwa restart
```

## 9.14.4 2.0.5

### Upgrade Type

- Enhancement
- Bug fix

### Backward compatibility

This release introduces a backwards incompatible database schema change. The relaysettings table has been modified to support the relay settings description.

### New dependencies

None

### New configuration options

- `baruwa.memcached.host` - Sets the address of the memcached server, this used for the distributed locking in a cluster.

### Upgrading

Review the changelog for version *2.0.5* and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
```

Modify the relaysettings table, you will need to supply the Baruwa PostgreSQL password:

```
psql -Ubaruwa baruwa
baruwa=> ALTER TABLE relaysettings ADD column description varchar(255);
```

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Perform the upgrade:

```
yum upgrade -y
cp /etc/puppet/manifests/toasters/baruwa/$(hostname).pp /etc/puppet/manifests/toasters/baruwa/$(hostname)
/etc/puppet/bin/update-puppet-config.pl -oldconfig /etc/puppet/manifests/toasters/baruwa/$(hostname)
-newconfig /etc/puppet/manifests/toasters/baruwa/init.pp > /etc/puppet/manifests/toasters/baruwa/$(hostname)
puppet -v /etc/puppet/manifests/toasters/baruwa/$(hostname).pp
service mailscanner restart
service uwsgi restart
service baruwa restart
```

### 9.14.5 2.0.4

#### Upgrade Type

- Enhancement
- Bug fix

#### Backward compatibility

This release introduces a backwards incompatible database schema change. The `quickpeek` database view has been modified to better order the options returned.

#### New dependencies

None

#### New configuration options

None

#### Upgrading

Review the changelog for version [2.0.4](#) and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
```

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Perform the upgrade:

```
yum upgrade -y
paster setup-app /etc/baruwa/production.ini
puppet -v /etc/puppet/manifests/toasters/baruwa/$(hostname).pp
service mailscanner restart
service uwsgi restart
service baruwa restart
```

## 9.14.6 2.0.3

### Upgrade Type

- Enhancement
- Bug fix

### Backward compatibility

This release does not introduce any backwards incompatible changes.

### New dependencies

None

### New configuration options

- `baruwa.dkim.selector` - Sets the DKIM selector name default: `baruwa`

### Upgrading

Review the changelog for version [2.0.3](#) and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
```

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Perform the upgrade:

```
yum upgrade -y
rm -rf /var/lib/baruwa/data/cache/*
rm -rf /var/lib/baruwa/data/sessions/*
rm -rf /var/lib/baruwa/data/templates/*
service uwsgi restart
```

```
service baruwa restart
puppet -v /etc/puppet/manifests/toasters/baruwa/${hostname}.pp
```

### 9.14.7 2.0.2

#### Upgrade Type

- Enhancement
- Bug fix

#### Backward compatibility

This release introduces a backwards incompatible database schema change. The `UNIQUE INDEX` on the `message-id` field has been dropped to allow for duplicate `message-id`'s to be supported. Duplicate `message-id`'s may occur in high volume environments.

The template variables for the `messages/preview.html` and the `status/preview.html` templates have changed. The changes allow for the support of alternative message format display as well as displaying correctly formatted HTML messages. If you have customized your templates, you will need to review the new variable format and update your customized templates.

#### New dependencies

- `cssutils`
- `pyzmail`

#### New configuration options

None.

#### Upgrading

Review the changelog for version *2.0.2* and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
```

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Modify the `message-id` index, you will need to supply the Baruwa PostgreSQL password:

```
psql -Ubaruwa baruwa
baruwa=> DROP INDEX ix_messages_messageid;
baruwa=> CREATE INDEX ix_messages_messageid ON messages(messageid);
```

Perform the upgrade:

```
yum upgrade -y
rm -rf /var/lib/baruwa/data/cache/*
rm -rf /var/lib/baruwa/data/sessions/*
rm -rf /var/lib/baruwa/data/templates/*
service uwsgi restart
service baruwa restart
puppet -v /etc/puppet/manifests/toasters/baruwa/$(hostname) .pp
```

If you had customized your interface, then update the changed templates to use the new variables.

## 9.14.8 2.0.1

### Upgrade Type

- Security [Severity: Medium]
- Bug fix
- Enhancement

### Backward compatibility

This release does not introduce any backwards incompatible changes.

### New dependencies

- sqlparse

### New configuration options

- `ms.quarantine.shared` - Enables and disables shared quarantine features default: `disabled`
- `baruwa.themes.base` - Sets the directory containing themes default: `/usr/share/baruwa/themes`
- `baruwa.custom.name` - Sets the custom product name for rebranding default: `Baruwa Hosted`
- `baruwa.custom.url` - Sets the url for the product default: `http://www.baruwa.net/`

### Upgrading

Baruwa Enterprise Edition has switched from using the certificate authenticated repository to a Spacewalk managed entitlement system. In order to access the new system you need to install the Spacewalk client tools and obtain an activation key for your server entitlement.

Review the changelog for version *2.0.1* and read the updated documentation before you proceed with the upgrade.

Backup your current system:

```
tar cjvf /usr/local/src/baruwa-configs.tar.bz2 /etc/baruwa
tar cjvf /usr/local/src/baruwa-software.tar.bz2 /usr/lib/python2.6/site-packages/baruwa
```

When ready to perform the upgrade, have your activation key handy then run the following commands, replace <activation-key> with your actual activation key:

```
rpm -Uvh https://www.baruwa.com/downloads/baruwa-enterprise-release-6-2.noarch.rpm
rpm -Uvh http://yum.spacewalkproject.org/1.9/RHEL/6/x86_64/spacewalk-client-repo-1.9-1.el6.noarch.rpm
yum install rhn-client-tools rhn-check rhn-setup rhnsd m2crypto yum-rhn-plugin -y
rhnreg_ks --serverUrl=http://bn.baruwa.com/XMLRPC --activationkey=<activation-key>
```

Download and install the updated puppet toaster:

```
curl -O https://www.baruwa.com/downloads/puppet-toaster-latest.tar.bz2
tar xjvf puppet-toaster-latest.tar.bz2 -C /etc/puppet/
```

Review the new options available to the puppet manifest and add to your previous manifest, then run:

```
yum upgrade -y
rm -rf /var/lib/baruwa/data/cache/*
rm -rf /var/lib/baruwa/data/sessions/*
rm -rf /var/lib/baruwa/data/templates/*
service uwsgi restart
service baruwa restart
puppet -v /etc/puppet/manifests/toasters/baruwa/$(hostname).pp
```

If you had customized your interface, then follow the theming guidelines to create a theme that will not be overridden by your next update.

## 9.15 Changelog

### 9.15.1 2.0.8

- Implemented the SPF Checks Exemptions list to allow for exemptions of domains from SPF checks.
- Added perl functions to block abusive clients
- Updated the yum plugin to run baruwa-setup -c
- Updated documentation
- Updated Spamassassin rules location
- Silence output from updatedelta.pl
- Disconnect from PostgreSQL and Sphinx after indexing
- Disabled paster delta index updates
- FIX: Untaint ENV{PATH}
- FIX: Template bugs
- FIX: Exception in lists module
- FIX: WebApp Error Is a directory exception
- FIX: Display more accurate message status info
- FIX: Catch LXML Error: Document is empty in message preview
- FIX: Only show quarantined flag if message not delivered

- FIX: Remove preview and release buttons when message is deleted
- FIX: IOError on deleted message preview
- FIX: Ajax alert message box not being removed.
- FIX: Correct SMTP error codes information
- FIX: Exception when users attempt to release dangerous messages
- FIX: Ensured API created domains belong to correct org
- FIX: Restrict the domain creation scope to admin users
- FIX: Release SQL connections on commandline apps
- FIX: Generate initial indexes if missing
- FIX: Incorrect certificate location

### 9.15.2 2.0.7

- Implemented the `baruwa-setup` utility that automates the configuration of Baruwa Enterprise Edition systems including clustered setups.
- Implemented Content Protection functionality within the interface. This allows admins to manage File name and Mime Type block policies from within the interface. The policies can be set globally and on a per domain basis.
- Implemented MTA settings functionality within the interface. This allows admins to manage various MTA exemption lists from within the web interface.
- Implemented functionality to support [Email Address tagging](#). It is now possible to add addresses using a regex such as `username-*@domain.com` or `username+*@domain.com`. The supported delimiters are - and +. This closes issue #55
- Implemented the theme licensing checks. Templates that do not follow the [guidelines](#) will not render.
- Implemented the `list to all domains` option for domain admins, when used the listing will be functional at SMTP time just as it is with when created by a server admin.
- Implemented SMTP Error information page. This provides a more in depth error message than provided at SMTP time. SMTP server will display links to this page for the detailed error message.
- Implemented timezone awareness for Baruwa reports, reports now sent to the user at the configured time in their own timezone not the server timezone. By default reports are sent at 07H00, users in New York or Sydney will each get the report at 07H00 their own localtime.
- Implemented the `baruwa.send.reports.at` to allow configuration of the hour at which reports are sent out.
- Implemented [CDB](#) based lookup files for Exim to improve performance and to ensure mail processing continues when the DB is inaccessible.
- Implemented Site signatures which allow you to add a site signature to all mail sent out through the server regardless of the status of user or domain signatures. Can be used to add `scanned by xxx` messages
- Implemented outbound relay rate limit settings, you can use this to control the sending speed of clients to prevent DNSBL listing during spam outbreaks.
- Implemented checks to prevent DOS and Memory exhaustion attacks via large datasets in the bulk operations module such as bayesian learn of 100 messages on a system with insufficient memory. Baruwa will now check if the memory is sufficient to perform the tasks before executing them, it polls to check if memory has been released and times out after 10 checks.

- Implemented online local scores management, this allows admins to set local spam rule scores. The local scores override the default system scores.
- Added the `msgfiles` database column to store the location of a message, this speeds up message operations as the location does not have to be dynamically looked up each time. Dynamic lookups are still available to ensure that messages logged in the old format are still accessible.
- Added tooltips to icon based links to assist screen readers.
- Improved the Backup DB table creation process, the creation will only be attempted if the table does not exist. For existing tables the schema is checked and upgraded if it should be.
- Implemented progress bar for Messages bulk processing
- FIX: Quarantined files were not being cleaned up.
- FIX: celery restore\_group is not supported by this backend is now fixed
- FIX: Select all checkbox for domains and accounts search results pages
- FIX: The change report options url in quarantine reports resulted in a 403 access denied error for non admin users.
- FIX: XML formatted email messages were incorrectly handling, thus failed to display in preview.
- FIX: Quarantine email logo was not displaying due to incorrect encoding of the attachment data.
- FIX: AJAX generated dates used to show the browser timezone not the timezone configured by the user. This has been updated to ensure that the dates are generated in the users configured timezone.
- FIX: prune-database was not honouring command line options
- FIX: Added missing newlines at the end of files.
- FIX: Virus checks ruleset generation task was duplicated.
- FIX: Message totals were not being updated via AJAX.
- FIX: It is now possible to download attached email .eml messages
- FIX: Improved bulk message operations by updating code to use the new celery API with group and GroupResult
- FIX: Ensure command line tools use the correct user and group id to ensure that files are created with the correct ownership.
- FIX: It was not possible to delete multi select settings.
- FIX: Incorrect defaults were being used in settings.
- FIX: It was not possible to add multiple non SMTP-AUTH IP based relays
- FIX: Branding not being done by the JS scripts
- FIX: Encoding detection of mail records
- FIX: DOM\_RE regex incorrectly matched IP addr
- FIX: Incorrect rules being generated.

### 9.15.3 2.0.6

- Added a REST based OAUTH authenticated API
- Moved MailScanner rulesets to file based rulesets, SQL rulesets were not scaling well for very large installations.
- Added support for After SMTP Anti-Virus Checks, This per domain setting allows AV checks to be ran after accepting the message to allow for actions to be applied such as delete,deliver, quarantine.



- Implemented support for setting default language and setting the languages available for translation. This allows users to limit languages to only those they can support.
- Added support for setting spam and high spam scores and actions on outbound relays. This setting only works on outbound relays that have an IP address specified.
- Added support for Virus infected actions allowing for deliver, delete and quarantine of Virus infected messages.
- Added cache control support
- Implemented the cleanup of the AWL database table
- FIX: Prevent normal users from previewing messages that are dangerous.
- FIX: Support new domain names such as .system.
- FIX: Improve email and domain name validation.
- FIX: Improve the previewing of messages with lots of embedded CSS.
- FIX: Possible XSS in Message Preview
- FIX: Unicode decoding errors in Message Preview
- FIX: Active Directory LDAP lookups failing when there are referrals
- FIX: Incorrect MS SQL configuration options being loaded
- FIX: Domain actions were not displayed in domain search results
- FIX: Disable weekly, daily reports for users in cron as they are not supported
- FIX: Fixed the Fanout router naming
- FIX: Ensure indexer is installed for updatedelta
- FIX: Bug #49 Confirmation text longer than field
- FIX: Fixed issue with corrupt PDF reports
- FIX: Destination server connection tests caused an exception instead of returning an error when the hostname can not be resolved.
- Improved the documentation especially the manual configuration
- Added the API documentation
- Updated translations

#### 9.15.4 2.0.5

- Implemented distributed locking to enable only one cluster member to execute commands within the cluster.
- Implemented standalone search index update script for use within clusters.
- Fixed issues with LDAP attributes not being updated.
- Fixed the prune database command
- Added support for domain aliases in rulesets
- Improvements to the caching system
- Added support for the Esets and F-Secure AV engines
- Improved the display formatting of DKIM keys
- Added a description to relay settings

- Prevent normal users from downloading prohibited or infected attachments
- Various fixes and minor improvements
- Point data feeds to datafeeds.baruwa.com
- Updated documentation

### 9.15.5 2.0.4

- Moved the sphinx configuration options to MailScanner.conf, Sphinx configuration options moved from the BS.pm module into the MailScanner.conf file to simplify updating the module.
- Improved the ConfigSQL view with better ordering.
- Implemented deletion of default settings from ConfigSQL, Make sure that options are deleted from the ConfigSQL database when updated to the default value. Previously the values were left in the database.
- Implemented validation of MailScanner ConfigSQL options
- Implemented online help for Scanner settings
- Updated the forms to display online help
- Updated CSS to display help popups

### 9.15.6 2.0.3

- Fixed unicode encode error in spamassassin rules update command.
- Implemented locking to update delta command to ensure only one instance runs.
- Fixed quarantine clean command date format exception.
- Replaced old commands with their new generation versions.
- Fixed issue with fake charsets causing exceptions.
- Prevented cron.d file from being overwritten during update.
- Made improvements to authentication and authorization subsystems.
- Fixed prune quarantine command issue where customized cleanup days options were not being honored for the messages and archive tables.
- Fixed display of bayesian auto learn status, Bayes auto learn status was displayed incorrectly on the message detail page when bayes learning was disabled by the engine.
- Fixed sphinx indexing cronjobs.
- Fixed issue with incorrect attachments being downloaded when messages contain an embedded image.
- Fixed Spam rules display, preventing the “required score” from displaying as a rule.
- Fixed MailScanner config spamactions option which was not being picked up correctly.
- Fixed delivery status information, which incorrectly displayed as quarantined messages that had been deleted.
- Implemented Default theme support, which allows for global overriding of built-in appearance.
- Fixed branding issue where the logo was not being replaced with the theme version. Closes issue #19
- Implemented a configurable DKIM selector. Closes issue #17. A new option `baruwa.dkim.selector` introduced to allow configuration of the DKIM selector.

- Fixed Error when adding address to approved/banned senders using an alias domain. Closes issue #20
- Made default settings match supplied mailscanner configuration file. Closes issue #17.
- Fixed Information Header Value not applying. Closes issue #13
- Implemented the Blue lagoon theme as base template, this is built using responsive design which scales to display on all device sizes.
- Updated the translations.
- Updated the documentation.

### **9.15.7 2.0.2**

- Fixed taskid session checks, which caused an exception when the session attribute did not exist.
- Fixed issue with headers which can not be decoded leading to exceptions
- Fixed issue with empty values breaking quarantine messages due to attempt to concat strings with None values.
- Added checks to prevent the creation of duplicate user accounts from external authentication mechanisms due to the case being different.
- Fixed the deletion of relay settings, which was causing an exception.
- Fixed accounts navigation issue, when paging using AJAX.
- Added support for custom logos in PDF reports, fixes issue #14.
- Fixed incorrect memory usage percentages in the status page.
- Improve daily totals calculation, it now supports users timezone settings.
- Fixed an exception with the Psutil backend which was not being caught.
- Added organization filters to the quarantine and pdf reports commands.
- Improvements to lost password handing, restrict requests to local users and fix the reset url.
- Added a top spammers generation command which can be used to export data to external or internal blacklists.
- Added a top clean senders generation command which can be used to export data to external or internal whitelists.
- Improvements to display all dates and times in users own timezone.
- Implemented JSON data exports to support JSON driven charts and graphs.
- Improvements to the search functions error handling.
- Improvements to the external authentication modules.
- Improvements to the message preview functionality, now able to display both the text and HTML alternatives of an email. HTML messages formatted correctly using embedded CSS styles which are sanitized.
- Added support for duplicate message id's which are generated on high mail volume installations.
- Various minor code cleanups and fixes.
- Updates to the documentation.

### **9.15.8 2.0.1**

- Fixed domains information leak when logged in as domain admin. Domain admins were able to see domains belonging to other users in the drop down menu under edit or delete accounts.
- Added support for theming and customization. Included are support for Interface, email, reports customization as well as productization with a custom name.
- Added support for shared quarantines on shared storage which allows messages to be accessed even when the node that processed them is offline.
- Implemented full cluster functionality for all components
- Improvements to Active Directory / LDAP including support for address verification of alias domain accounts, import of aliases from LDAP servers that use the mail attribute such as OpenLDAP, fix case sensitivity issue with Active Directory servers.
- Fixed MailScanner SQL config keyword issue.
- Fixed duplicates of account listings when user belonged to more than one domain
- Fixed various issues that caused quarantine reports not to be sent to some user accounts.
- Fixed auto user logout when they delete their account.
- Improve the predicate matching system for authorization of actions.
- Fixed previewing of embedded images in emails.
- Fixed the searching of archives when did not display the actual messages found.
- Fixed signature processing on the nodes after configuration in the interface.
- Added experimental PDF reporting command with theme support
- Added experimental Quarantine reporting command with theme support
- Fix to various cronjobs like the ones pruning database tables.
- Disabled NJABL
- Updated translations

### **9.15.9 2.0.0**

- Initial release

## 10.1 Signing In and Signing Out

### 10.1.1 Signing In

To sign in to Baruwa, you enter your username and password and select the language to use if the auto detected language is not the one you prefer to use.

If you are signing in using external authentication such as your AD/LDAP or IMAP credentials then you need to provide the full username with the domain part included.

Your session will automatically timeout after 8 hours and you will have to login again.

### 10.1.2 Signing Out

To sign out click the Logout link on the top right corner of your screen.

Your session will automatically timeout after 8 hours and you will have to login again.

## 10.2 Changing Your Password

You can change your password if your account is setup to use local (internal) authentication.

If your account uses external authentication then use the system hosting your account credentials to change them.

### 10.2.1 Change a Known Password

While logged in.

1. Go to the Account page.
2. Click Change Password.
3. Enter your new password twice then your old password.
4. Click the Change Password button.

## 10.2.2 Reset a Forgotten Password

At the login page.

1. Click `Forgotten password ?`
2. Enter your email address, Click the `Reset my password Button`
3. Check your email, follow the instructions in the email

## 10.3 Personalizing Your Account

You can personalize various settings of your account using the account page.

### 10.3.1 Account names

You can change the First and Last name used to address you in any correspondence from Baruwa.

1. Go to the `Account page`
2. Click `Update Account`
3. Enter `First name and Last name`
4. Click the `Update account button`

### 10.3.2 Change Your Default Time Zone

By default your account uses the time zone setup for your domain by your domain administrator.

This option allows you change the time zone, All times in the Baruwa interface will be displayed in this time zone.

1. Go to the `Account page`
2. Click `Update Account`
3. In the `Timezone drop-down menu` select the time zone you want to use.
4. Click the `Update account button`

### 10.3.3 Enable or Disable reports

You can enable or disable reports using this option. Reports include your daily quarantine report and a monthly usage report.

1. Go to the `Account page`
2. Click `Update Account`
3. In the `Send reports checkbox`, select to enable, deselect to disable
4. Click the `Update account button`

### 10.3.4 Enable or Disable Spam Checks

You can choose to enable or disable Spam checks on messages destined to your account.

1. Go to the `Account` page
2. Click `Update Account`
3. In the `Enable spam checks` checkbox, select to enable, deselect to disable
4. Click the `Update account` button

### 10.3.5 Customize Spam scores

You can customize the scores at which messages are determined to be either Spam or definite Spam.

---

**Note:**

- The `Spam High score` must be higher than the `Spam low score`
  - Setting `0.0` makes Baruwa use the Domain or system defaults.
- 

1. Go to the `Account` page
2. Click `Update Account`
3. In the `Spam low score` or `Spam high score` input, enter the score
4. Click the `Update account` button

### 10.3.6 Add Email signatures/Disclaimers

Baruwa can manage email signatures / disclaimers that are added to messages that are sent outbound through it. Both HTML and Text signatures are supported. HTML signatures support a single embedded image.

A WYSIWG Editor is used to setup the HTML signatures and it allows you to upload images that you can embed in your HTML signature.

1. Go to the `Account` page
2. Click `Add signature`
3. Select `Signature type` from the drop down
4. Enter signature content
5. Ensure the `Enabled` checkbox is checked
6. Click the `Add signature` button

## 10.4 Messages

### 10.4.1 Most Recent Messages

When you login the default view you see is the most recent messages for your account. By default the latest 50 messages are shown.

If you want to change the number of recent messages displayed you can use the drop down select `Show: items per page` to do that.

The selected number will be displayed during your current session, when you logout the number will reset to 50.

### 10.4.2 Full message listing

If you want to see more then the most recent messages you should,

1. Mouse over `Messages`
2. Click `Full message list`
3. Use the pagination links to see more messages.

### 10.4.3 Quarantine

If you want to see only quarantined messages,

1. Mouse over `Messages`
2. Click `Quarantine`
3. Use the pagination links to see more messages.

You can carry out message operations on several messages from within this view. Refer to *Bulk Message Operations* for details.

### 10.4.4 Archived messages

If you want to see older archived messages,

1. Mouse over `Messages`
2. Click `Archive`
3. Use the pagination links to see more messages.

### 10.4.5 Message Details

If you want to see the details of any specific message click the link to the message.

The following information is available.

- Message ID
- From Address
- To Address
- Subject
- Received date and time (Displayed in your timezone)
- Received by server (The server that received the message)
- Received from (The server that sent the message)
- Received via (Servers that processed this message, includes country information)
- Size
- Message headers



- Quarantined
- Virus infected
- Prohibited file
- Other infection
- Spam checks information (Spam check results and rules used to make determination)
- Delivery information (Status of mail delivery to final destination)

If the message is quarantined you are able to preview, release, learn or delete the message. Refer to *Message operations* on how to do this.

You are also able to add the sender to an authorized or banned sender list from with this view using email address, domain name or IP address. Refer to *To add the sender to a list* on how to do this.

## 10.4.6 Message operations

The Baruwa interface allows you to preview, release, learn or delete quarantined messages and authorize or ban senders of messages using email address, domain name or IP address.

### Previewing a quarantined message

To preview a quarantined message,

1. Click the message link
2. Click Preview message
3. Click Attachments to download any attachments
4. Click Display images to display any remote images (This is not advisable)

### Releasing a quarantined message

To release a quarantined message,

---

**Note:** Released messages are not removed from the quarantine, if you want to remove a message from the quarantine, you need to delete it. Messages are automatically deleted from the quarantine at an interval that is set by the system administrator. The default interval is 30 days.

---

1. Click the message link
2. Click Release message
3. Check Release checkbox
4. Enter Alt recipients if you want to send the message to another email address
5. Click the Submit Button

### Bayesian learning a message

You can update the Bayes system by teaching it if a message is Spam or Not Spam.

1. Click the message link

2. Go to the bottom of the page
3. Check `Bayesian Learn` checkbox
4. Select `Spam` or `Clean` from the drop down
5. Click the `Submit Button`

### Deleting a quarantined message

You can delete a message from the quarantine.

1. Click the message link
2. Go to the bottom of the page
3. Check `Delete` checkbox
4. Click the `Submit Button`

### 10.4.7 To add the sender to a list

1. Click `Add sender to list`
2. Select the type of list you want to add them to using the `List type` drop down
3. Check `Add to aliases as well` if you want it to apply to your aliases as well
4. Check `Use IP address to use the IP address`
5. Check `Use Domain to list the whole domain`
6. Click the `Add to list button`

### 10.4.8 Bulk Message Operations

It is possible to carry out message operations (release, learn or delete) on multiple messages at ago.

To do this.

1. Select the messages using the check box
2. Select the operations (release, learn or delete) at the top
3. Click the `Process` button
4. View the operations results

### 10.4.9 Filters

Message filters are available on the *Full message listing*, *Quarantine* and *Archived messages* pages.

Refer to *Manage Filters* on how to manage these filters.

## 10.5 Approved and Banned Sender Lists

Baruwa supports the use of Approved and Banned sender lists.

Addresses on your approved sender list will skip all spam checks allowing their emails to always get delivered to you.

Addresses on your banned sender list will have their messages to you rejected.

### 10.5.1 Adding addresses to lists

1. Mouse over `Lists`
2. Click `Add to List`
3. Enter the address can be an `Email Address`, `Domain Name` or `IP address`
4. Select the list type from the `List type` drop down menu
5. Check `Add to aliases` as well if you want it added to your aliases
6. Click the `Add to list` button

### 10.5.2 Deleting addresses from lists

1. Mouse over `Lists`
2. Click either `Approved senders` or `Banned senders`
3. Find the address
4. Click the red `x` under the action column

## 10.6 Reports

The reports view allows you to run a set of predefined reports. The following reports are available.

### 10.6.1 Available reports

- Top Senders by Quantity
- Top Senders by Volume
- Top Sender Domains by Quantity
- Top Sender Domains by Volume
- Spam Score Distribution
- Top Mail hosts
- Top Recipients by Quantity
- Top Recipients by Volume
- Message Totals

You can use `filters` to filter the results available in your report. These `filters` can be saved for later reuse. Refer to *Manage Filters* for details.

Reports are exportable, and can be exported as PDF or CSV. Refer to *Export report* for details on how to export a report.

## 10.6.2 Export report

### Export report to PDF

1. Click report link
2. Click `Download PDF`

### Export report to CSV

1. Click report link
2. Click `Download CSV`

## 10.6.3 Manage Filters

A filter rule consists of one message property and one condition. If the message matches the property and condition it is selected.

### Filter properties

The following properties are available to filter messages on.

- Message ID
- Message size
- From Address
- From Domain
- To Address
- To Domain
- Subject
- Received from
- Was scanned
- Is Spam
- Is Definite spam
- Is RBL listed
- Is approved sender
- Is banned sender
- Spam score
- Spam report

- Is virus infected
- Is name infected
- Is other infected
- Date
- Time
- Headers
- Is quarantined
- Processed by host

### Filter conditions

Different properties support different conditions. The conditions supported by a specific property will automatically be selected when you select the property.

The following conditions are available.

- is equal to
- is not equal to
- is greater than
- is less than
- contains
- does not contain
- matches regex
- does not match regex
- is null
- is not null
- is true
- is false

### Setting Up Filter Rules

1. Go to the `Reports` page Or within the *Full message listing*, *Quarantine* and *Archived messages* pages.
2. Select the property from the first drop down menu
3. Select the condition
4. Enter condition text if the condition requires one
5. Click `Add filter`

## Saving Filter Rules

1. Go to the `Reports` page
2. Select the filter rule under `Active Filter(s)`
3. Click `Save`

## Deleting a saved Filter Rule

1. Go to the `Reports` page
2. Select the filter rule under `Saved Filter(s)`
3. Click `Delete`

## 10.7 Mail queues

Messages that are yet to be processed are kept in the `inbound` queue, messages that have been processed but are yet to be delivered are kept in the `outbound` queue.

The status of both the `inbound` and `outbound` mail queues is provided. The following actions can be performed on messages that are in the queues:

- `Delivery`
- `Bounce`
- `Hold`
- `Delete`
- `Preview`

You can access these mail queues by clicking the numbers next to `In :` and `Out :` at the top of your screen

### 10.7.1 Processing queued messages

#### Deliver a message in the outbound queue

Delivery only applies to messages that have already been processed by Baruwa, that is why only messages in the `outbound` queue can be delivered.

To deliver a message:

1. Click the number next to `Out :` at the top of your screen
2. Select the message
3. Scroll to the bottom of the screen
4. Select `Deliver`
5. Click the `Process` button

---

**Note:** Delivery is only possible if the destination server is up and accepting mail.

---

### Delete a queued message

1. Click the number next to `In :` or `Out :` at the top of your screen
2. Select the message
3. Scroll to the bottom of the screen
4. Select `Delete`
5. Click the `Process` button

### Bounce a queued message

1. Click the number next to `In :` or `Out :` at the top of your screen
2. Select the message
3. Scroll to the bottom of the screen
4. Select `Bounce`
5. Click the `Process` button

### Hold a queued message

1. Click the number next to `Out :` at the top of your screen
2. Select the message
3. Scroll to the bottom of the screen
4. Select `Hold`
5. Click the `Process` button

### Preview a queued message

1. Click the number next to `In :` or `Out :` at the top of your screen
2. Select the message
3. Click `Preview message`

## 10.8 Baruwa Search Tips and Tricks

Baruwa supports many of the search tricks you use in popular web search engines.

### 10.8.1 Search with an exact phrase

To search for an exact phrase enclose the phrase in quotes `"Blocked message"`

### 10.8.2 Search for one or other

Use the pipe character `|` to separate the phrases `"Barrack Obama" | "Mike Tyson"`

### 10.8.3 Search using a wildcard

Use the star character `*` For example `boy*` will match `boy`, `boyfriend`

### 10.8.4 Search using the negate operator

`shaken !stirred` or `shaken -stirred` will match phrases with `shaken` but not `shaken stirred`

### 10.8.5 Search using grouping

`(red | green | blue) car` will match `red car`, `green car` or `blue car`

### 10.8.6 Search Specific fields

---

**Note:** It is also possible to limit your search to specific fields, the field operators will be provided later.

---



## 11.1 Free support

Email only support is available via the Enterprise edition support email address `enterprise-support (AT) baruwa.com`.

A mailing [list](#) also exists where you can discuss Enterprise edition related issues as well as ask for help and advise from fellow subscribers. The developers subscribe to and actively monitor this list.

## 11.2 Paid for support

Paid for support and consultancy services are available. All hands on or On device support which includes troubleshooting, investigation and resolution is only provided under paid for support.

Prepayment of an initial support fee is required before any hands on support tasks are carried out.

To request for paid support or to obtain our rate card, please email `enterprise (AT) baruwa.com`.



## PREVIOUS DOCUMENTATION

The documentation for previous versions is available using at the following locations

- [2.0.7](#)
- [2.0.6](#)
- [2.0.5](#)
- [2.0.4](#)