Baruwa Enterprise Edition Documentation

Release 2.1.7

Andrew Colin Kissa

Jul 23, 2018

CONTENTS

1 What is Baruwa Enterprise Edition **3**
- 1.1 How does it work . . . 3
- 1.2 Features . . . 4
- 1.3 Subscriptions . . . 5
- 1.4 System Requirements . . . 5
- 1.5 Topologies . . . 5

2 Feature List **9**
- 2.1 System Features . . . 9
- 2.2 Management and Reporting . . . 9
- 2.3 High Availability . . . 10
- 2.4 Antispam, AntiSpam, Malware Protection . . . 10
- 2.5 Subscriptions . . . 11
- 2.6 Customer Support . . . 11

3 Obtaining Baruwa Enterprise Edition **13**
- 3.1 Download ISO image . . . 13
- 3.2 Making an Installation CD/DVD . . . 13

4 Planning for Installation **15**
- 4.1 Required Skills . . . 15
- 4.2 Hardware Compatibility . . . 15
- 4.3 Supported Installation Hardware . . . 15
- 4.4 RAID and Other Disk Devices . . . 16
- 4.5 Network Firewall . . . 17
- 4.6 DNS . . . 18
- 4.7 Hostnames . . . 19
- 4.8 Clustering . . . 19
- 4.9 System Profiles . . . 19

5 On Premise Installation **23**
- 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 . . . 33
- 5.6 Configuration . . . 37

6 Cloud Installation **39**
- 6.1 Overview . . . 39
- 6.2 Installation . . . 40

6.3 Configuration . . . 43

7 Configuration **45**
7.1 StandAlone System . . . 45
7.2 Automated Configuration . . . 45
7.3 Post Configuration . . . 63

8 Cluster Configuration **65**
8.1 Backend System . . . 65
8.2 Database System . . . 85
8.3 Search Index System . . . 106
8.4 Message Queue System . . . 110
8.5 Cache System . . . 114
8.6 Web and Mail System . . . 118
8.7 Mail System . . . 129
8.8 Web Interface System . . . 140

9 Advanced configuration **151**
9.1 Content Protection . . . 151
9.2 External Authentication . . . 152
9.3 Clustering . . . 153
9.4 Customization . . . 156
9.5 Addons . . . 159
9.6 Additional Anti Virus Engines . . . 159
9.7 Themes . . . 167
9.8 Baruwa API . . . 169
9.9 Email Protection Best Practices . . . 171

10 Administrators guide **173**
10.1 Managing Organizations . . . 173
10.2 Managing Domains . . . 179
10.3 Managing Accounts . . . 188
10.4 Managing API Applications . . . 192
10.5 Managing Settings . . . 193
10.6 System Status . . . 211
10.7 Command line Reference . . . 213
10.8 Scheduled commands . . . 216
10.9 Baruwa Backups . . . 217
10.10 Monitoring . . . 218
10.11 Baruwa log files . . . 220
10.12 Languages supported . . . 221
10.13 YAML Import File format . . . 222
10.14 Man Pages . . . 229
10.15 Frequently Asked Questions . . . 237
10.16 Release Notes . . . 243
10.17 Upgrading . . . 261
10.18 Changelogs . . . 287

11 User guide **303**
11.1 Signing In and Signing Out . . . 303
11.2 Changing Your Password . . . 303
11.3 Personalizing Your Account . . . 304
11.4 Messages . . . 305
11.5 Approved and Banned Sender Lists . . . 309
11.6 Reports . . . 309

11.7 Mail queues . . . 312
11.8 Baruwa Search Tips and Tricks . . . 313

12 Support **315**
12.1 Bundled support . . . 315
12.2 Paid support . . . 315
12.3 Support Package Matrix . . . 315

13 Previous Documentation **317**

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

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 with several *API Libraries* are provided to ensure the efficient and easy management of the System. You can even craft your own Infrastructure as Code deployment solution using SaltStack and our packaged salt states.

CHAPTER

ONE

WHAT IS BARUWA ENTERPRISE EDITION

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

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 with several *API Libraries* are provided to ensure the efficient and easy management of the System. You can even craft your own Infrastructure as Code deployment solution using SaltStack and our packaged salt states.

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 and runs on a slimmed down and customized Linux OS based on CentOS. All the bloat has been trimmed leaving only an OS dedicated to email security.

Baruwa Enterprise Edition can be installed on Premise or in the cloud.

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. Clusters are made up of frontend and backend segments. In the frontend segment 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. Backend segment clustering was introduced in version 2.1.7.

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
- DMARC Checks and Reporting
- Reporting graphs
- Emailed PDF reports
- Audit trails
- Archiving of old message logs
- Multi Tenancy
- IP / network addresses supported in approved/banned list manager
- System status information
- IPv6 Support
- Import and Export of User accounts and Domains
- AD/Exchange integration to auto populate account and group information
- TOTP OTP Two Factor Authentication
- Easy plug-in authentication to external authentication systems
- AD/LDAP, POP3, IMAP, SMTP, RADIUS, SAML2 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.
- Free Certbot/Lets Encrypt TLS/SSL certificates
- Email Address tagging support

A full feature list is available at *Feature List*

1.3 Subscriptions

Baruwa Enterprise Edition is available under a `PAID` subscription, subscriptions can be paid for monthly or annually.

There are `NO` restrictions or limitations on the number of domains, email addresses and users that you can configure on your systems. You are only limited by the system resources on your hardware. Unlike competing products we do not charge based on the number of domains or users.

Subscription are purchased via the Baruwa website, using PayPal or PayFast. The order system is automated, as soon as PayPal/PayFast processes the payment and notifies our system your subscription will be generated and the subscription details emailed to you. This should take no more than 5 minutes. If you do not receive email confirmation of your subscription within 15 minutes please contact *Support*.

1.3.1 Trial Subscriptions

30 day Trial subscriptions can be obtained via the Baruwa website, a valid PayPal/PayFast account is required to access the Trial subscription. There is no obligation and the Trial can be cancelled at any point within the 30 Days.

Refer to *Why do you require a PayPal/PayFast account for the 30 day Trial ?* for the reason why a valid PayPal/PayFast account is required.

1.4 System Requirements

- Intel/AMD 2.0 GHZ+ 64-bit CPU
- Minimum - 6 GB RAM
- 12 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.

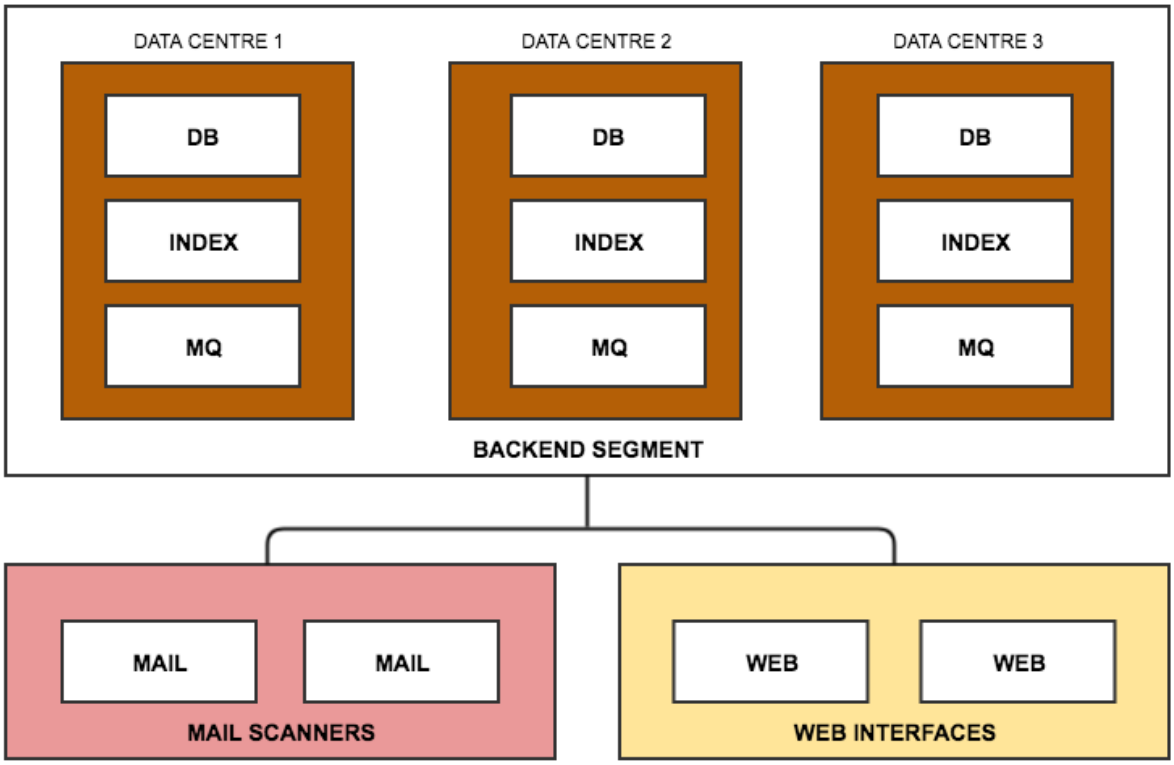
1.5 Topologies

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.

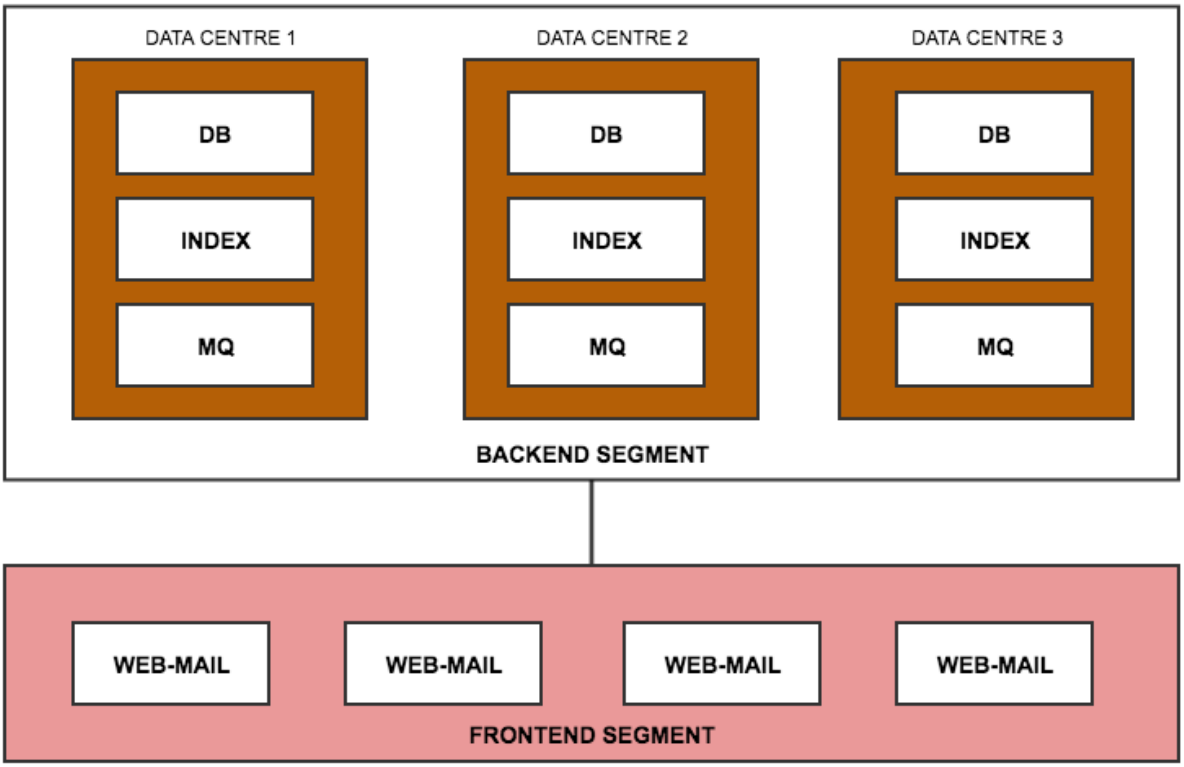
1.5.1 Distributed Backend Distributed Frontend

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.



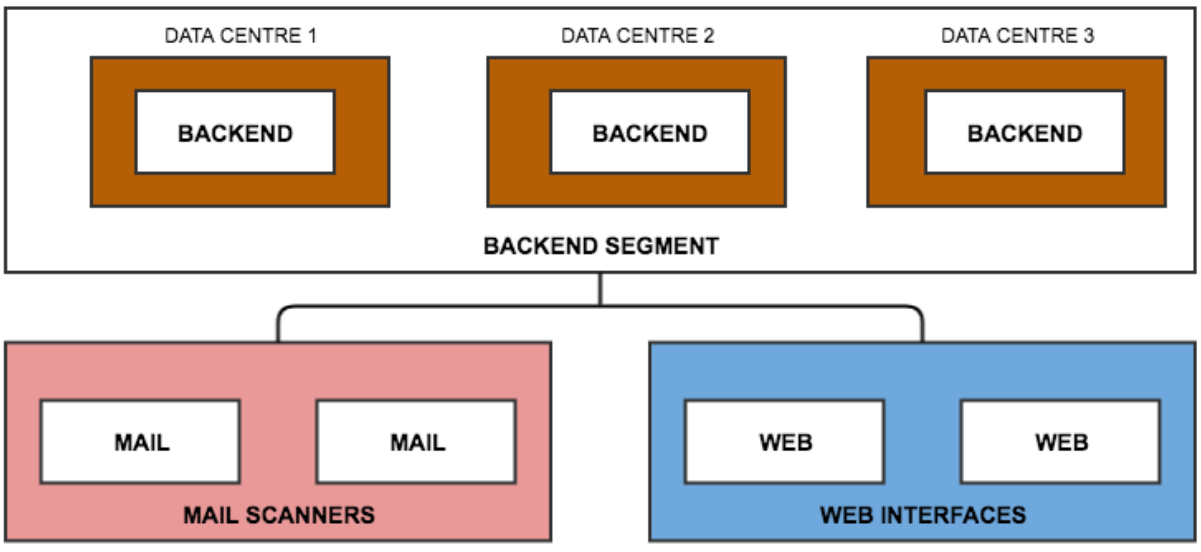
1.5.2 Distributed Backend Hybrid Frontend

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 growing the frontend or backend cluster segments.



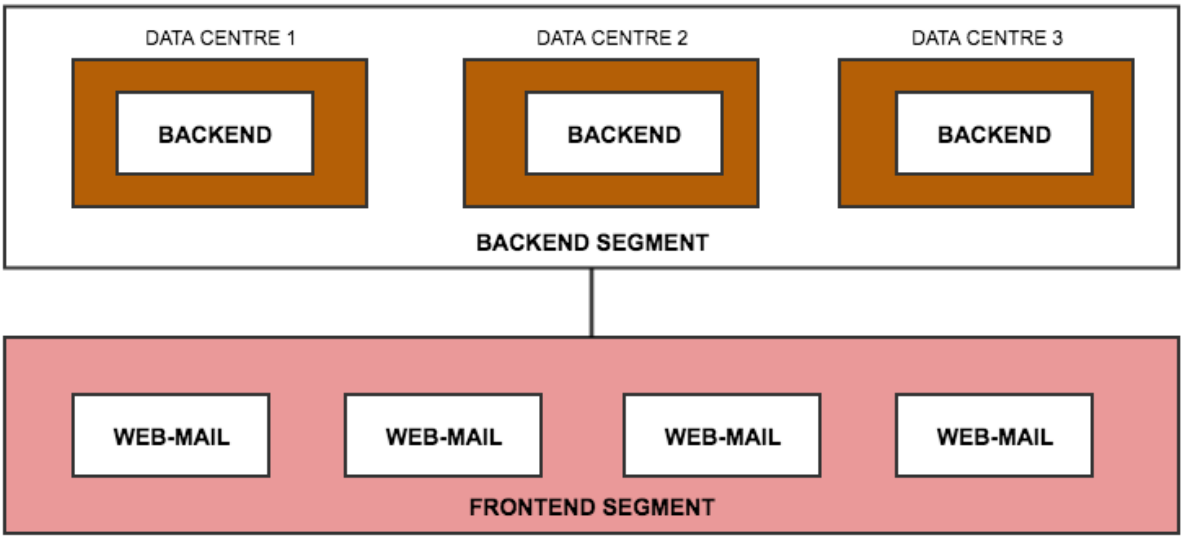
1.5.3 Single Backend Distributed Frontend

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 growing the frontend or backend cluster segments.



1.5.4 Single Backend Hybrid Frontend

In this topology all backend components are installed on a single system in and the frontend components are combined on to a node. Scaling is achieved by growing the frontend or backend cluster segments.



CHAPTER

TWO

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

- Multi Tenancy
- Per Domain policies
- Mail Queue Management
- Multiple Language Support
- Customized Linux based OS
- SMTP Authentication Support
- Ultra fast full text search
- Themes/Skins for rebranding
- IPv6 and IPv4 Address Support
- Email Address tagging support
- Extensive Spam Detection checks
- Random IP address pools support
- Inbound and Outbound protection
- AJAX support for most UI operations
- Dedicated customer IP address assignment
- Spam, Virus, Phishing, Malware protection
- Free Certbot/Lets Encrypt TLS/SSL certificates
- TOTP OTP Two Factor Authentication
- AD/LDAP, POP3, IMAP, SMTP, RADIUS, SAML2 Authentication support

2.2 Management and Reporting

- Audit trails

- DMARC Reports
- DKIM management
- Reporting graphs
- REST OAUTH based API
- External Syslog support
- System status information
- Themes/Skins for rebranding
- NRPE and SNMP v3 Monitoring
- Advanced Setup Wizard Utilty
- Signature management / Branding
- Message delivery/relay information
- Mail queue management and reporting
- Reporting with AJAX enabled query builder
- Import and Export of User accounts and Domains
- Centralized Quarantine for large scale cluster deployments
- Easy plug-in authentication to external authentication systems

2.3 High Availability

- Shared Quarantine
- No Master clustering
- Active-Active clustering
- Quarantine syncronization
- Easy clustering of multiple servers
- Node Failure Detection and Notification
- Split Read/Write Database operations
- Automated Master/Slave failover

2.4 Antispam, AntiSpam, Malware Protection

- URL Filtering
- Rate limiting
- Archive Scanning
- Malware Detection
- Content Protection
- Reverse DNS Checks
- Email Header Inspection

- Local Sender Reputation
- SPF, DKIM, DMARC, DANE, IDNA
- Spam URI and Real-Time Lists
- Forged Sender Address Checks
- Denial of service protection
- Bayesian Statistical Analysis
- Baruwa Datafeeds reputation services
- Anti-Virus with Spam and Malware signatures
- Quarantine with end user reporting and notification
- Approved/Banned Lists at Global, Domain, and User levels

2.5 Subscriptions

- Competitive pricing
- Easy to understand pricing structure
- No limitations on number of domains or users

2.6 Customer Support

- Remote monitoring services
- On device support available
- Design and consulting services
- 24x7 Support packages available
- Responsive and knowledgeable support team
- SLA / System maintenance contacts available.
- Active Development and Updates release circles
- Free standard email support as part of subscription
- Continuous Research and Development to cope with new threats

CHAPTER

THREE

OBTAINING BARUWA ENTERPRISE EDITION

Note: If you intend on setting up your Baruwa Enterprise Edition server on a supported cloud platform then you do not have to download the installation media. Information on installing to a cloud server can be found in the *Cloud Installation* section.

If you have a Baruwa Enterprise Edition subscription, you can download ISO image files of the Baruwa Enterprise Edition 6.10 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 6.10 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 6.10 directory then click Baruwa-6.10.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 enviroments.

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.

CHAPTER

FOUR

PLANNING FOR INSTALLATION

4.1 Required Skills

To install and manage Baruwa Enterprise Edition you need to have basic Linux command line skills such as the ability to login via SSH or console and run commands, interpret command output, check log files etc.

Baruwa Enterprise Edition is RPM based, so you also require working knowledge of Redhat-like specific commands such as `rpm`, `chkconfig`, etc.

To configure Baruwa Enterprise Edition, you need to have an understanding of how internet email works, how email is routed and the various protocols in use.

If you do not possess the required skills you can purchase installation support and or ongoing maintanance support, contact *Support* to do so.

4.2 Hardware Compatibility

Hardware compatibility is particularly important if you have an older system or a system that you built yourself. Baruwa Enterprise Edition 6.10 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 6.10 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.

4.3 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.

4.3.1 Minimum and Recommended Hardware

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

- 6GB RAM
- Multicore Intel/AMD 64-bit CPU
- 12 GB OS
- 10 GB Data

The recommended system requirements for all in one system are:

- 8GB RAM
- Multicore Intel/AMD 64-bit CPU
- 12 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.

4.4 RAID and Other Disk Devices

Baruwa Enterprise Edition 6.10 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 6.10. 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.

4.4.1 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.

4.4.2 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.

4.4.3 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
/boot/efi	200MB	VFAT	EFI Partition
/boot	500MB	EXT4	BOOT Partition
/	10GB	EXT4	Root Partition
Swap	3GB		Max size 3GB
/var		XFS	Rest of the disk.

If you would like to setup `software RAID`, `LVM` or use `SAN storage`, you should use the expert mode.

4.4.4 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 by manually partitioning the system.

4.5 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
6277	UDP	OUTBOUND	DCC TRAFFIC
873	TCP/UDP	OUTBOUND	UPDATES TRAFFIC
11211	UDP	BETWEEN NODES	CACHE SYNC TRAFFIC
3542	UDP	BETWEEN NODES	CLUSTER TRAFFIC
4369	TCP	BETWEEN NODES	AMQP TRAFFIC
25672	TCP	BETWEEN NODES	OTP TRAFFIC
5672	TCP	BETWEEN NODES	AMQP TRAFFIC
5432	TCP	BETWEEN NODES	DB TRAFFIC
6432	TCP	BETWEEN NODES	DB TRAFFIC
9306	TCP	BETWEEN NODES	SEARCH QUERY TRAFFIC
8300	TCP	BETWEEN NODES	CLUSTER TRAFFIC
8500	TCP	BETWEEN NODES	CLUSTER TRAFFIC
8301	TCP/UDP	BETWEEN NODES	CLUSTER TRAFFIC
8302	TCP/UDP	BETWEEN NODES	CLUSTER TRAFFIC

4.6 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 on systems configured using the `Standalone System`, `Web and Mail System` and `Mail System` profiles.

This local caching server is independent of your other DNS systems and resolves from the DNS 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/unbound/conf.d/local.conf` file, if you have any private address reverse zones you need to configure entries for these in `/etc/unbound/local.d/local.conf` and then restart the `unbound` 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.

Warning: The use of public DNS servers such as Google, OpenDNS or your ISP's name servers is not supported as these servers will be blocked/throttled by URIBL and DNSBL servers thus leading to poor performance of your system. Our Datafeeds system only accepts DNS requests from the IP address of the system running Baruwa.

The use of your own DNS infrastructure is no longer supported, do not forward all queries to your own DNS infrastructure only forward requests for your internal zones. Add the internal zones to be forwarded to `/etc/unbound/conf.d/local.conf`

Note: After setting up your server ensure that the only entry in /etc/resolv.conf points to 127.0.0.1. You also need to make sure that your firewall or ISP is not redirecting DNS queries to their own infrastructure.

4.6.1 Testing DNS

To test that your server is correctly resolving DNS requries use the following command.

```
host -t txt 2.0.0.127.test.rbl.baruwa.net.
```

You should get the following response if it is working correctly.:

```
2.0.0.127.test.rbl.baruwa.net descriptive text "The DNS checks working correctly"
```

If you do not get the above response after setup then your DNS is not resolving correctly, you need to fix that before putting the system into production.

4.7 Hostnames

When choosing the hostnames for your web and mail services be careful to choose a well established TLD.

It is recommended you not choose the new GTLDs which were recently introduced. Most of these new GTLD's have a bad reputation and are constantly blocked by spam filters.

4.8 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 the distributed backend is:

1. Database Systems
2. Search Index Systems
3. Message Queue Systems
4. Cache Systems [Optional]
5. Nodes

The recommended installation order for the single Backend is:

1. Backend Systems
2. Nodes

The first system that you setup should be configured as a *Bootstrap server*.

4.9 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.

4.9.1 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.

4.9.2 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 [Optional]

This profile is used in the *Single Backend Distributed Frontend* and *Single Backend Hybrid Frontend* topologies.

Servers setup using this profile can be setup as a *Bootstrap server*.

4.9.3 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.

This profile is used in the *Distributed Backend Hybrid Frontend* and *Single Backend Hybrid Frontend* topologies.

4.9.4 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Single Backend Distributed Frontend* topologies.

4.9.5 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Single Backend Distributed Frontend* topologies.

4.9.6 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

4.9.7 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

Servers setup using this profile can be setup as a *Bootstrap server*.

4.9.8 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

4.9.9 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

4.9.10 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.

CHAPTER

FIVE

ON PREMISE INSTALLATION

Note: This section describes a new on premise installation, if you are upgrading from an older version please refer to the *Upgrading* section. If you would like to install to a cloud provider then refer to the *Cloud Installation* 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.

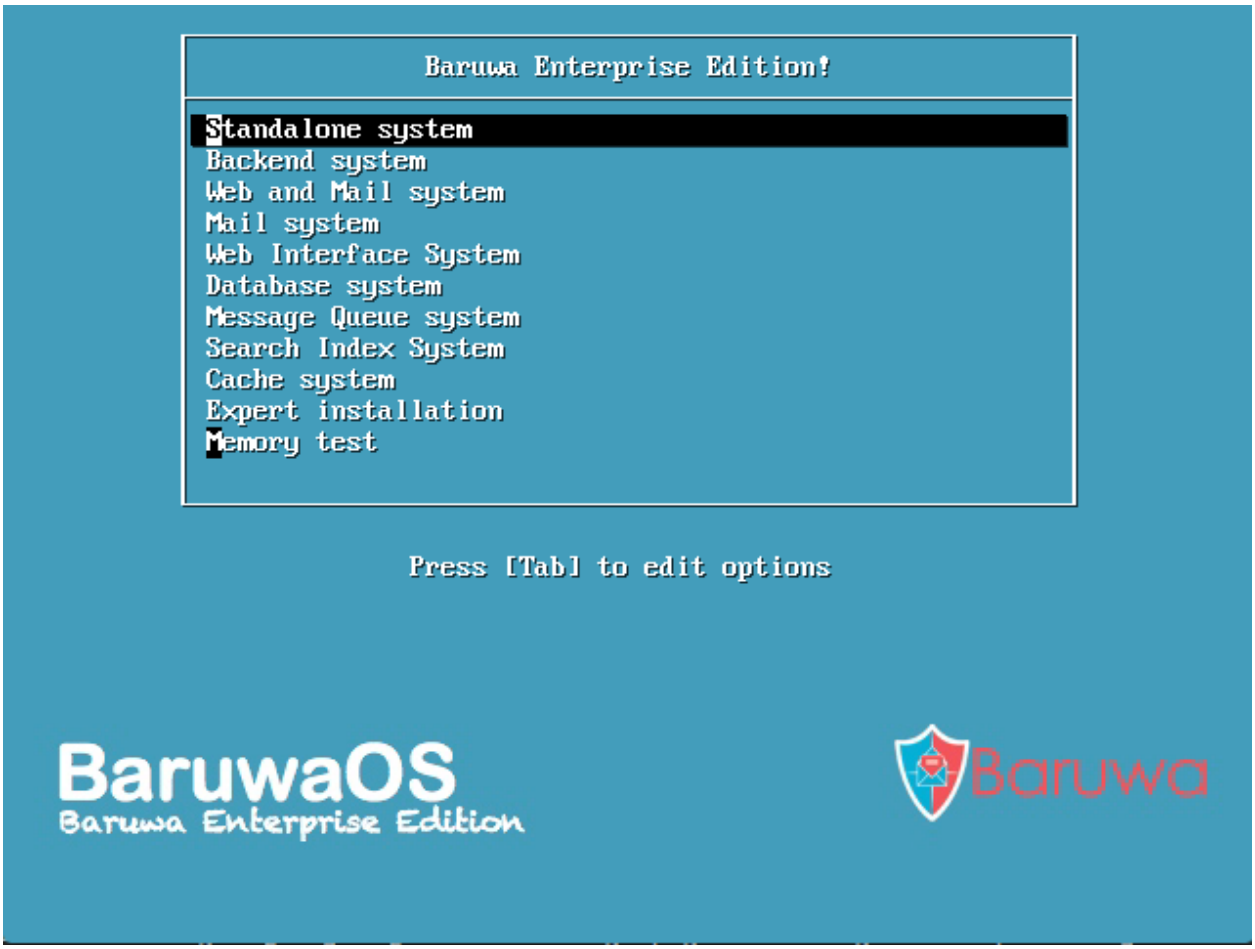
The installation program then probes your system and attempts to identify your DVD drive. It starts by looking for an IDE (also known as an ATAPI) DVD drive.

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*

Warning: Make sure you choose the correct profile in the boot menu.

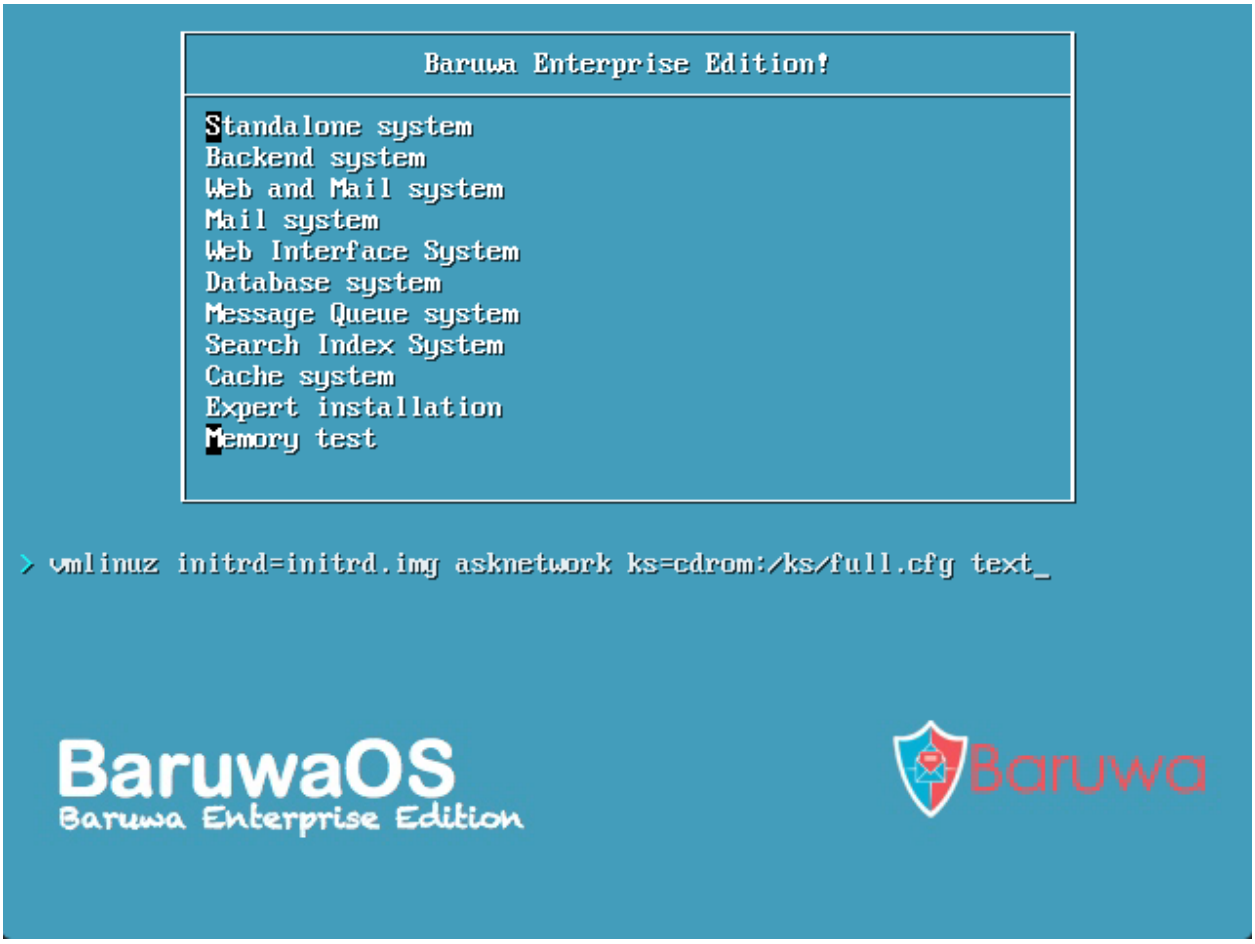
5.2.1 Additional Boot Options

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

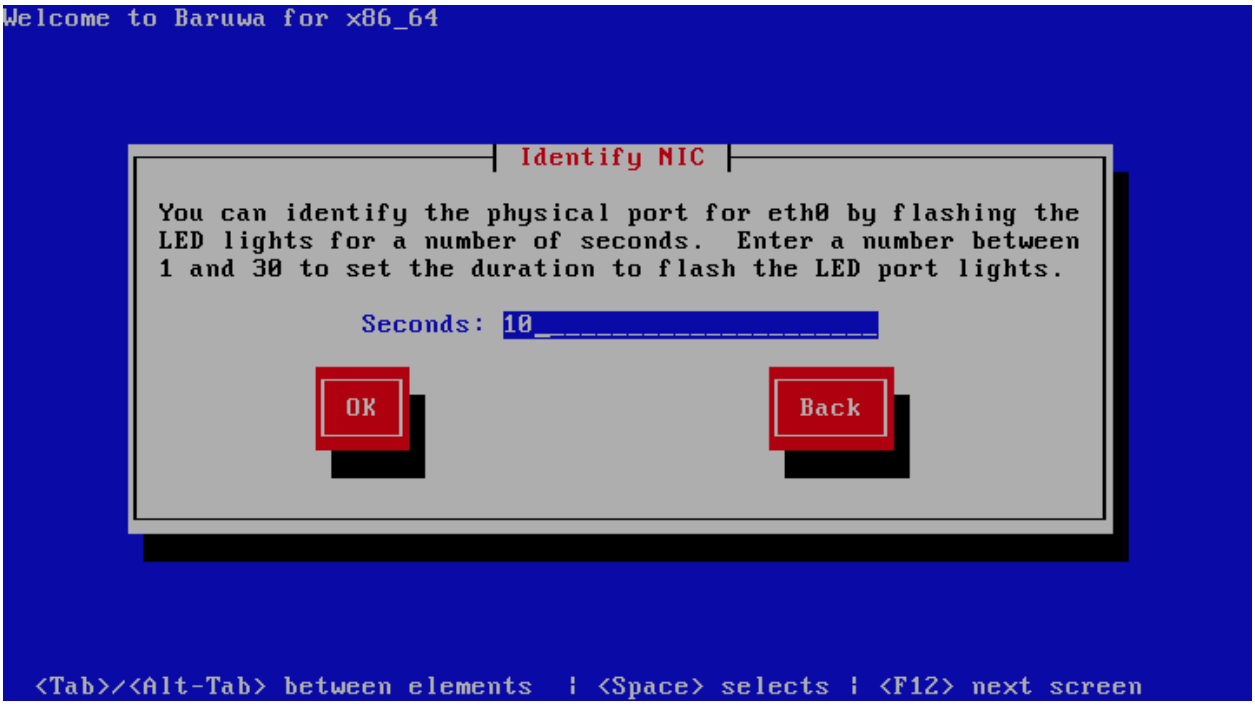
The DVD offers an option to verify the integrity of the media. Recording errors sometimes occur while producing DVD media. An error in the data for package chosen in the installation program can cause the installation to abort. To minimize the chances of data errors affecting the installation, verify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

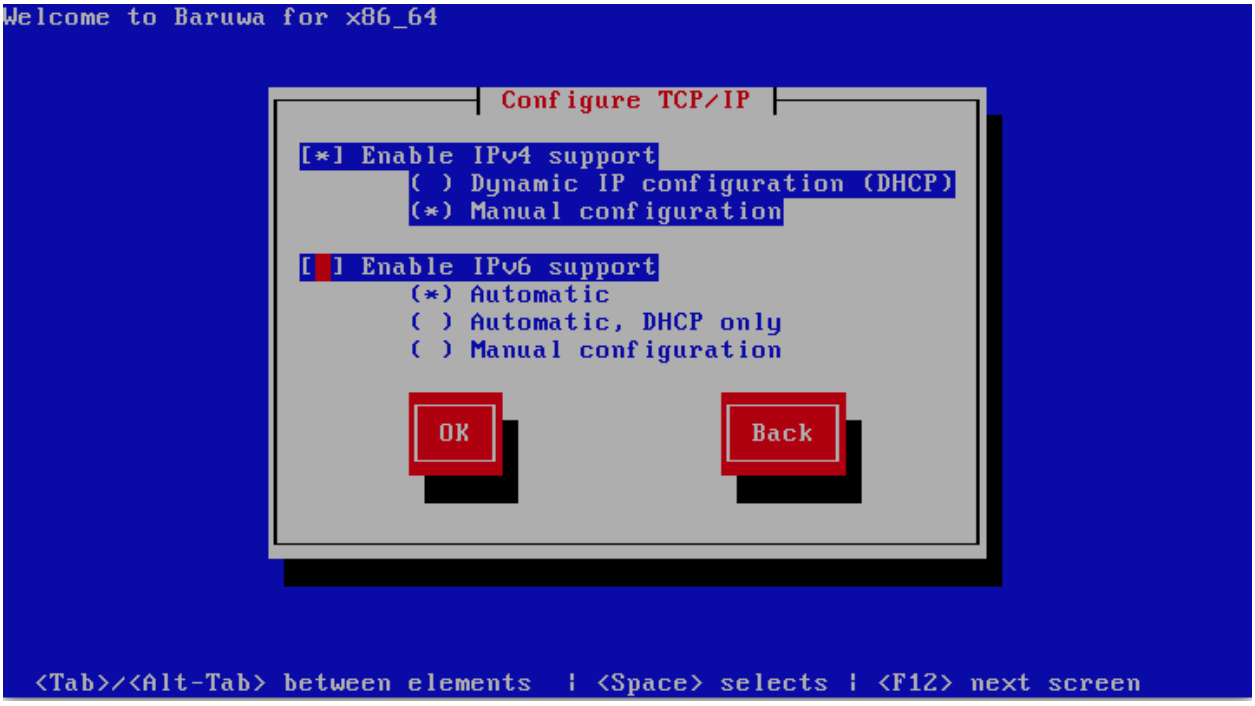
The installer uses DHCP running on the network to supply the network configuration automatically. Ensure that you DHCP server assigns a static IP address to the server and does not provide DNS infomation that overwrites the local settings.

If your DHCP server is unable to assign static addresses or cannot be configured to not modify DNS settings then use Manual configuration instead.

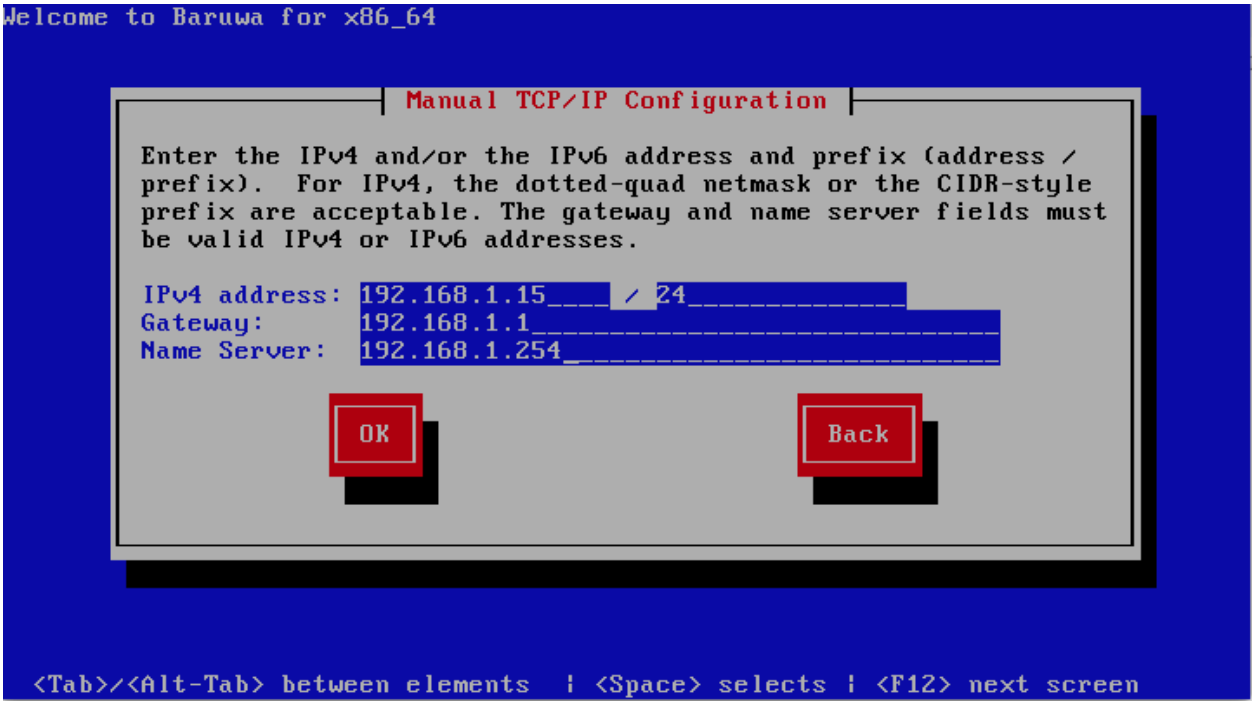
5.3.2 Manual configuration

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.



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



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.

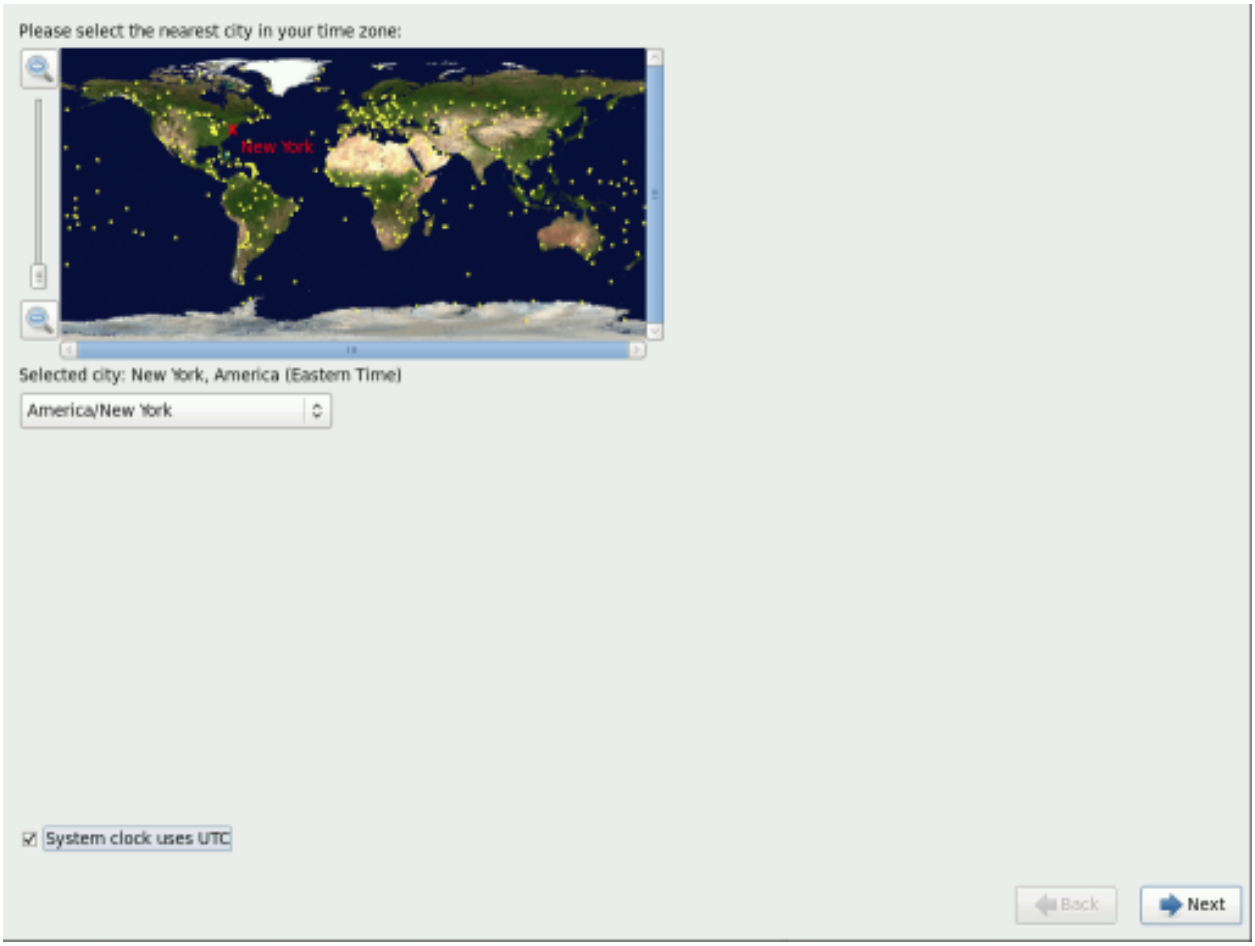
5.4.2 Time Zone Configuration

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.

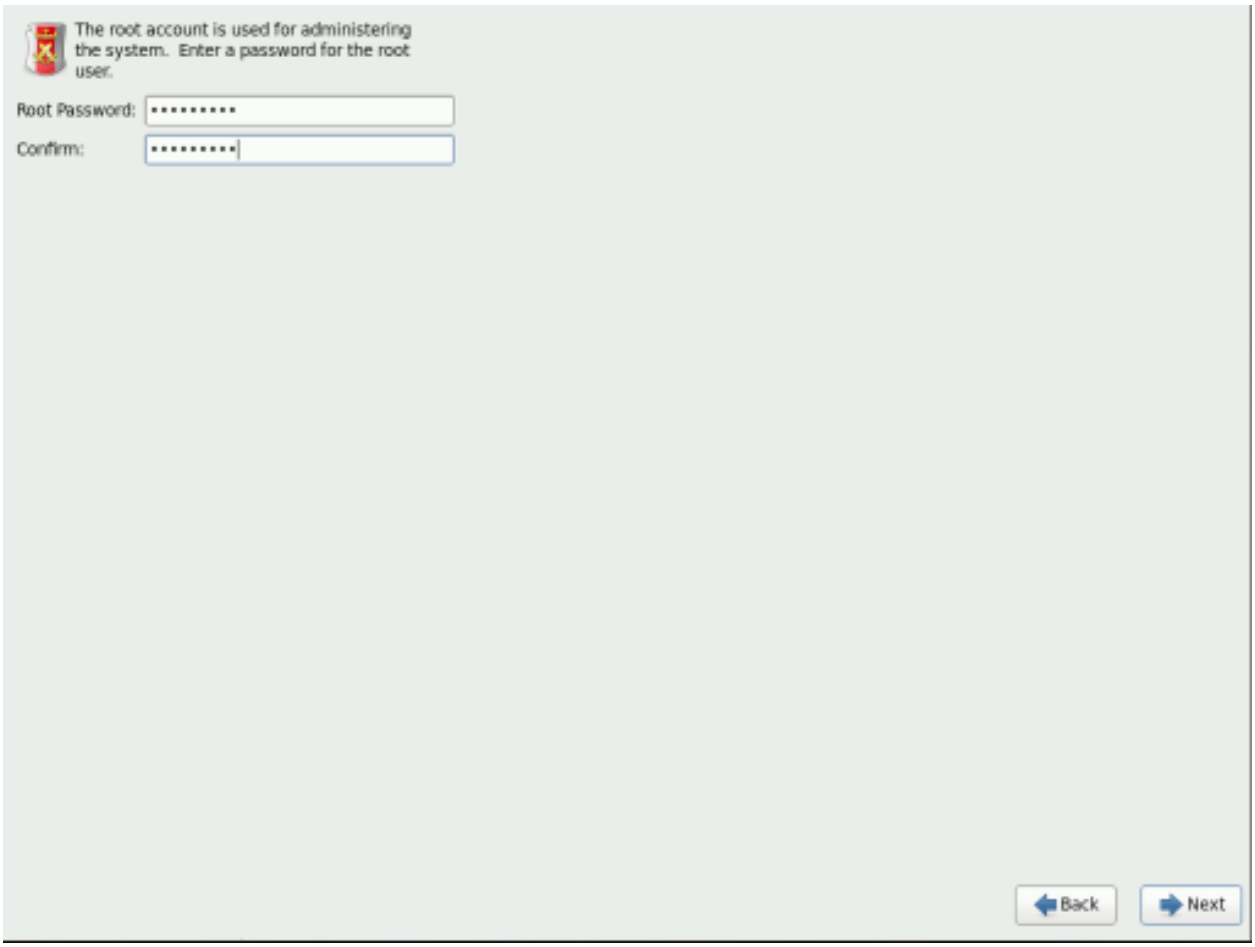


Select System clock uses UTC. The system clock is a piece of hardware on your computer system. Baruwa Enterprise Edition uses the timezone setting to determine the offset between the local time and UTC on the system clock. This behaviour is standard for systems that use UNIX, Linux, and similar operating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

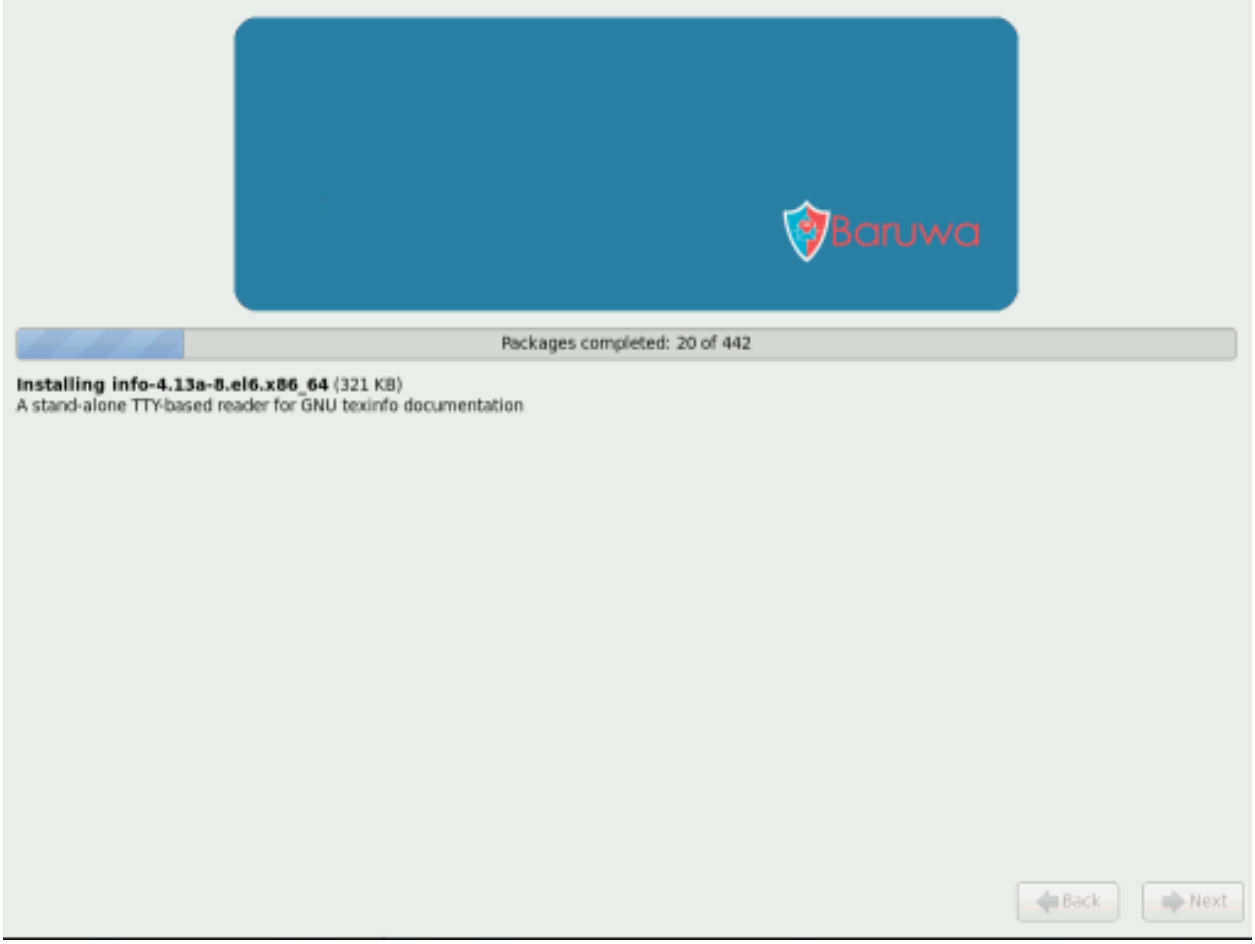
The root password must be at least six characters long; the password you type is not echoed to the screen. You must enter the password twice; if the two passwords do not match, the installation program asks you to enter them again.

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 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.

5.4.4 Installing Packages

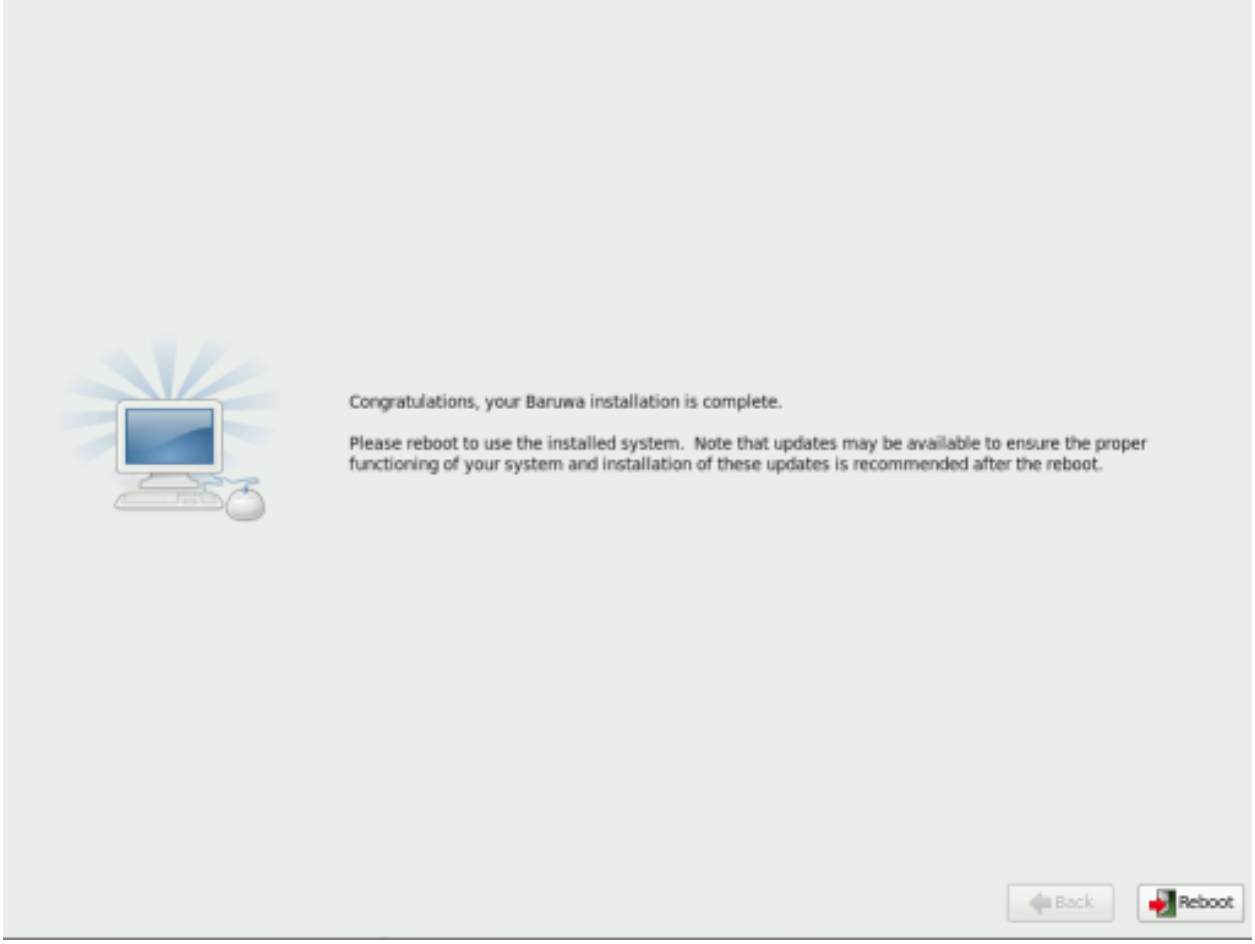
At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the profile you have selected and your computer's speed.

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.

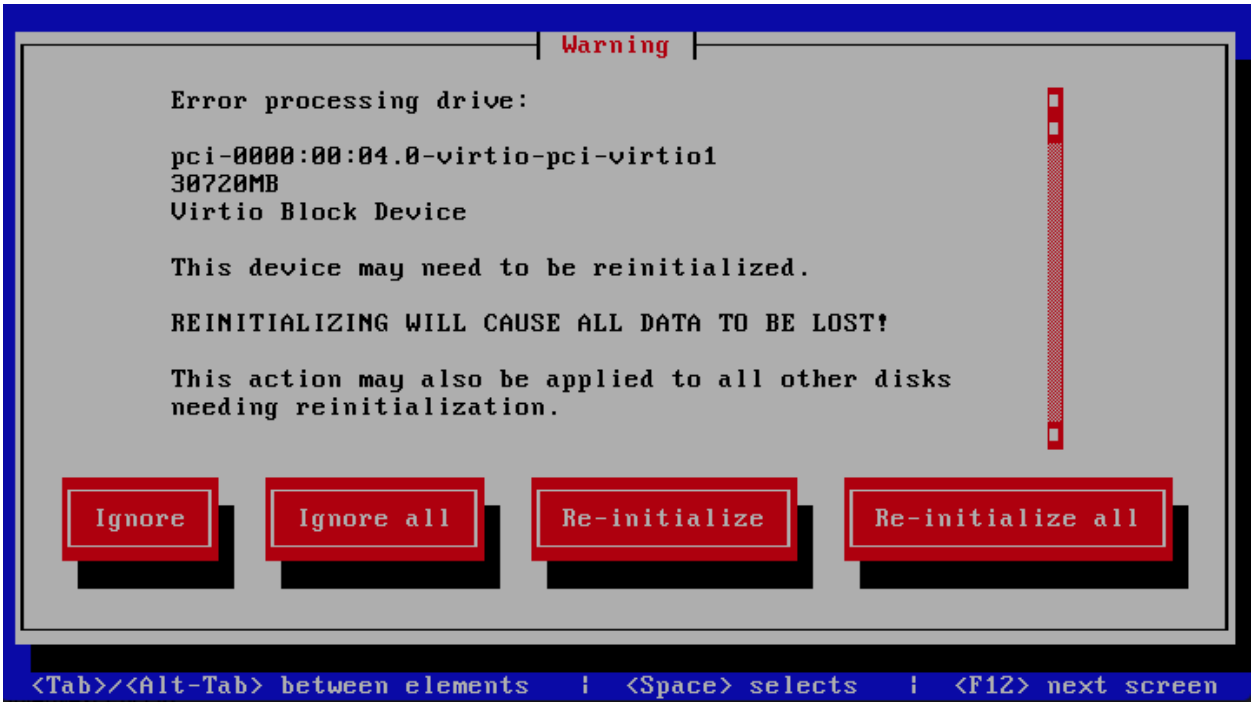
5.5 Text Mode Installation

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`.

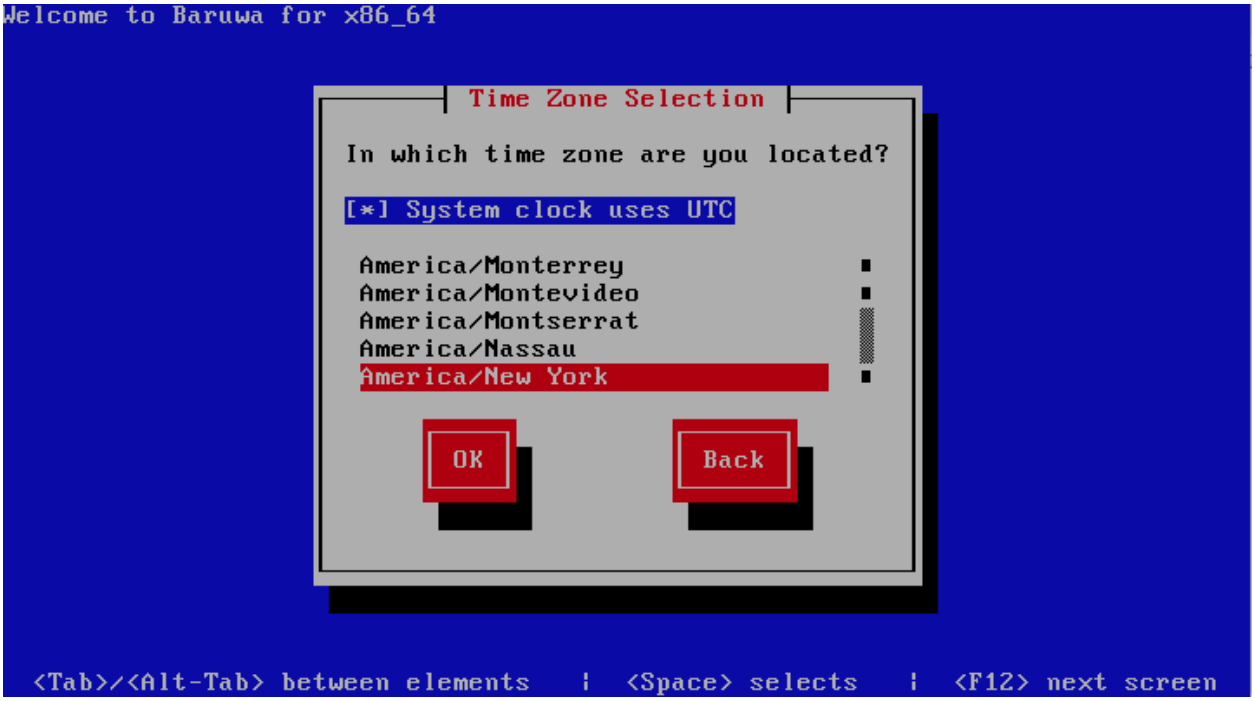
The installation program presents you with a separate dialog for each disk on which it cannot read a valid partition table. Click the `Ignore all` button or `Re-initialize all` button to apply the same answer to all devices.



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.

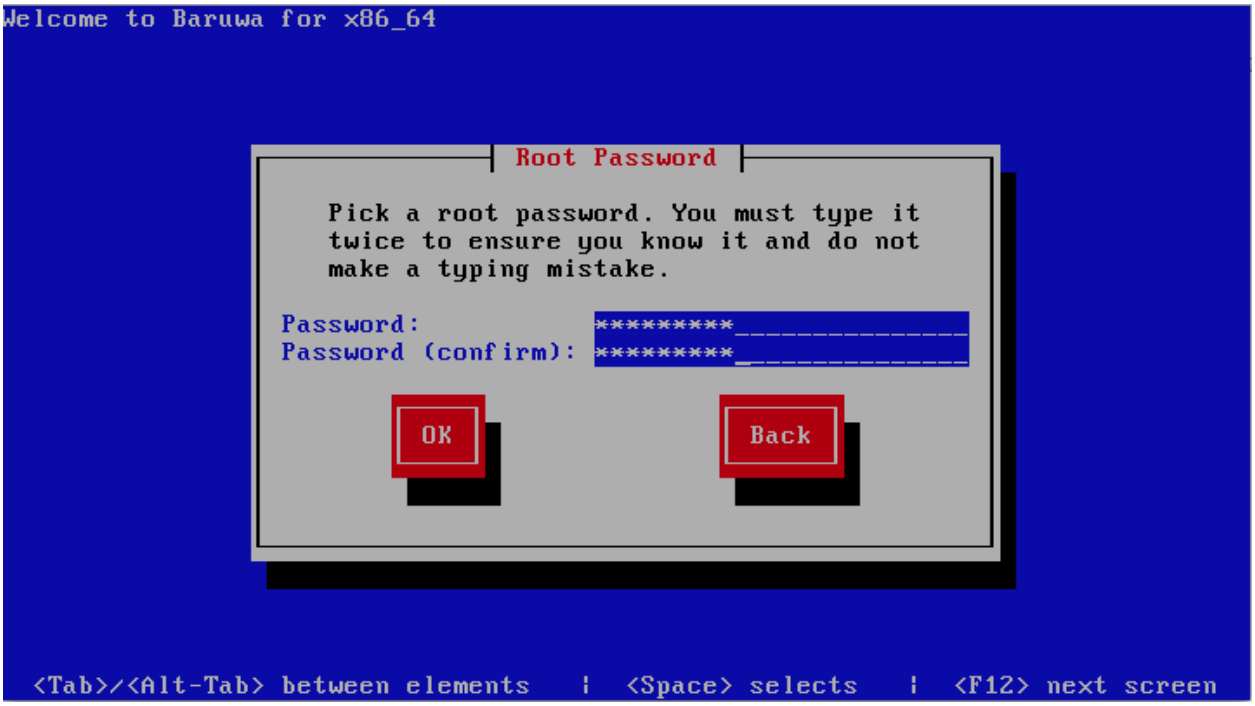


Select System clock uses UTC. The system clock is a piece of hardware on your computer system. Baruwa Enterprise Edition uses the timezone setting to determine the offset between the local time and UTC on the system clock. This

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.

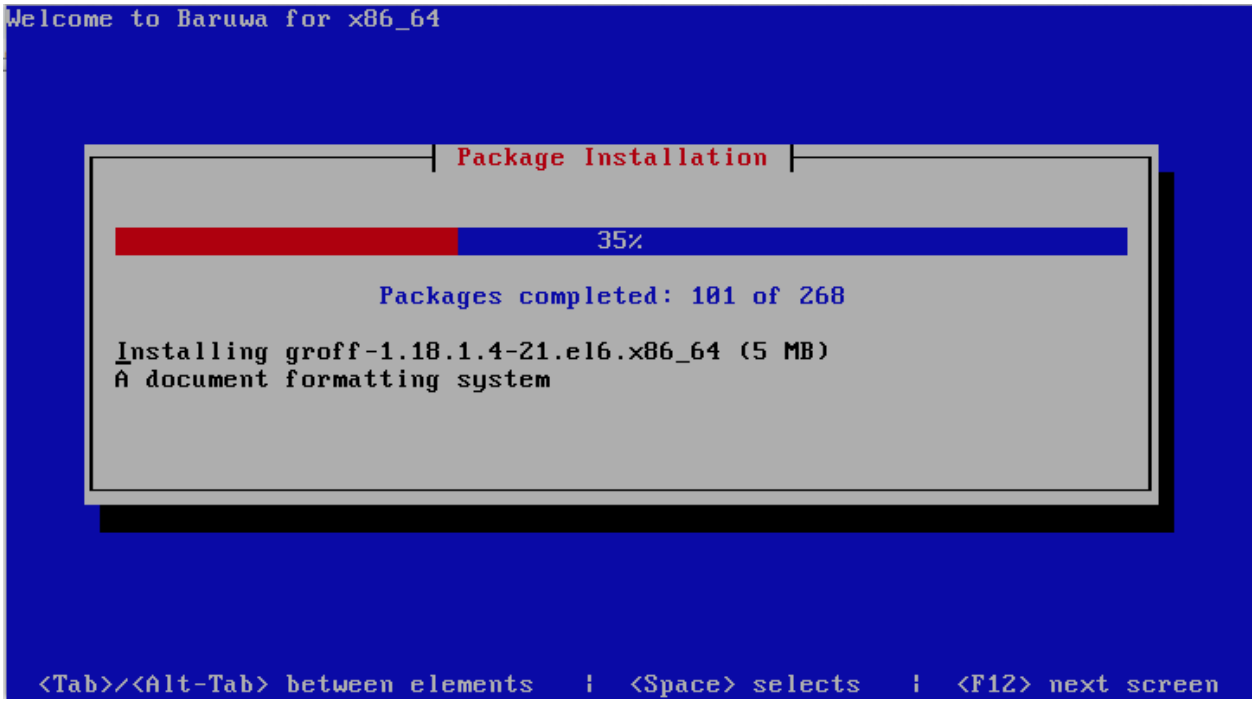
The root password must be at least six characters long; the password you type is not echoed to the screen. You must enter the password twice; if the two passwords do not match, the installation program asks you to enter them again.

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

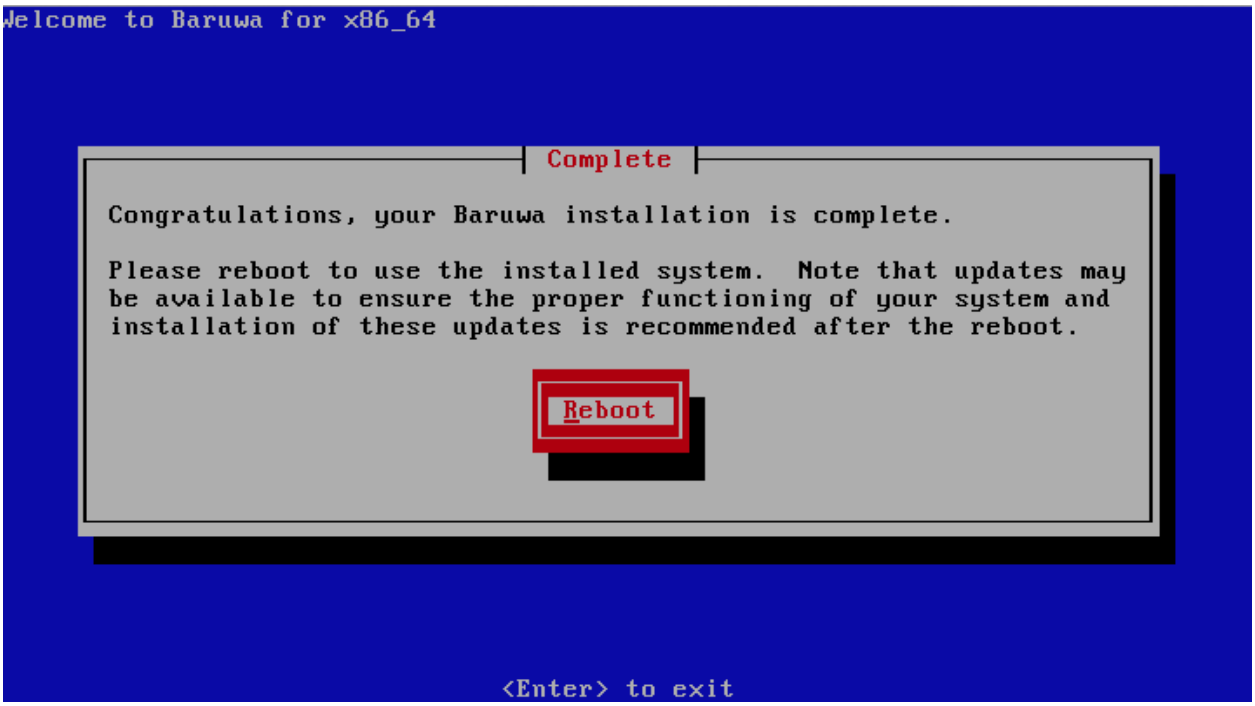
At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the profile you have selected and your computer's speed.

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.



5.6 Configuration

After the VPS has rebooted, you should login and run *baruwa-setup* to complete configuration. Refer to the *Configuration* section for details.

CHAPTER

SIX

CLOUD INSTALLATION

Note: This section describes installation on a clould server, if you would like to install on premise, refer to the *On Premise Installation* section.

6.1 Overview

Baruwa Enterprise Edition can be installed on a cloud server. At the moment the following cloud providers are supported.

- Rimuhosting
- Vultr
- DigitalOcean
- Linode

The cloud installation system is based on Vagrant. You need to have vagrant installed on your local system to be able to provision a Baruwa Enterprise Edition system to one of these cloud providers. Vagrant provides installers for all major operating systems. Please refer to their site to download the installer for your operating system.

Of course you will need to create an account with your prefered cloud provider and signup for an API key.

You also require the Vagrant plugin for the cloud provider that you want to use installed.

6.1.1 Rimuhosting

To install the Rimuhosting Vagrant plugin, run:

```
vagrant plugin install vagrant-rimu
```

6.1.2 Vultr

To install the Vultr Vagrant plugin, run:

```
vagrant plugin install vagrant-vultr
```

6.1.3 DigitalOcean

To install the DigitalOcean Vagrant plugin, run:

```
vagrant plugin install vagrant-digitalocean
```

6.1.4 Linode

To install the Linode Vagrant plugin, run:

```
vagrant plugin install vagrant-linode
```

6.2 Installation

Once you have downloaded and installed Vagrant and the plugin you need to clone the Baruwa Enterprise Edition Vagrant files to your system:

```
git clone https://github.com/akissa/baruwa-vagrant.git
```

The above command should create a *baruwa-vagrant* directory, you need to change into that directory to issue the commands that follow.:

```
cd baruwa-vagrant
```

Configuration is by use of environment variables. You should export the variable to the environment to set them.

6.2.1 Rimuhosting

The following variables are required.

- RIMUHOSTING_APIKEY - The Rimuhosting API Key
- BARUWA_HOSTNAME - The hostname to assign to the server
- BARUWA_ACTIVATION_KEY - The Baruwa Enterprise Edition Activation Key
- BARUWA_PROFILE - The System Profile to setup options are `standalone`, `web`, `node`, `indexer`, `mq`, `backend`, `db`, `cache`

The following variables are optional.

- RIMUHOSTING_DISK1 - defaults to 20GB
- RIMUHOSTING_REGION - defaults to DCDALLAS, the Dallas DC
- RIMUHOSTING_SIZE - defaults to 4GB

Additional variables are available and you can review those in the plugin documentation at https://github.com/akissa/vagrant-rimu

Generate an SSH key pair for use by the plugin.:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/rimuhosting_rsa
```

After generating the ssh key pair, you should run the following command to setup the VPS.:

```
export RIMUHOSTING_APIKEY="rimuhosting apikey"
export BARUWA_HOSTNAME="baruwa.example.com"
export BARUWA_ACTIVATION_KEY="key"
export BARUWA_PROFILE="standalone"
vagrant up --provider=rimu
```

After the VPS has been setup you can login and proceed with configuration.:

```
vagrant ssh
```

6.2.2 Vultr

The following variables are required.

- VULTR_TOKEN - The API token
- BARUWA_HOSTNAME - The hostname to assign to the server
- BARUWA_ACTIVATION_KEY - The Baruwa Enterprise Edition Activation Key
- BARUWA_PROFILE - The System Profile to setup options are `standalone`, `web`, `node`, `indexer`, `mq`, `backend`, `db`, `cache`

The following variables are optional.

- VULTR_REGION - defaults to Frankfurt
- VULTR_SIZE - defaults to "4096 MB RAM,90 GB SSD,4.00 TB BW"

Generate an SSH key pair for use by the plugin.:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/vultr_rsa
```

After generating the ssh key pair, you should run the following command to setup the VPS.:

```
export VULTR_TOKEN="vultr token"
export BARUWA_HOSTNAME="baruwa.example.com"
export BARUWA_ACTIVATION_KEY="key"
export BARUWA_PROFILE="standalone"
vagrant up --provider=vultr
```

After the VPS has been setup you can login and proceed with configuration.:

```
vagrant ssh
```

6.2.3 DigitalOcean

The following variables are required.

- DIGITAL_OCEAN_TOKEN - The API token
- BARUWA_HOSTNAME - The hostname to assign to the server
- BARUWA_ACTIVATION_KEY - The Baruwa Enterprise Edition Activation Key
- BARUWA_PROFILE - The System Profile to setup options are `standalone`, `web`, `node`, `indexer`, `mq`, `backend`, `db`, `cache`

The following variables are optional.

- DIGITAL_OCEAN_REGION - defaults to Frankfurt 1
- DIGITAL_OCEAN_SIZE - defaults to 4GB

Additional variables are available and you can review those in the plugin documentation at https://github.com/smdahlen/vagrant-digitalocean

Generate an SSH key pair for use by the plugin.:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/digital_ocean_rsa
```

After generating the ssh key pair, you should run the following command to setup the VPS.:

```
export DIGITAL_OCEAN_TOKEN="digitalocean token"
export BARUWA_HOSTNAME="baruwa.example.com"
export BARUWA_ACTIVATION_KEY="key"
export BARUWA_PROFILE="standalone"
vagrant up --provider=digital_ocean
```

After the VPS has been setup you can login and proceed with configuration.:

```
vagrant ssh
```

6.2.4 Linode

The following variables are required.

- LINODE_TOKEN - The Linode API Token
- BARUWA_HOSTNAME - The hostname to assign to the server
- BARUWA_ACTIVATION_KEY - The Baruwa Enterprise Edition Activation Key
- BARUWA_PROFILE - The System Profile to setup options are `standalone`, `web`, `node`, `indexer`, `mq`, `backend`, `db`, `cache`

The following variables are optional.

- LINODE_REGION - defaults to frankfurt
- LINODE_SIZE - defaults to 4096
- LINODE_LABEL - defaults to baruwa-enterprise-edition-vagrant

Additional variables are available and you can review those in the plugin documentation at https://github.com/displague/vagrant-linode

Generate an SSH key pair for use by the plugin.:

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/linode_rsa
```

After generating the ssh key pair, you should run the following command to setup the VPS.:

```
export LINODE_TOKEN="linode token"
export BARUWA_HOSTNAME="baruwa.example.com"
export BARUWA_ACTIVATION_KEY="key"
export BARUWA_PROFILE="standalone"
vagrant up --provider=linode
```

After the VPS has been setup you can login and proceed with configuration.:

```
vagrant ssh
```

6.3 Configuration

After the VPS has been setup and converted you can now run *baruwa-setup* to complete configuration. Refer to the *Configuration* section for details

CHAPTER

SEVEN

CONFIGURATION

The configuration, update and management 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*

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.

7.2 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

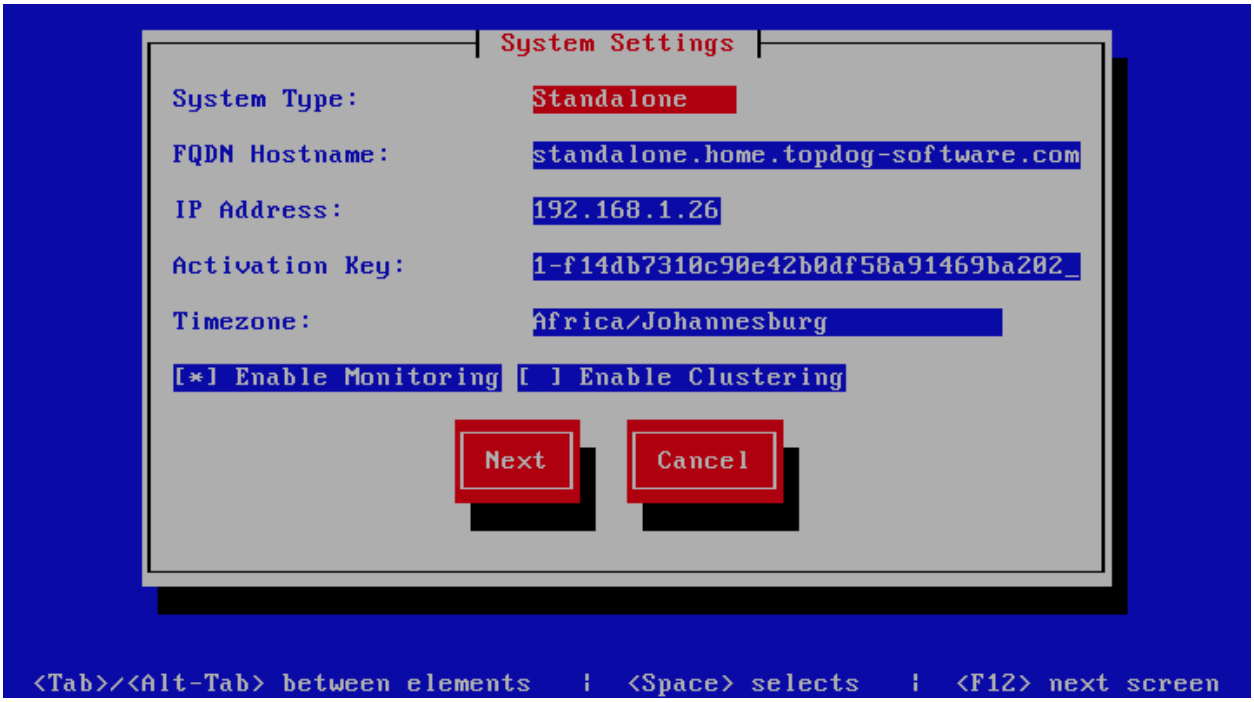
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

7.2.1 System Settings

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

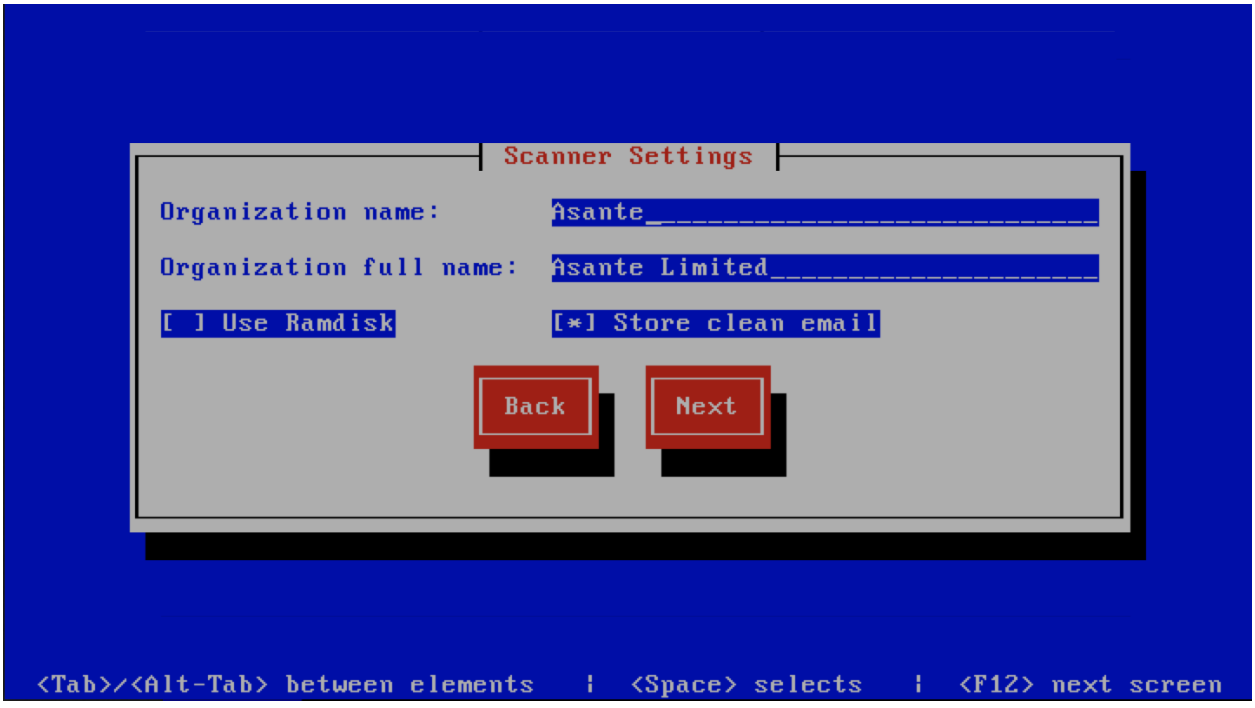
Option	Description
System Type	Set this to Standalone
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system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



7.2.2 Scanner Settings

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

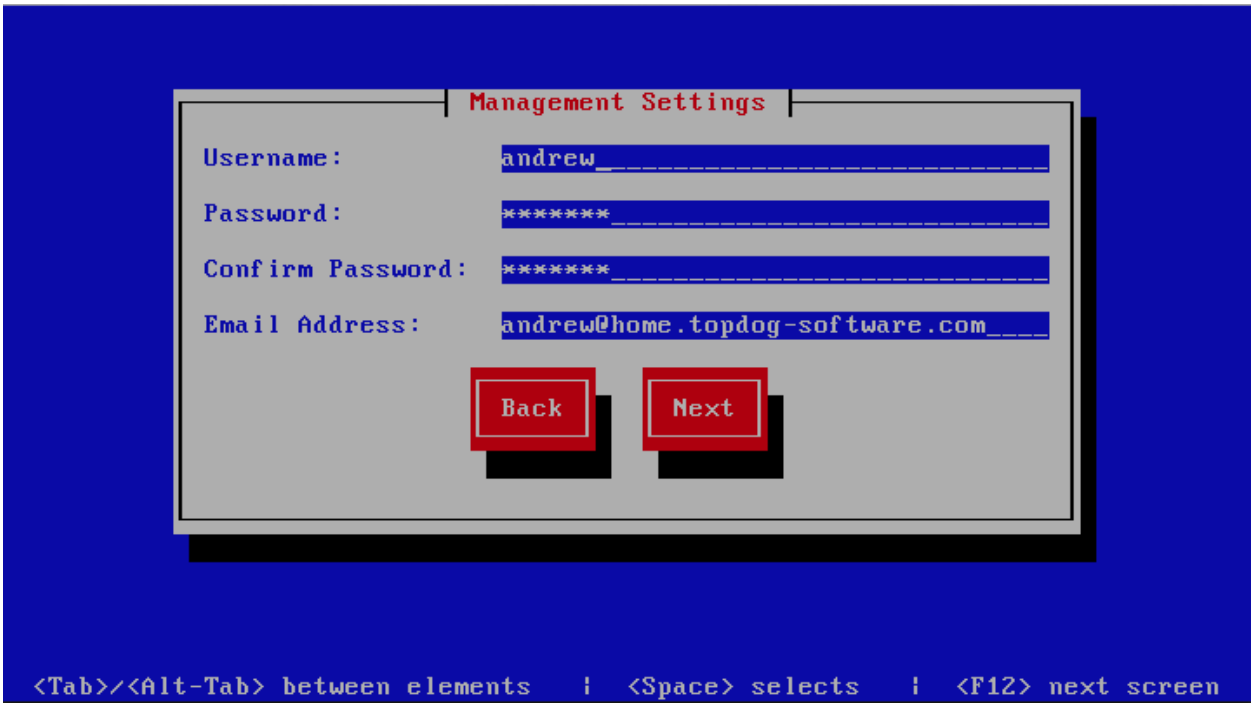
Option	Description
Organization name	Enter a short identifying name for your organisation this is used to make the X-Baruwa headers unique for your organisation Multiple servers within one site should use an identical value here. It must not contain any spaces.
Organization full name	Enter the full name 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 Ramdisk	Check this to enable using a RAM disk for mail scanning This makes scanning more efficient, but it uses 1GB of RAM. Make sure you provision sufficient RAM.
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



7.2.3 Management Settings

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

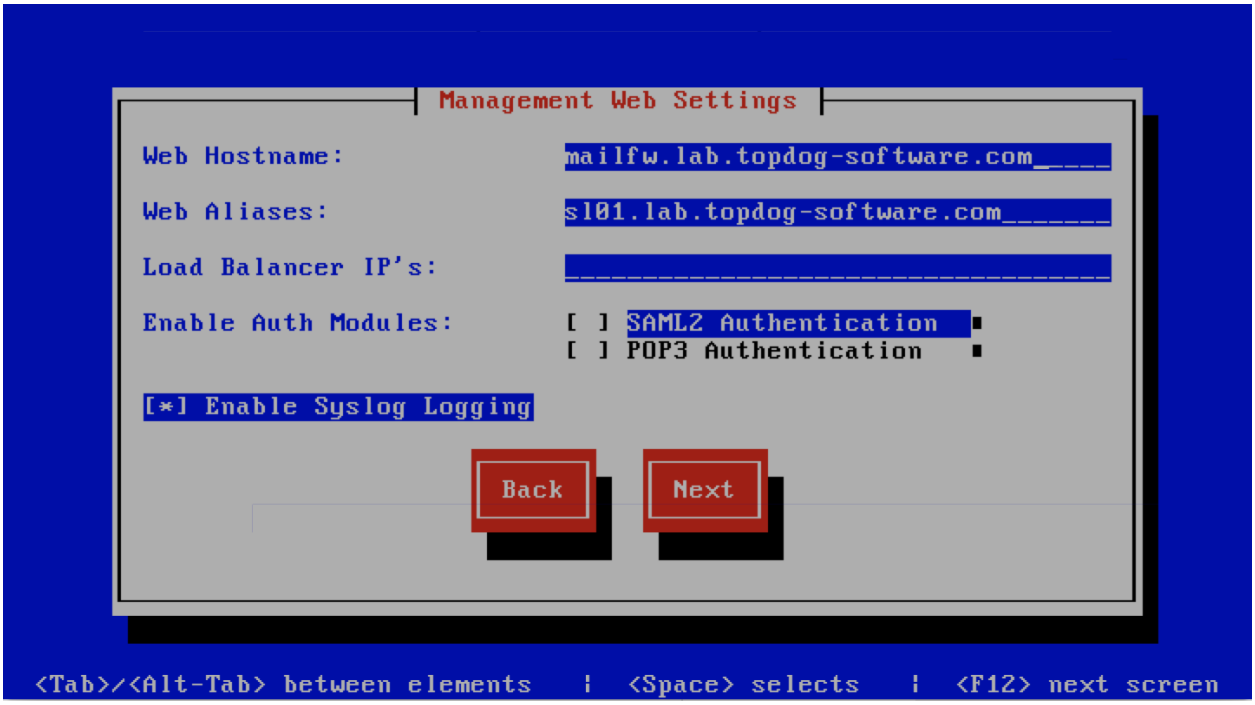
Option	Description
Username	Administrator username
Password	Administrator password, Only strong passwords will be accepted use a service such as passwordsgenerator.net to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address



7.2.4 Management Web Settings

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

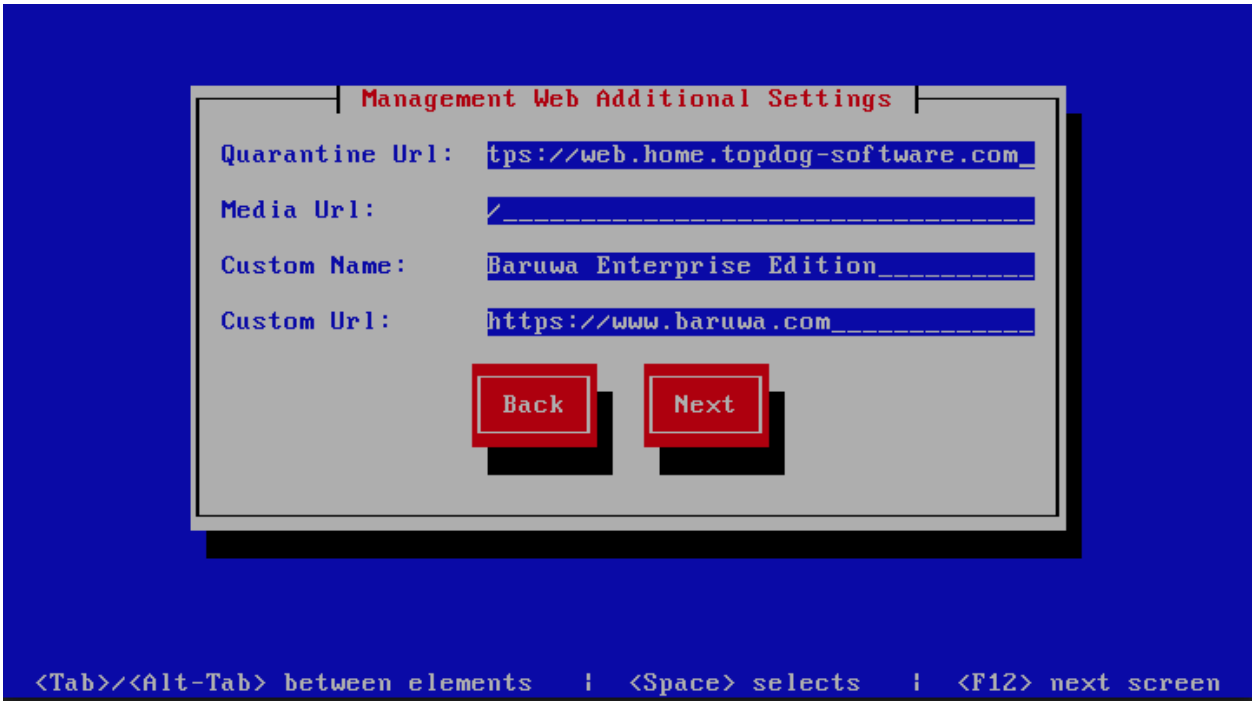
Option	Description
Web Hostname	The hostname to be used to access the web interface
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable Auth Modules	The external authentication modules to enable
Enable Syslog Logging	Turns on Web logging to syslog



7.2.5 Management Web Additional Settings

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

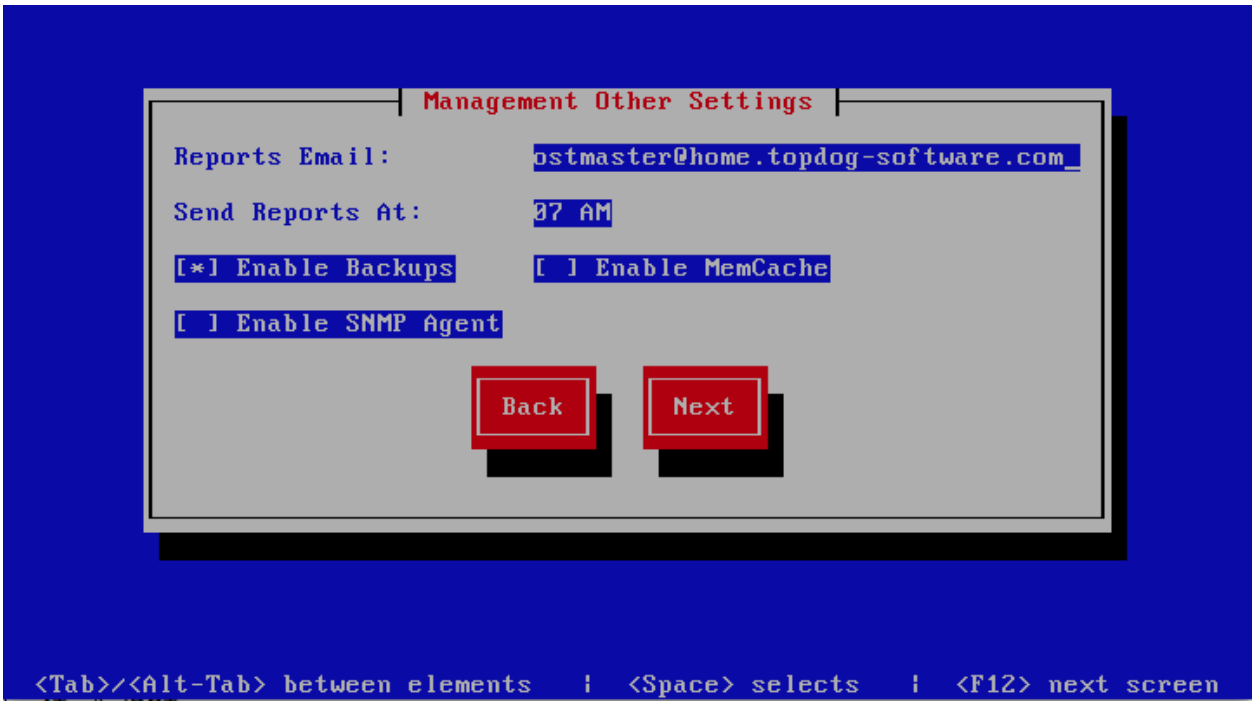
Option	Description
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the web interface as well.
Custom URL	This creates links to your product page within the web interface and email reports that are sent out.



7.2.6 Management Other Settings

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

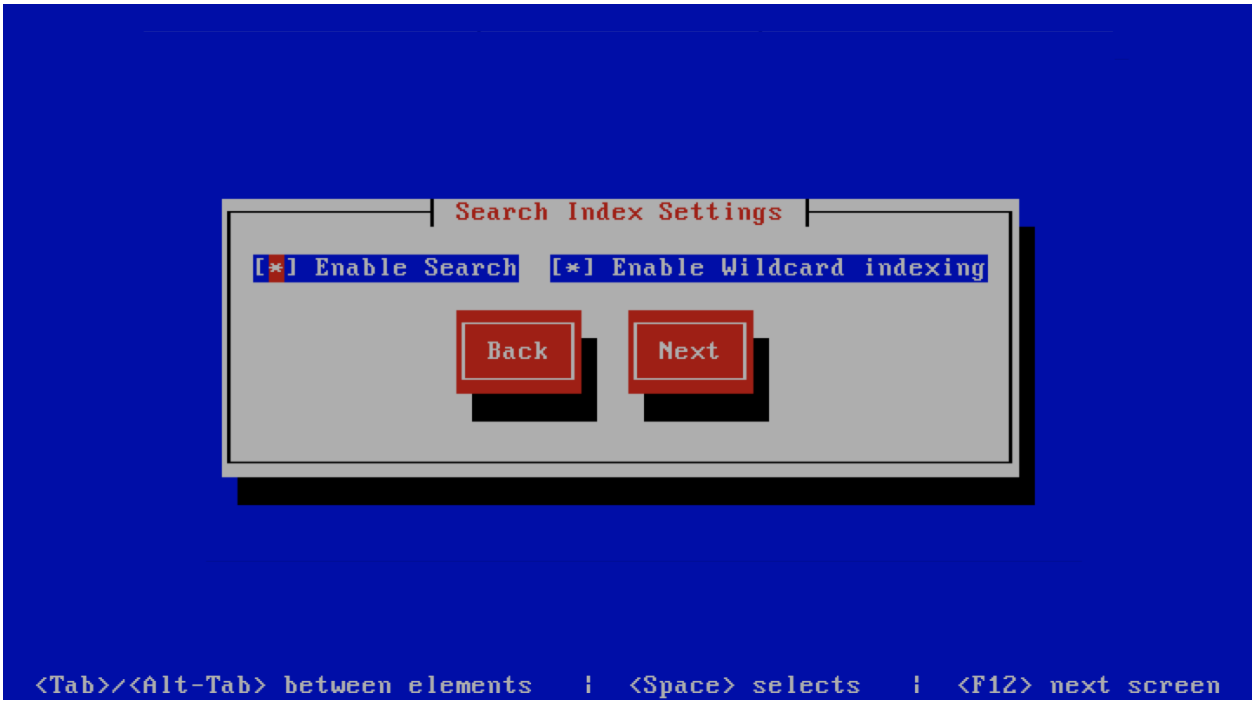
Option	Description
Reports Email	The email address used to send out email reports
Send Reports At	The hour at which to send reports, this is localized to the users location based on their timezone setting
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable Memcache	Enables or disables the Memcached cache system, when disabled the builtin cache system will be used. The builtin cache system is more efficient on standalone systems
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.



7.2.7 Search Index Settings

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

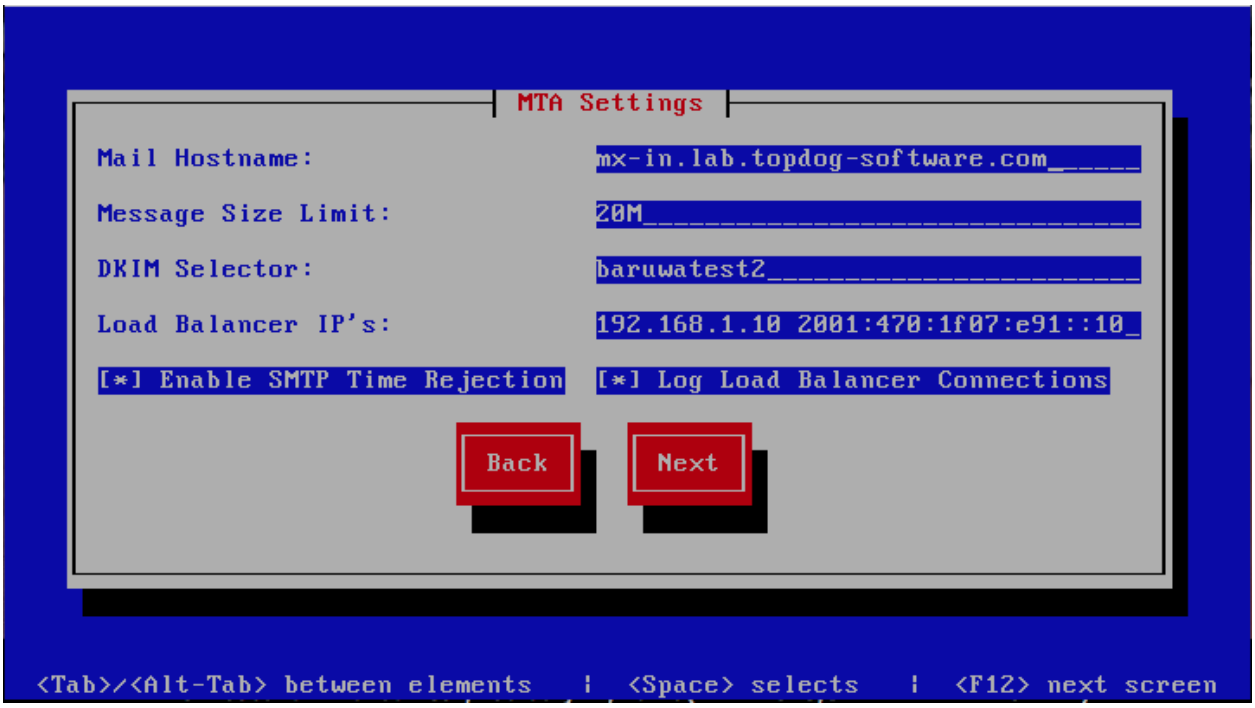
Option	Description
Enable Search	Enables Search functionality
Enable wildcard indexing	Enables Search wildcard indexing, Setting this to true will generate very large index files.



7.2.8 MTA Settings

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

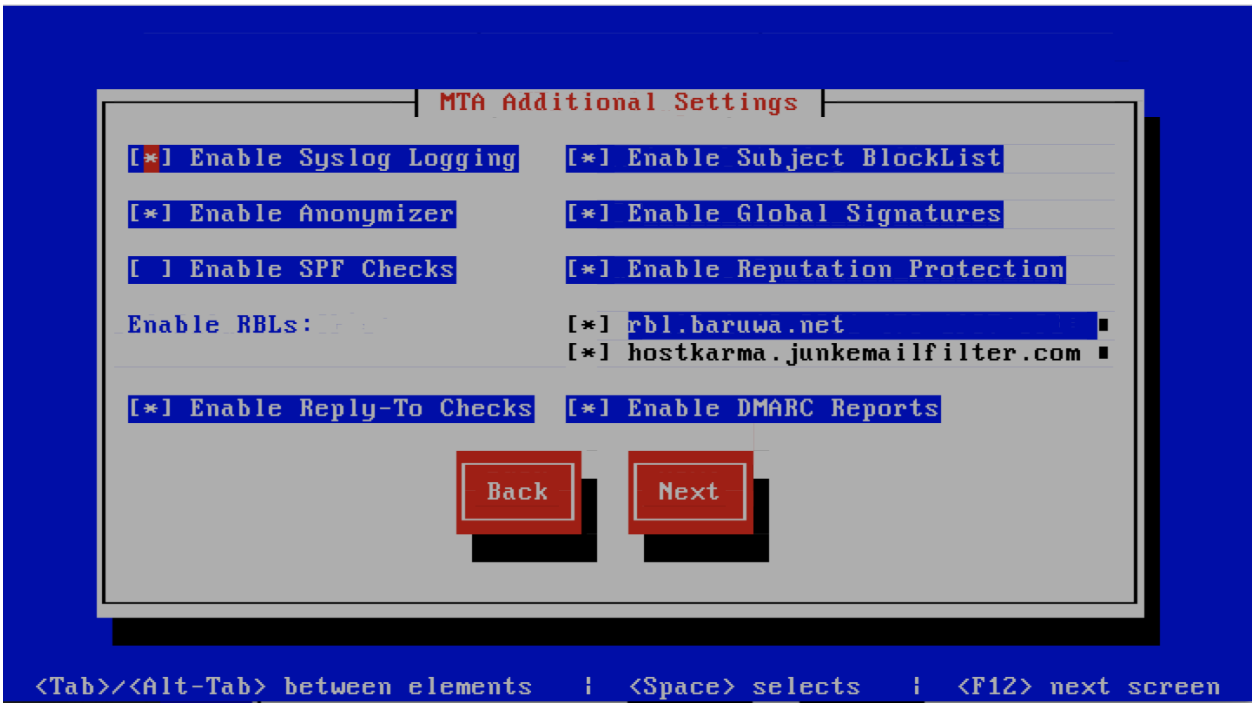
Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable SMTP Time Rejection	Enable SMTP rejection of messages which either match Anti-Virus signatures or exhibit definite SPAM like charactaristics at SMTP Time without queueing or logging the message.
Log Load Balancer Connections	Log Load Balancer connections to the MTA log



7.2.9 MTA Additional Settings

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

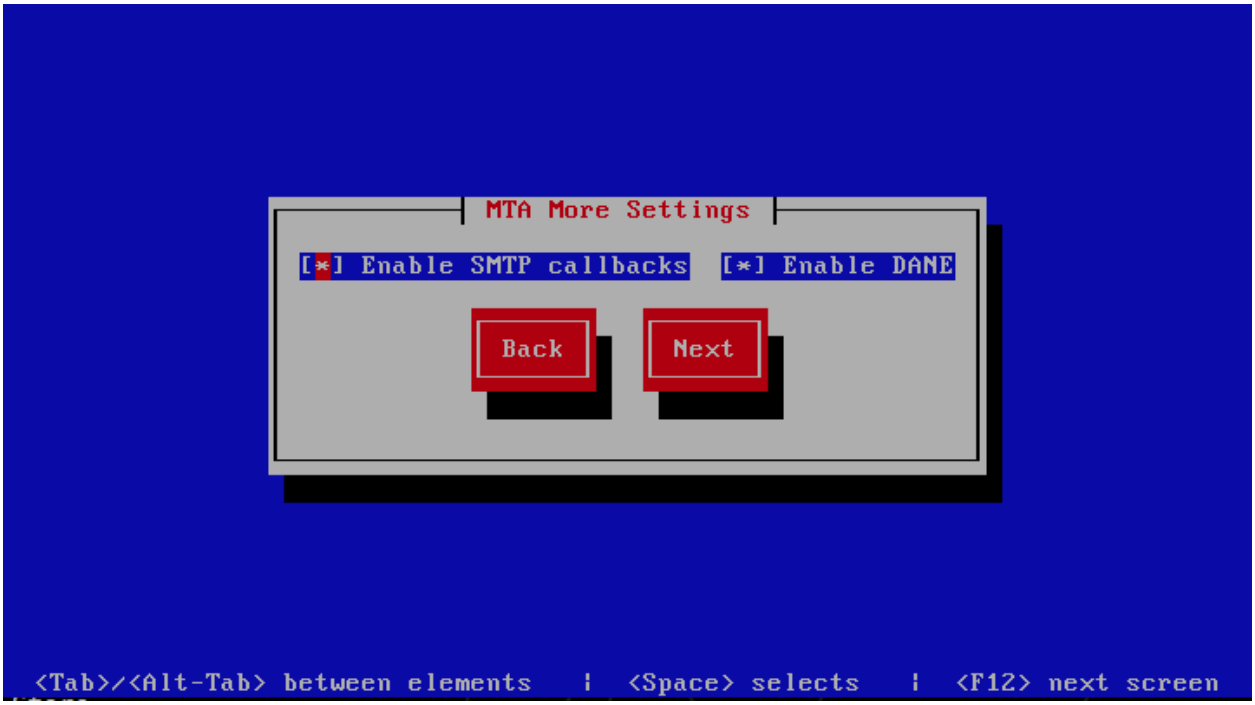
Option	Description
Enable Syslog Logging	Turns on MTA logging to syslog
Enable Subject Blocklist	Enable the blocking by subject functionality
Enable Anonymizer	Enable the Anonymizer functionality
Enable Global Signatures	Enable Global Signatures
Enable SPF Checks	Enable SPF checking functionality
Enable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



7.2.10 MTA More Settings

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

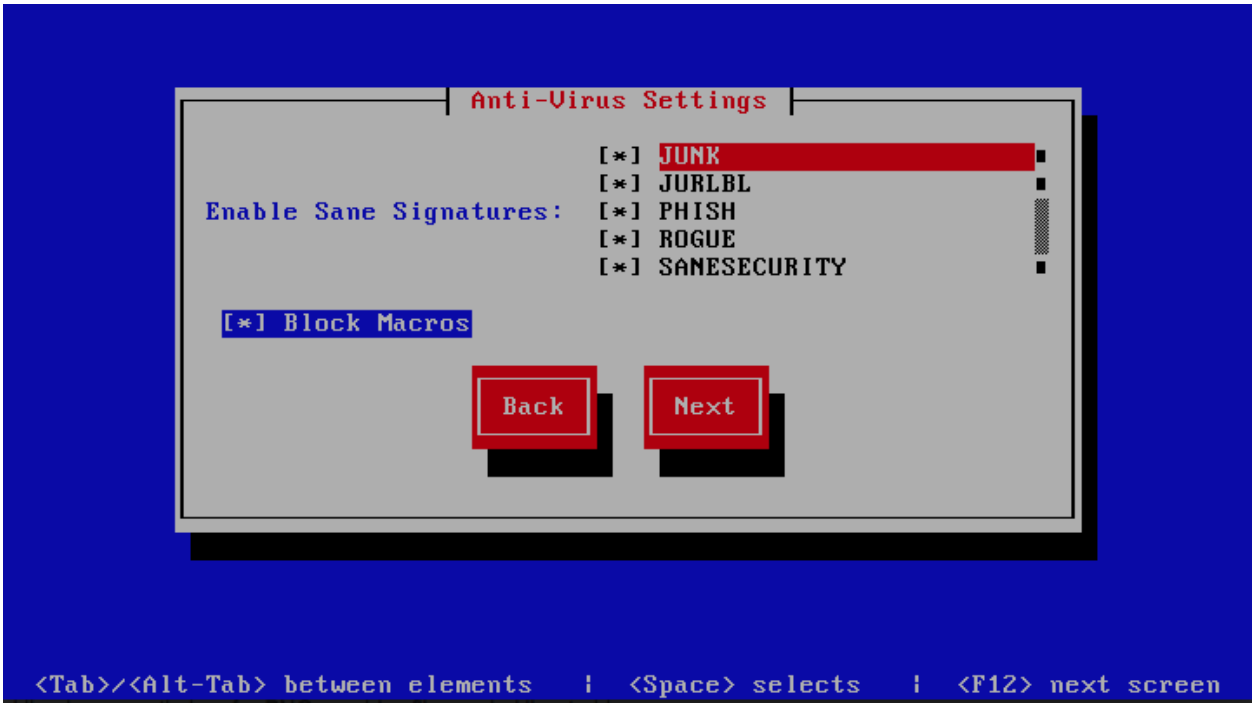
Option	Description
Enable SMTP callbacks	Enable SMTP Callback verification for senders who do not have reverse DNS records configured.
Enable DANE	Enable the DANE protocol support.



7.2.11 Anti Virus Settings

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

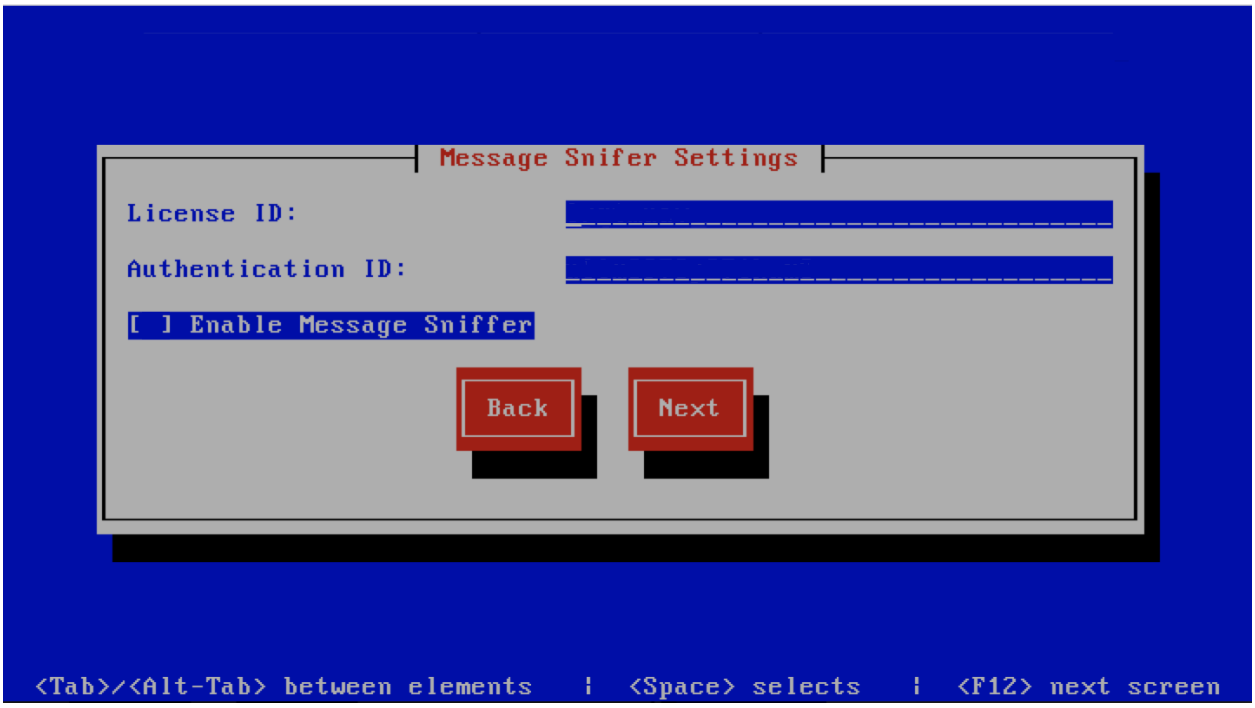
Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Block Macros	Block documents that contain macros



7.2.12 Message Sniffer Settings

This 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



7.2.13 SSL/TLS Settings

The Baruwa web interface MUST ran 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 request a CertBot certificate or generate a non recognised Builtin 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.

Certbot certificate

The issuance of a CertBot certificate is based on an automated check that verifies that the hostnames specified are under your control. Baruwa performs a precheck to verify that the hostnames resolve to a public IP address on the host itself. If this check fails then the Certbot certificate will not be requested. This check will fail if your public IP address is on another device and you are forwarding connections to a private address on your Baruwa system. To work around that you need to create a check file:

```
touch /etc/baruwa/acme.enable
```

For the validation process to succeed, Certbot systems need to be able to connect to port 80 on your system, ensure that that is allowed on your network devices.

Certbot certificates are only issued to systems of the *Standalone System*, *Web and Mail System* and *Web Interface System* profiles.

Certbot certificates are issued only to the web hostname, web aliases and the mail hostname. Cluster members names are not included in the certificate.

Support for CertBot certificates was added in BaruwaOS 6.8, refer to the *ACME TLS Certificates* section of the release notes for more information.

Note: It is currently not possible to issue or syncronize certificates in a cluster that uses the same hostname. If you are operating a cluster you should either purchase a Commercial CA issued certificate or use Builtin certificates.

Commercial CA issued certificate

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

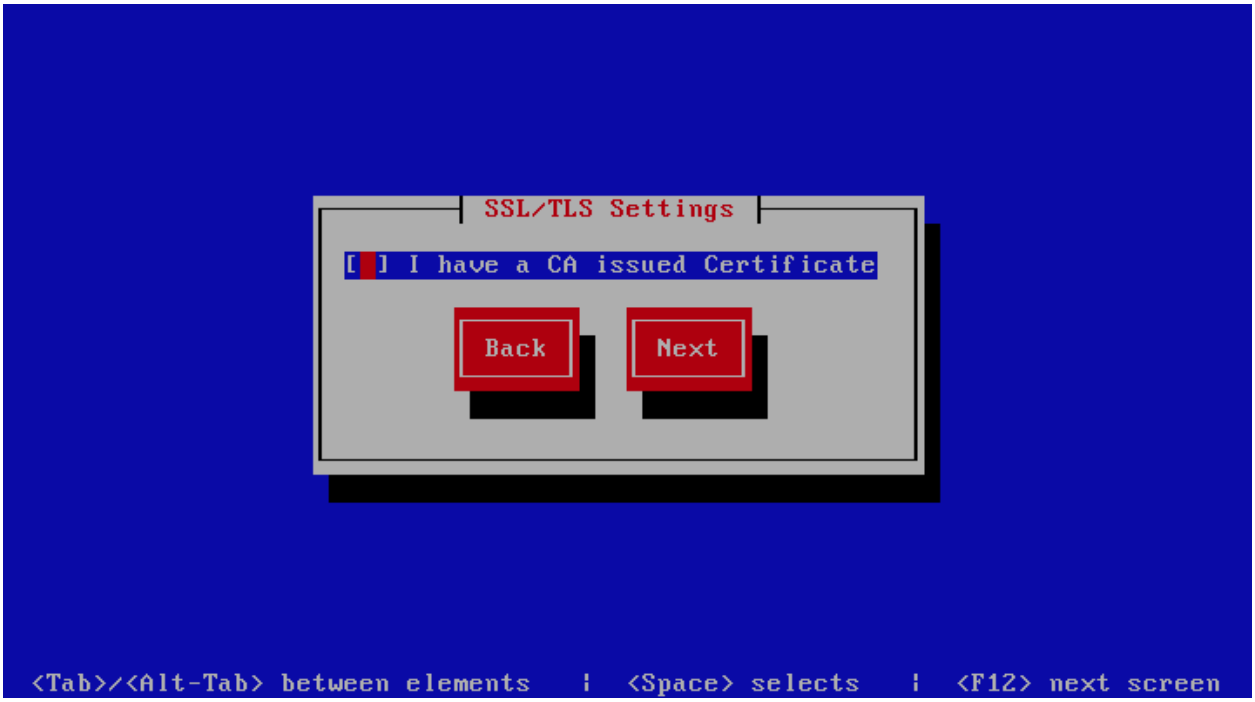
If your SSL certificate is signed using an intermediate certificate, you need to append the intermediate certificate to the file `/etc/pki/baruwa/certs/baruwa.pem`. The server certificate must appear before the intermediate certificate in the combined file.

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.

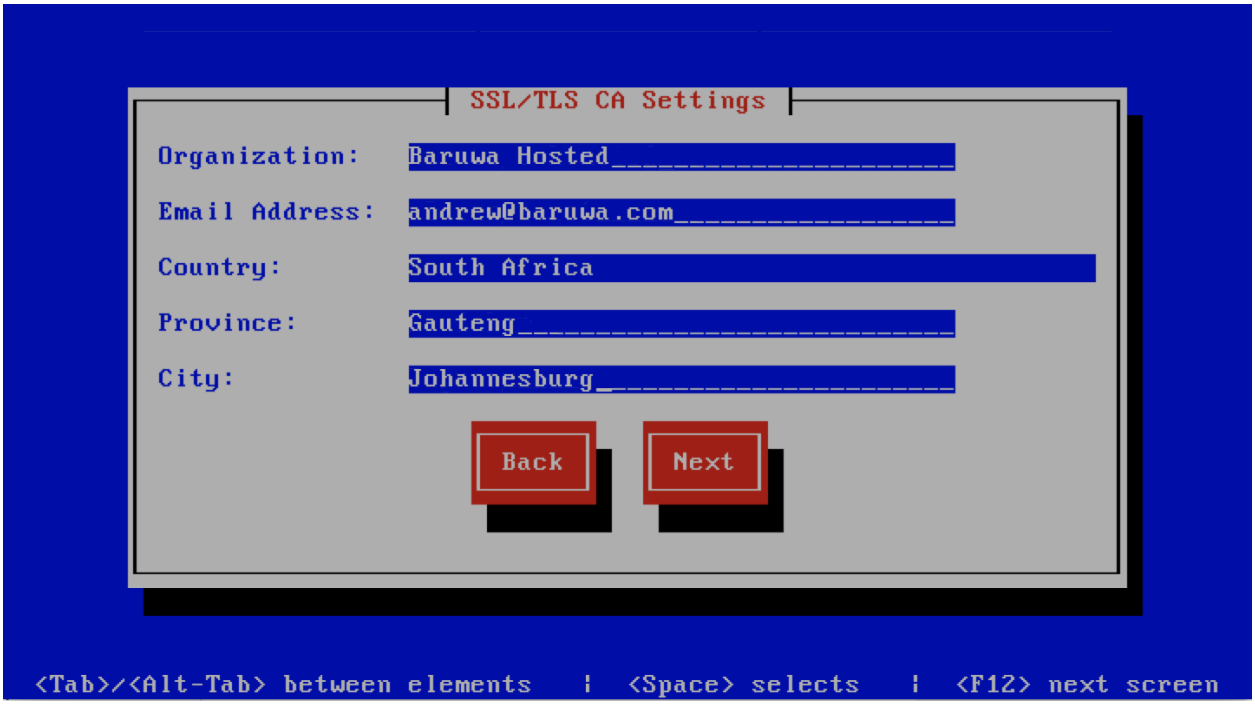
Builtin certificate

The certificate that `baruwa-setup` generates contains all the relevant system names. The downside to the builtin certificates is that they are signed by the BaruwaCA meaning they will not be recognized by browsers and will generate unknown CA errors in browsers.



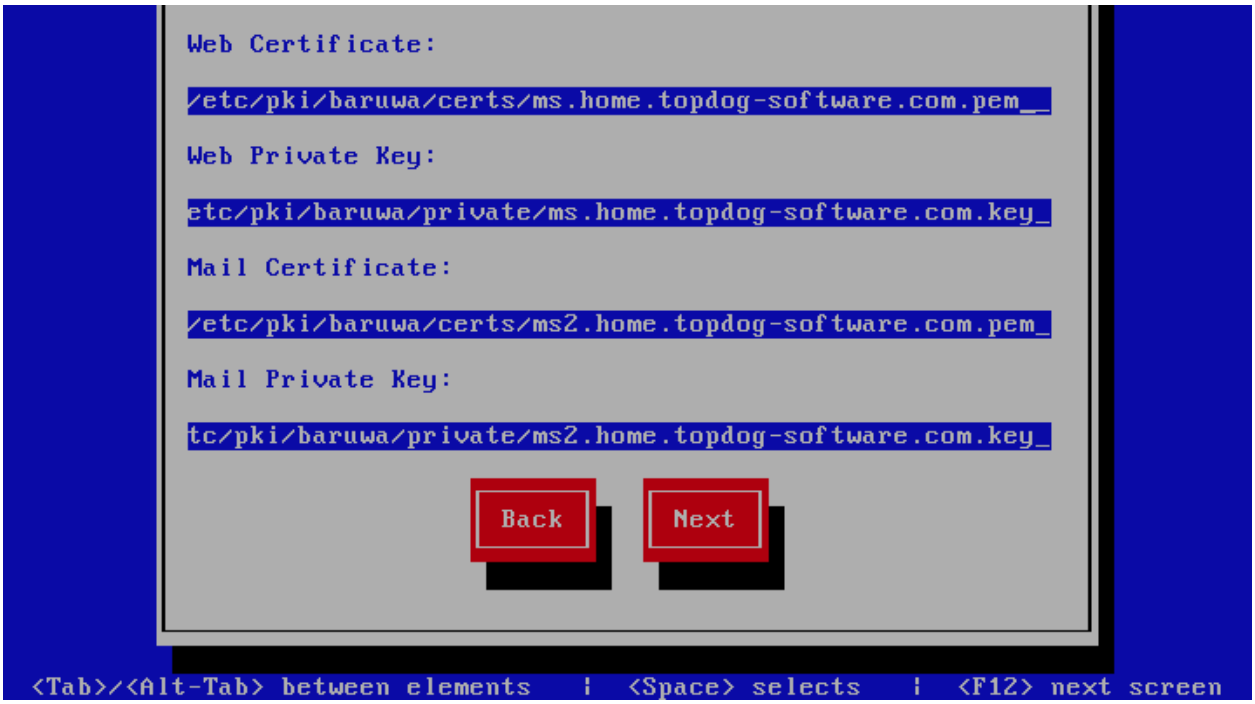
If you left `I have a CA issued Certificate` unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

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

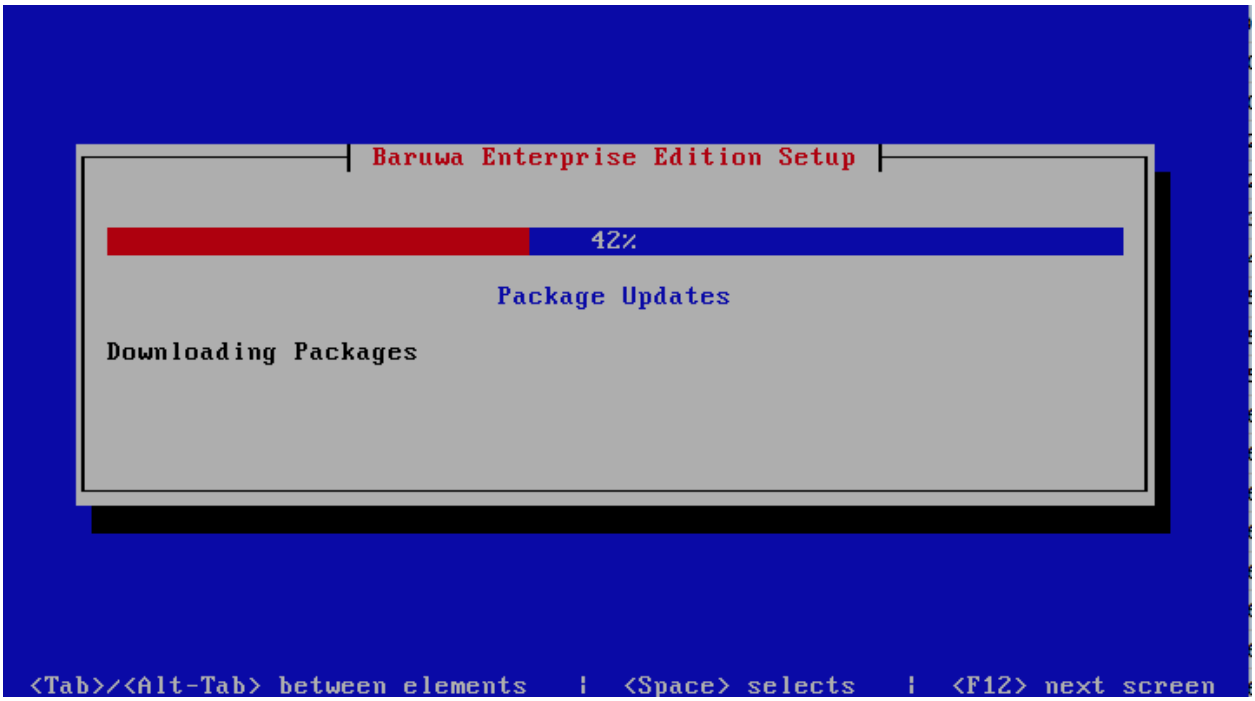


7.2.14 Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

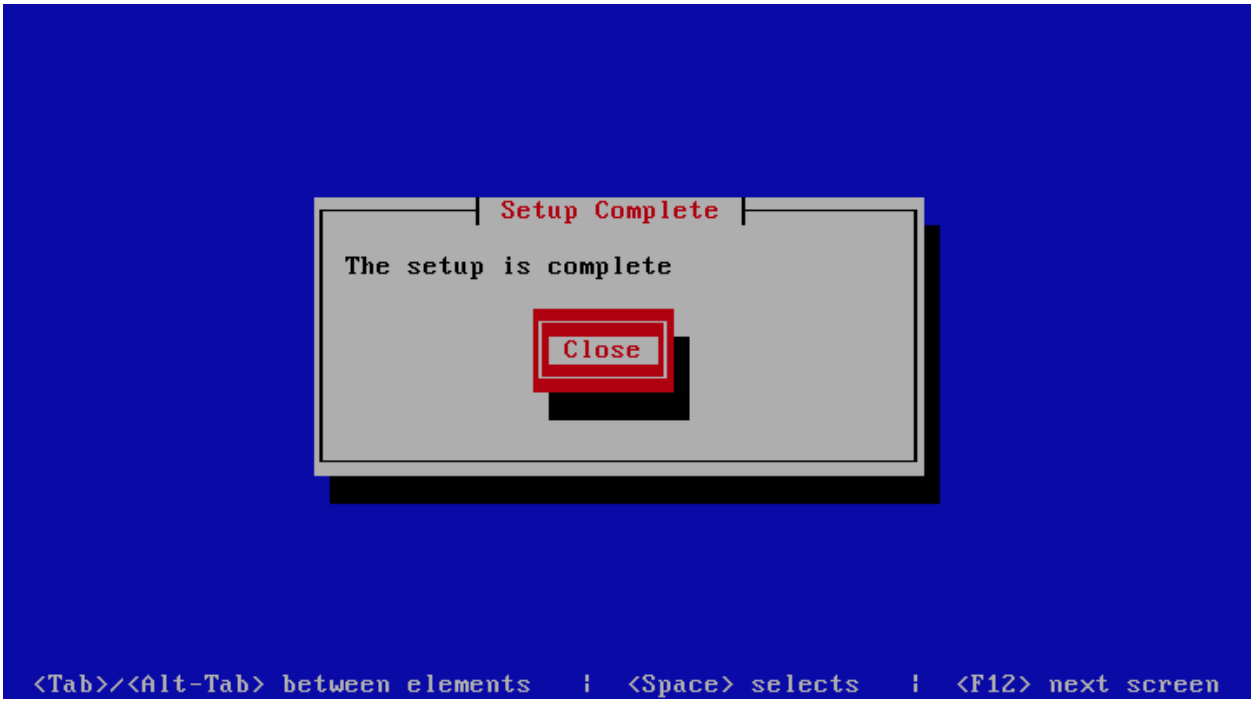
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

Warning: If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



7.2.15 Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

7.3 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a Scanning Node*, *Adding 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 to the Organization
- Add a delivery server for the Domain
- Add a Domain Administrator Account for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add any user accounts to the Domain if not using external authentication

Review the *DNS*, *Administrators guide*, *Email Protection Best Practices* and *Advanced configuration* sections for other configuration and setup options available.

CHAPTER

EIGHT

CLUSTER CONFIGURATION

In a cluster configuration each system has to be configured based on it's 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.

8.1 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 [Optional]

This profile is used in the *Single Backend Distributed Frontend* and *Single Backend Hybrid Frontend* topologies.

Servers setup using this profile can be setup as a *Bootstrap server*.

8.1.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

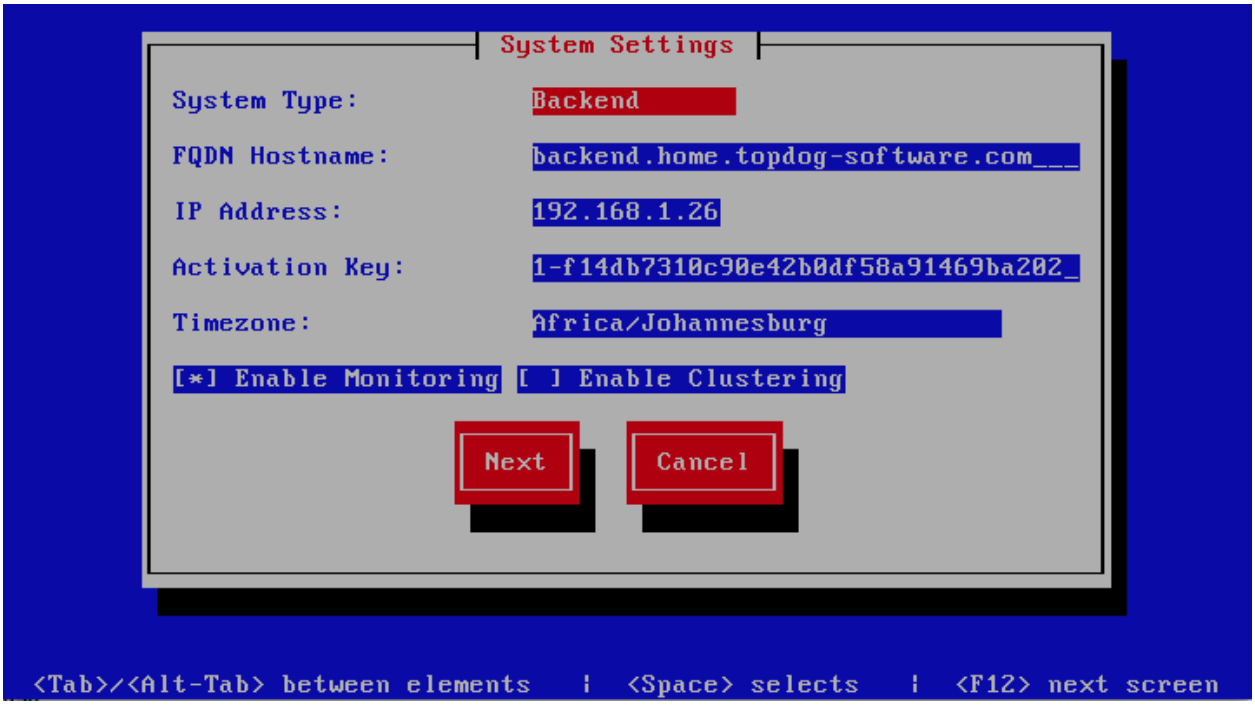
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

> **Warning:** Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

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	Check/Uncheck this to enable or disable backend segment *Clustering*
Enable Monitoring	Check this to enable the *Monitoring*

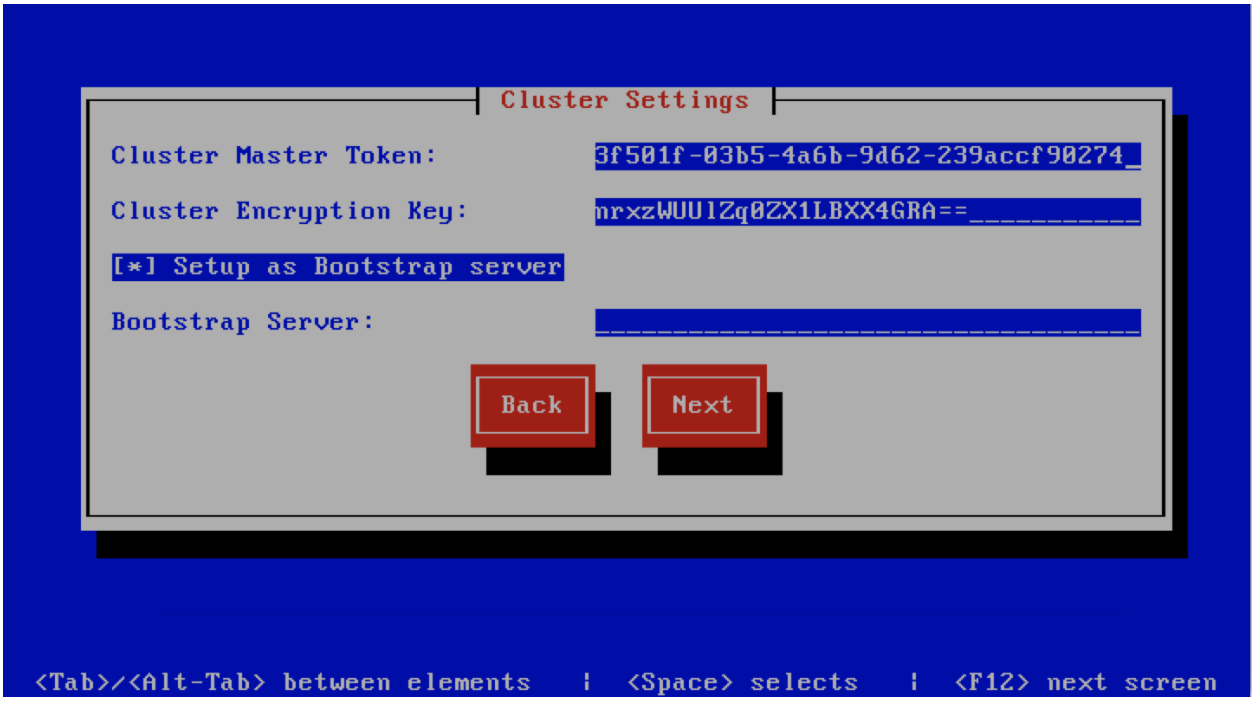


Cluster Settings

Note: This screen is only displayed if `enable clustering` is checked on the `System Settings` page.

This screen sets backend segment cluster settings. The description of the options is as follows:

Option	Description
Cluster Master Token	The cluster's master token, this is generated on the bootstrap server and it should be copied to other members in the cluster.
Cluster Encryption Key	The cluster's encryption key, this is generated on the bootstrap server and it should be copied to the other members in the cluster.
Setup as Bootstrap server	Check this on the first server to set it up as the bootstrap server. You can only have one server setup as a bootstrap server in a cluster.
Bootstrap server	The IP address of the bootstrap server, this is used on the subsequent servers that are setup after the first server.

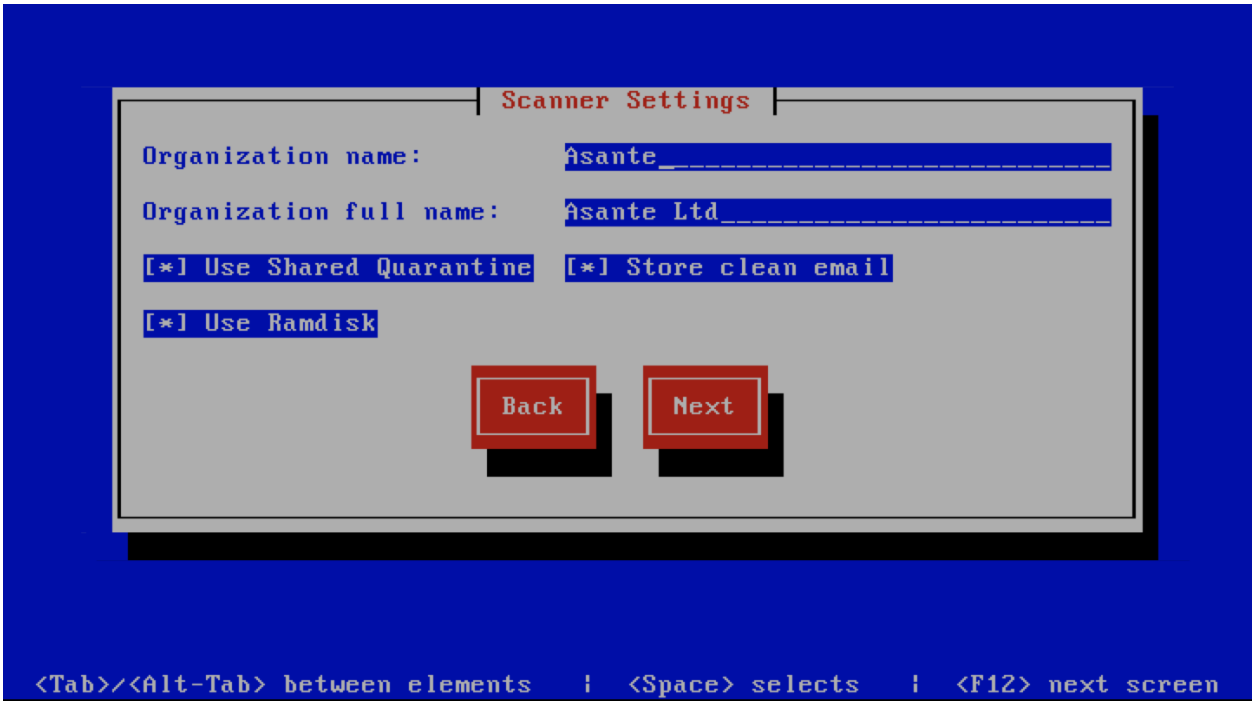


Scanner Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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 to enable *Shared quarantine* This option is only displayed if `enable clustering` is checked on the `System Settings` page.
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
Use Ramdisk	Check this to enable using a RAM disk for mail scanning This makes scanning more efficient, but it uses 1GB of RAM. Make sure you provision sufficient RAM.

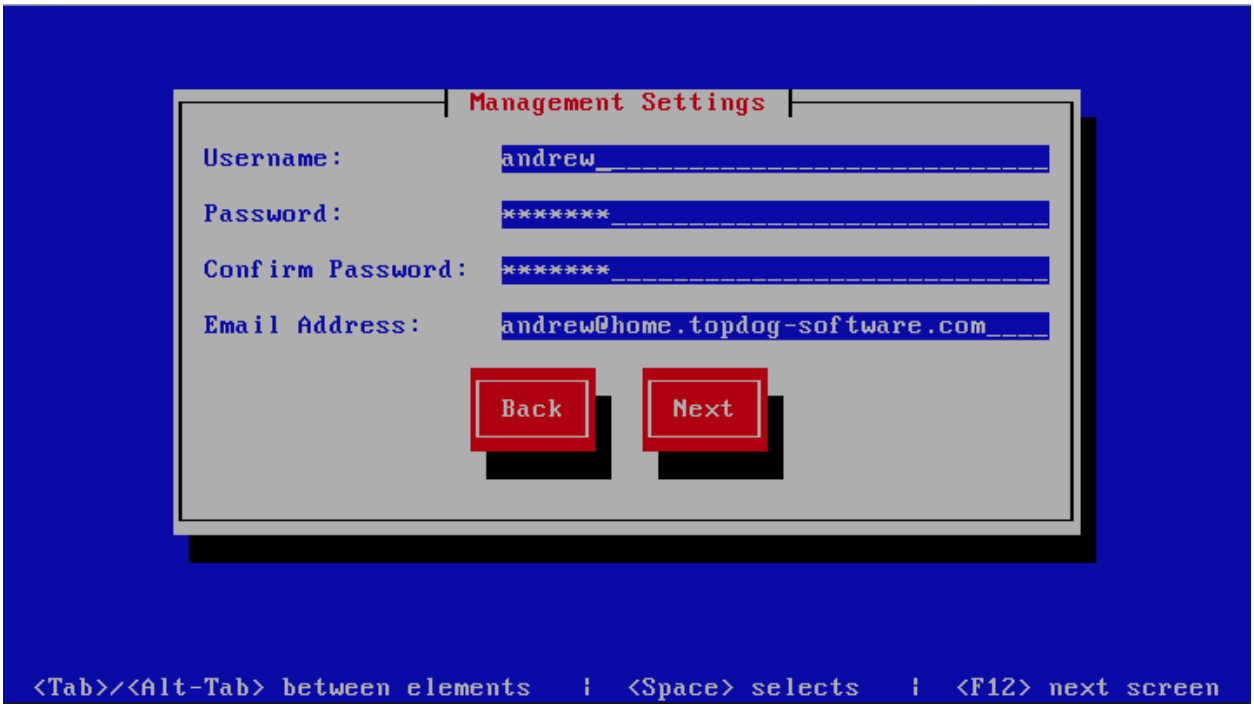


Management Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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 passwordsgenerator.net to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address

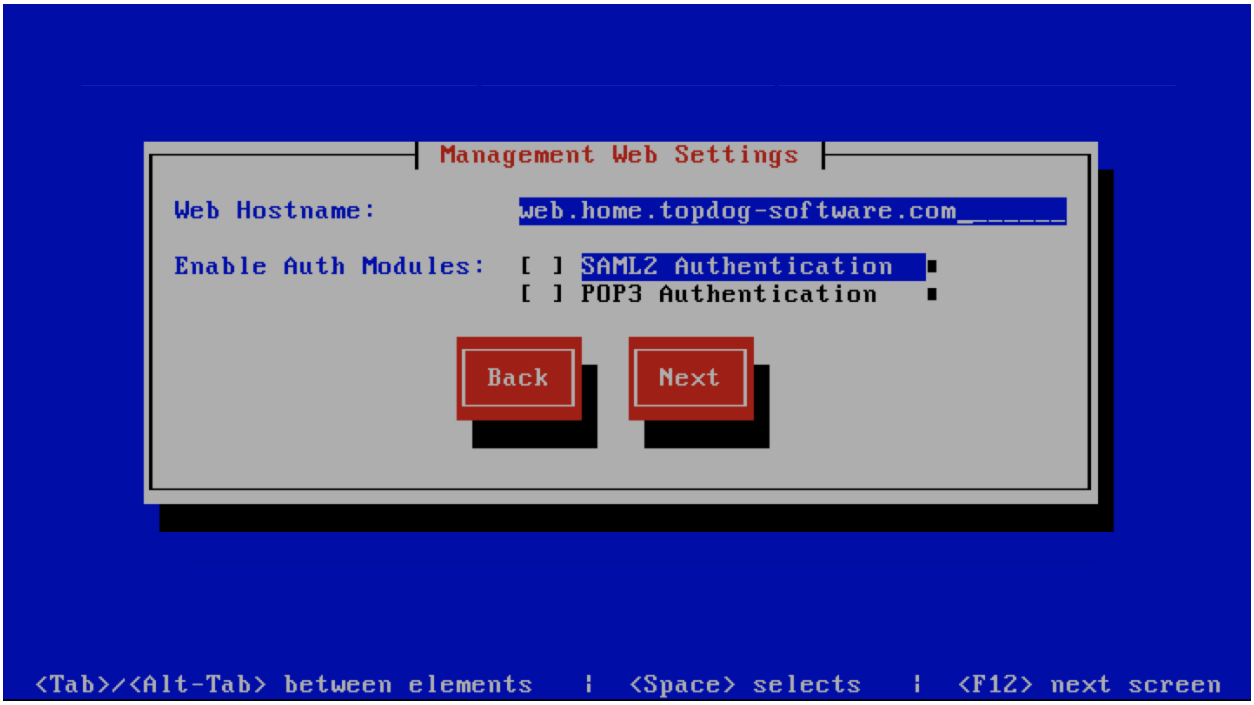


Management Web Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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
Enable Auth Modules	The external authentication modules to enable

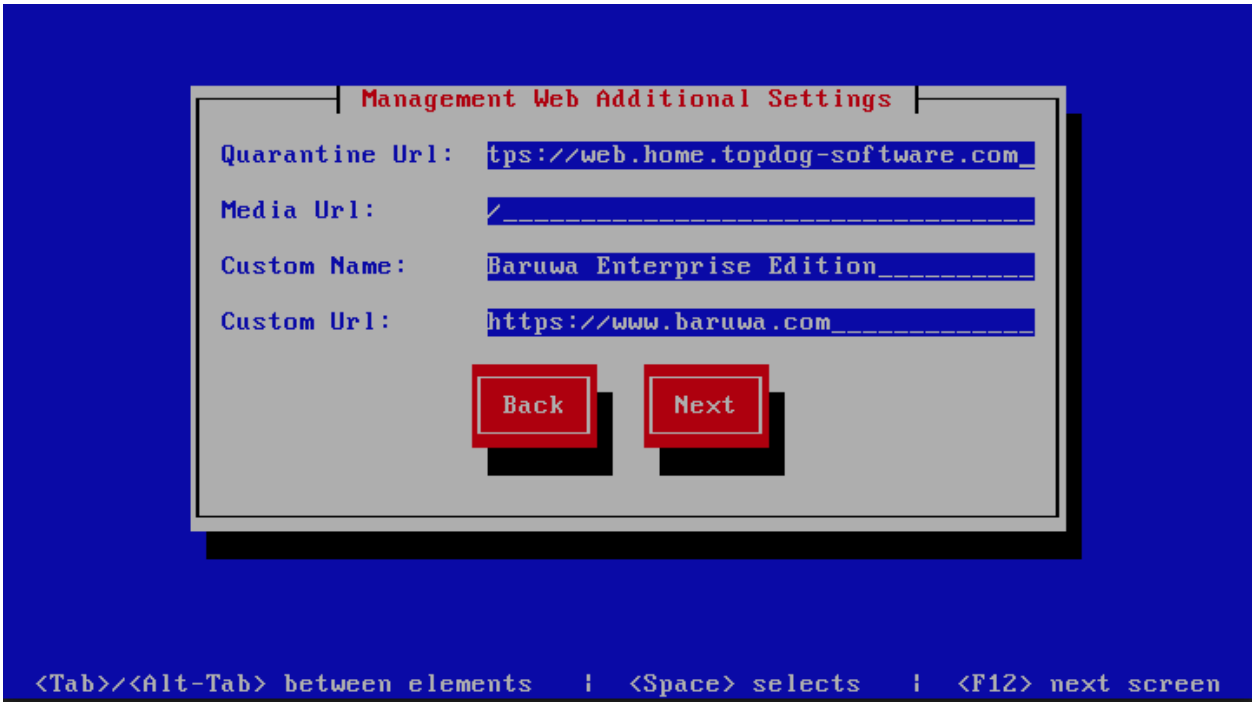


Management Web Additional Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

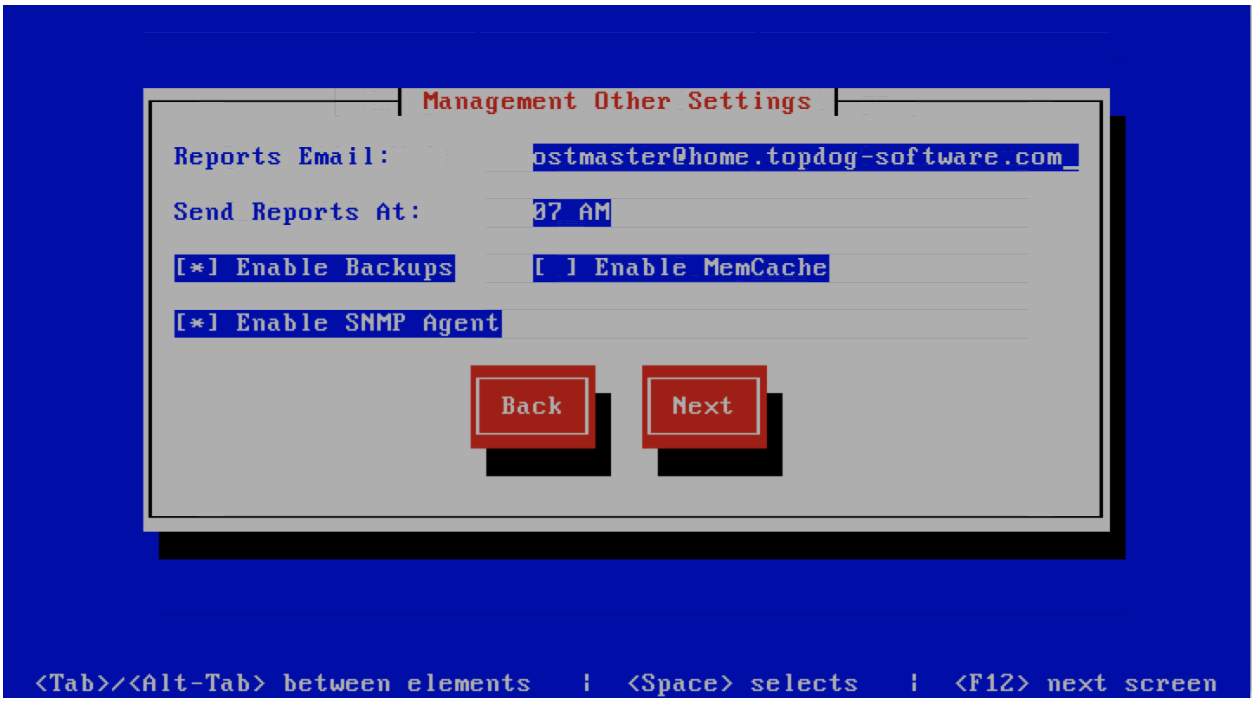
Option	Description
Quarantine URL	This is default host url used in quarantine report links, is overridden by domain settings.
Media URL	This can allow you to host media on a CDN or media host, leave as default to serve of the same system.
Custom Name	This will replace all occurrences of Baruwa in the 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

This 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
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable Memcache	Enables or disables the Memcached cache system, when disabled the builtin cache system will be used. The builtin cache system is more efficient on standalone systems
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.

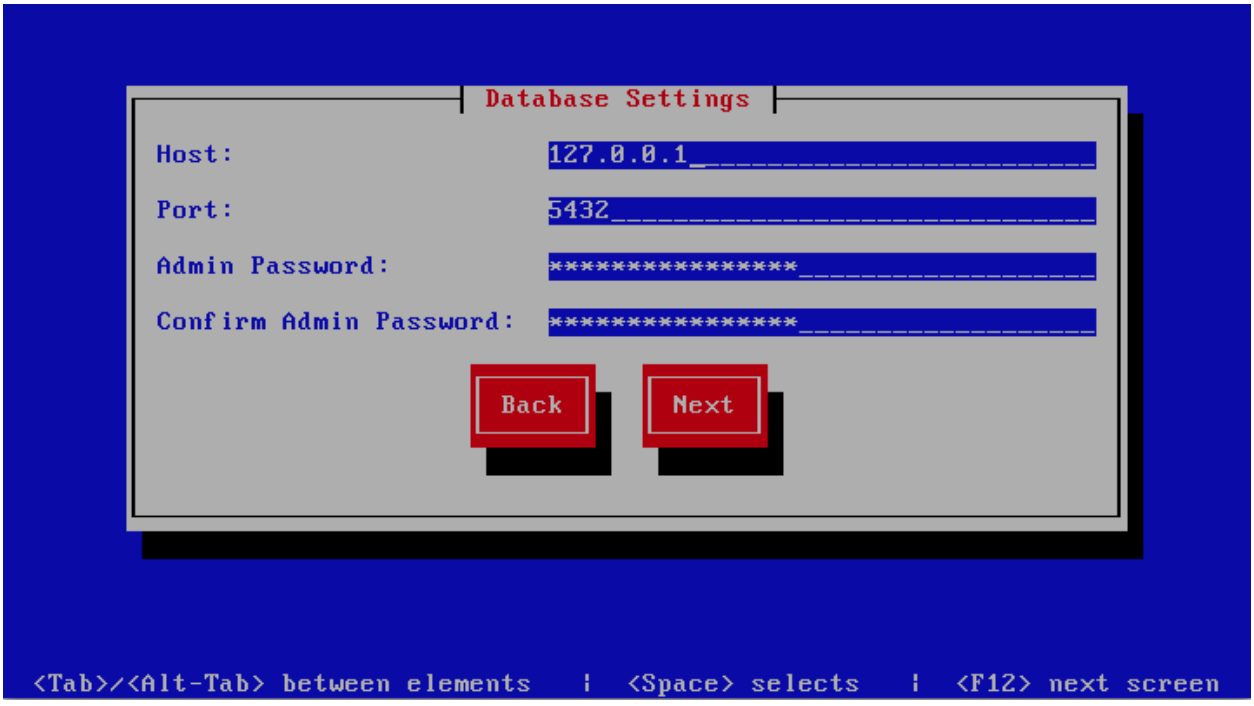


Database Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

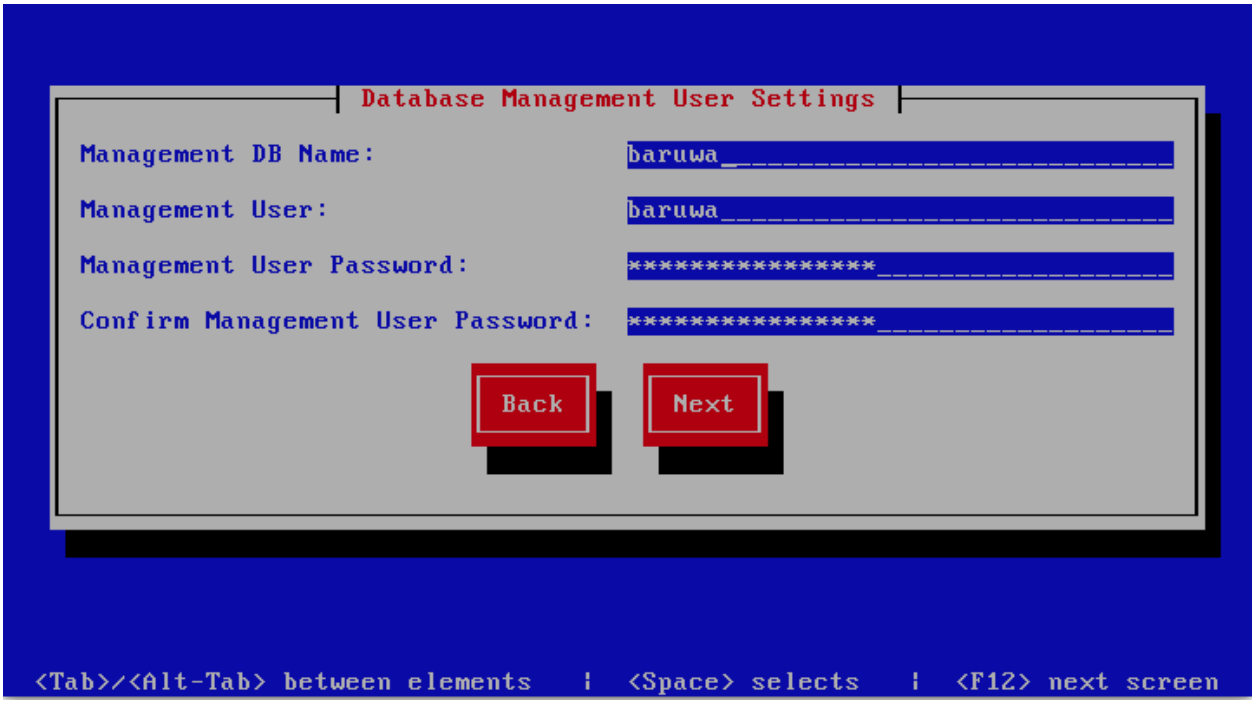


Database Management User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

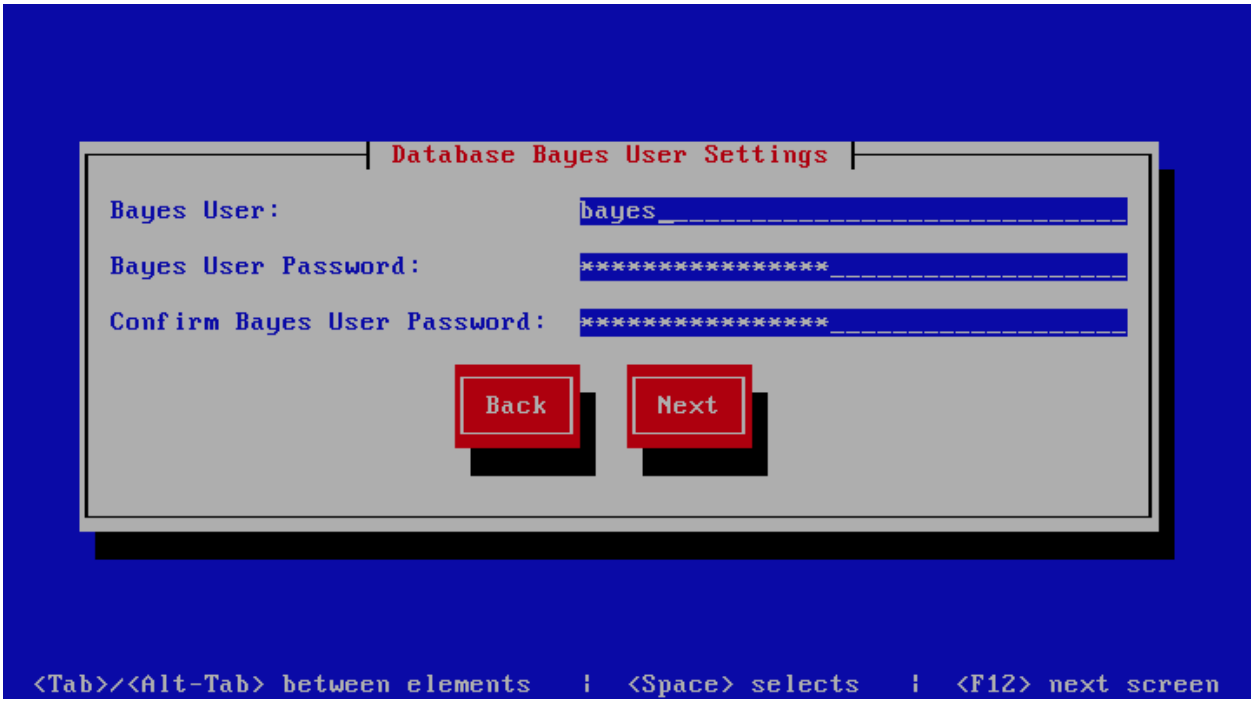


Database Bayes User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

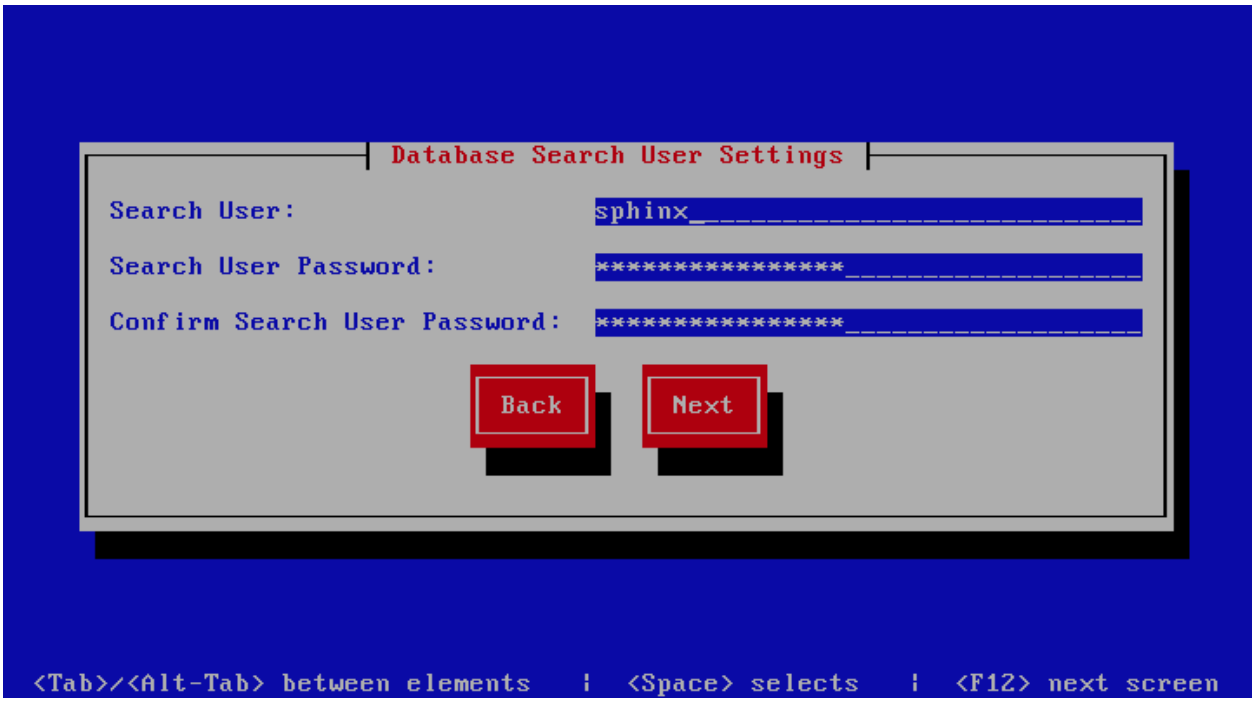


Database Search User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

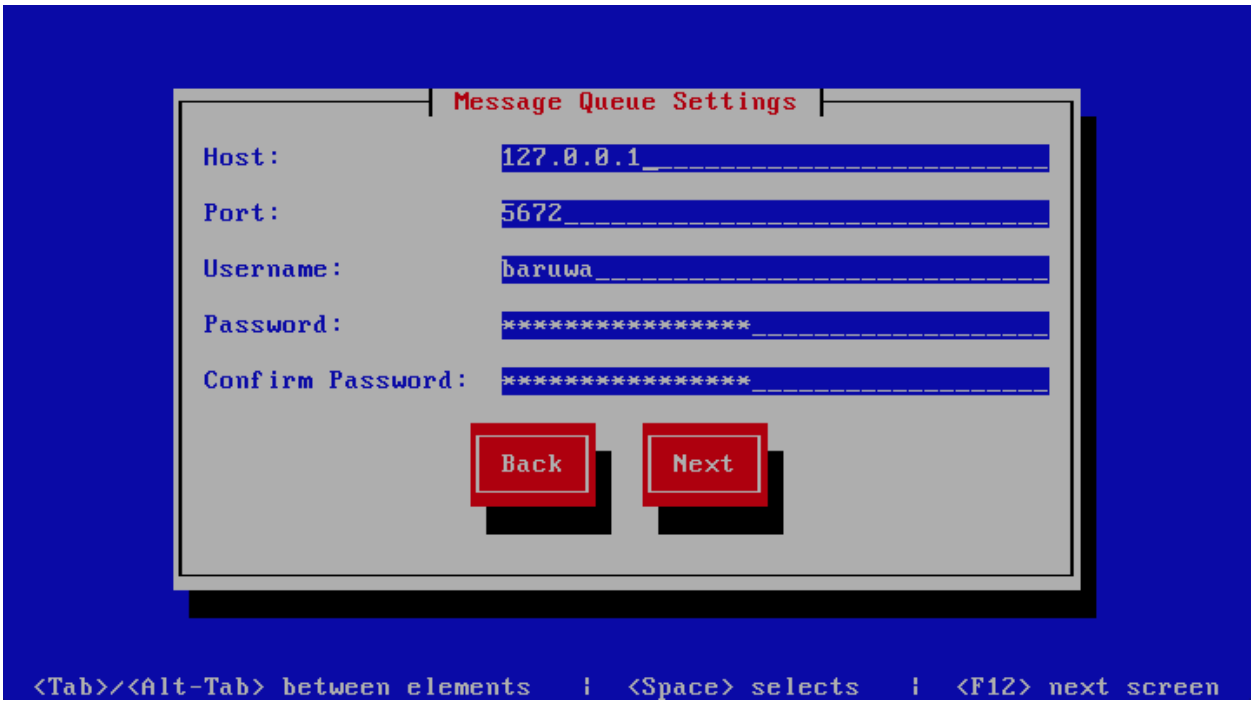


Message Queue Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

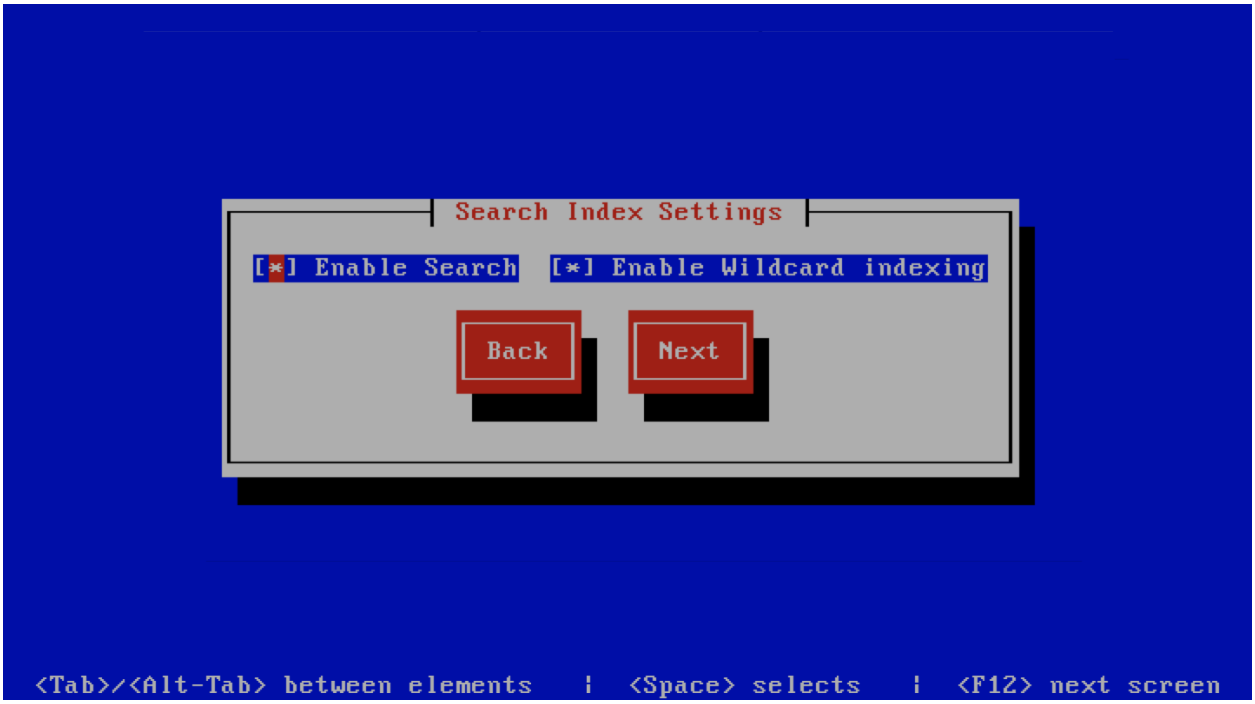


Search Index Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
Enable Search	Enables Search functionality
Enable wildcard indexing	Enables Search wildcard indexing, Setting this to true will generate very large index files.

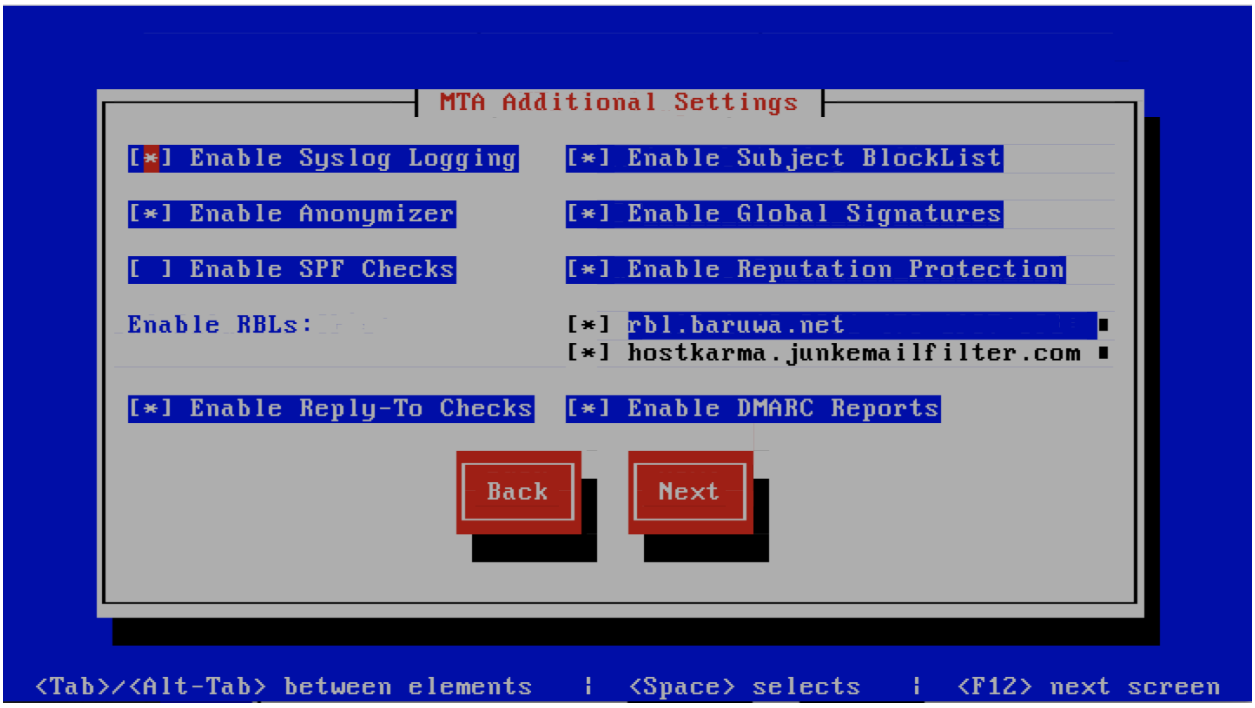


MTA Additional Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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
Enable Reply-To Checks	Enable Empty Reply-To Checks
Enable DMARC Reports	Enable DMARC Reports

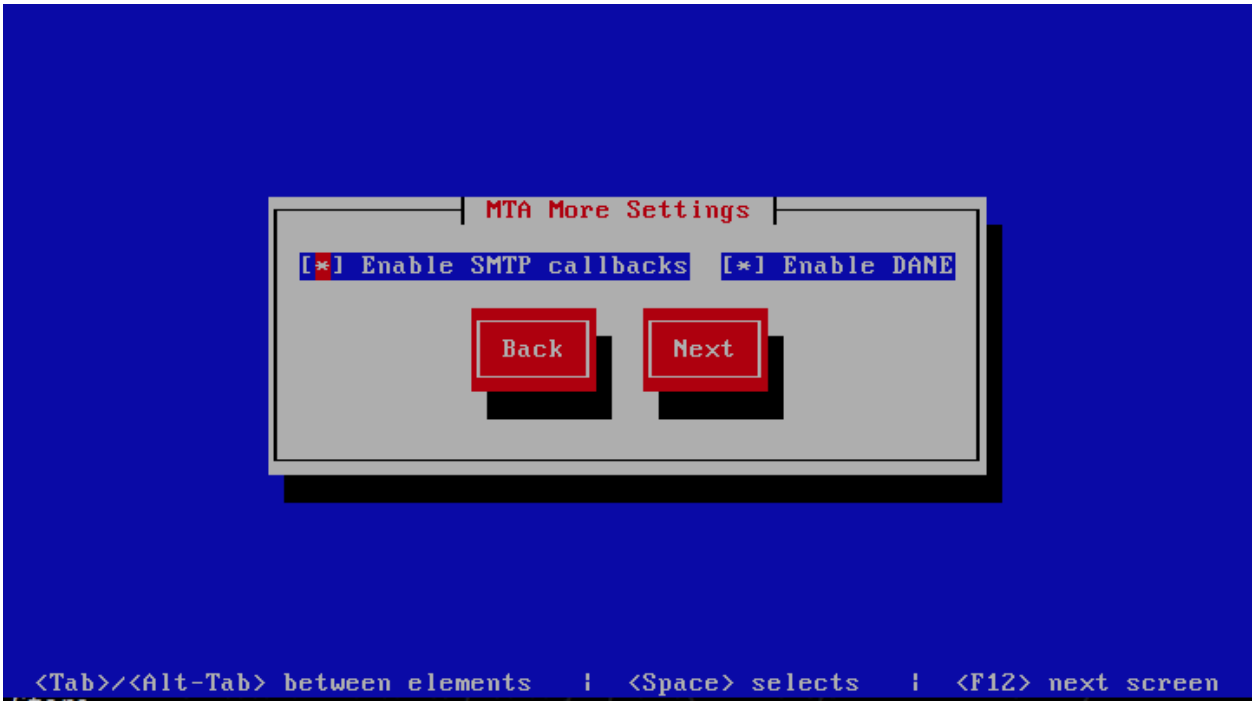


MTA More Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
Enable SMTP callbacks	Enable SMTP Callback verification for senders who do not have reverse DNS records configured.
Enable DANE	Enable the DANE protocol support.

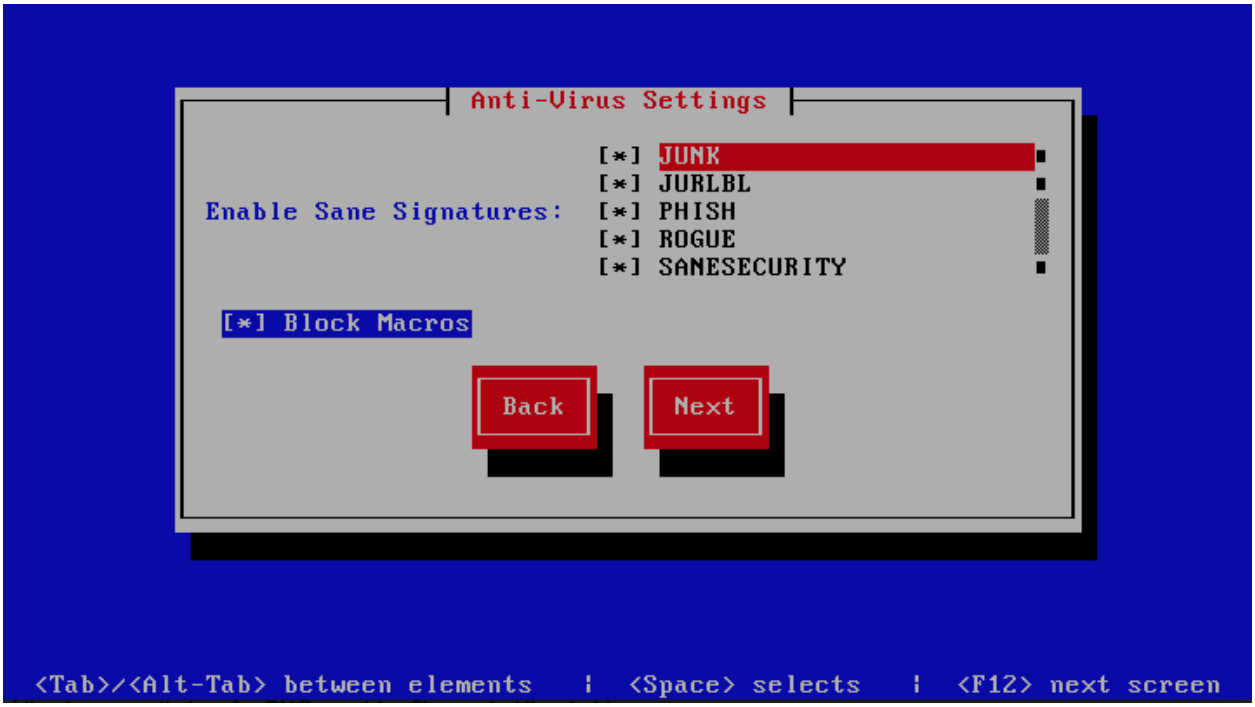


Anti Virus Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Block Macros	Block documents that contain macros

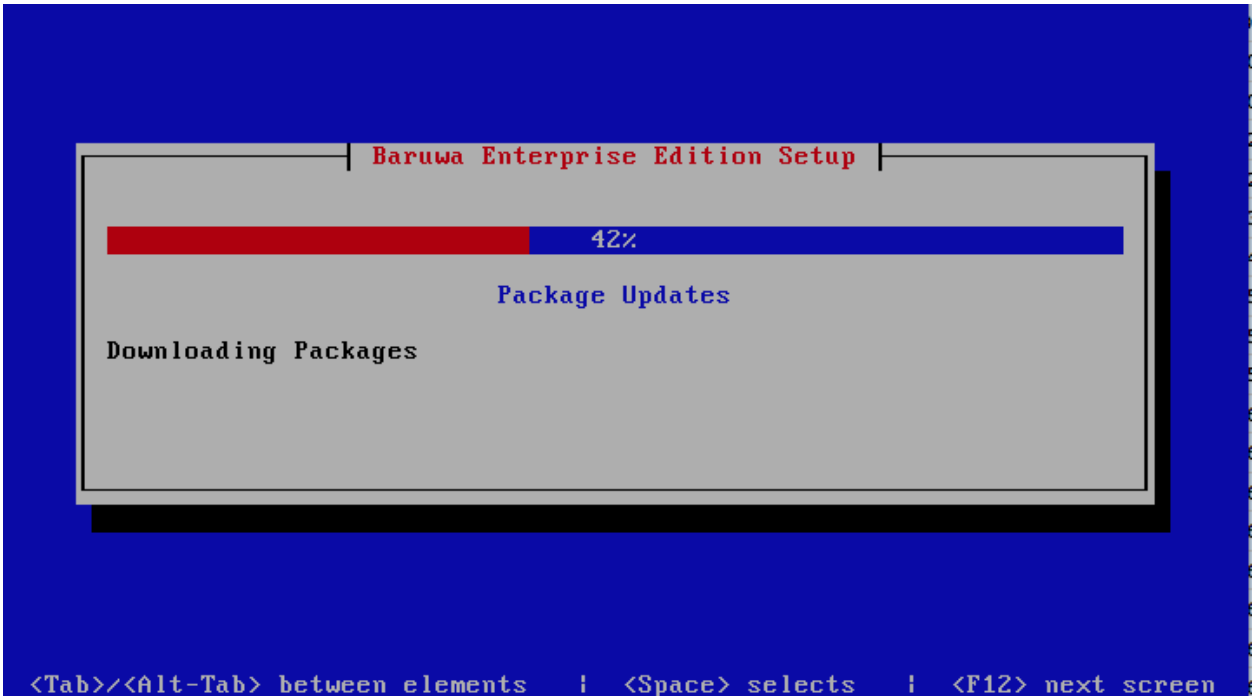


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

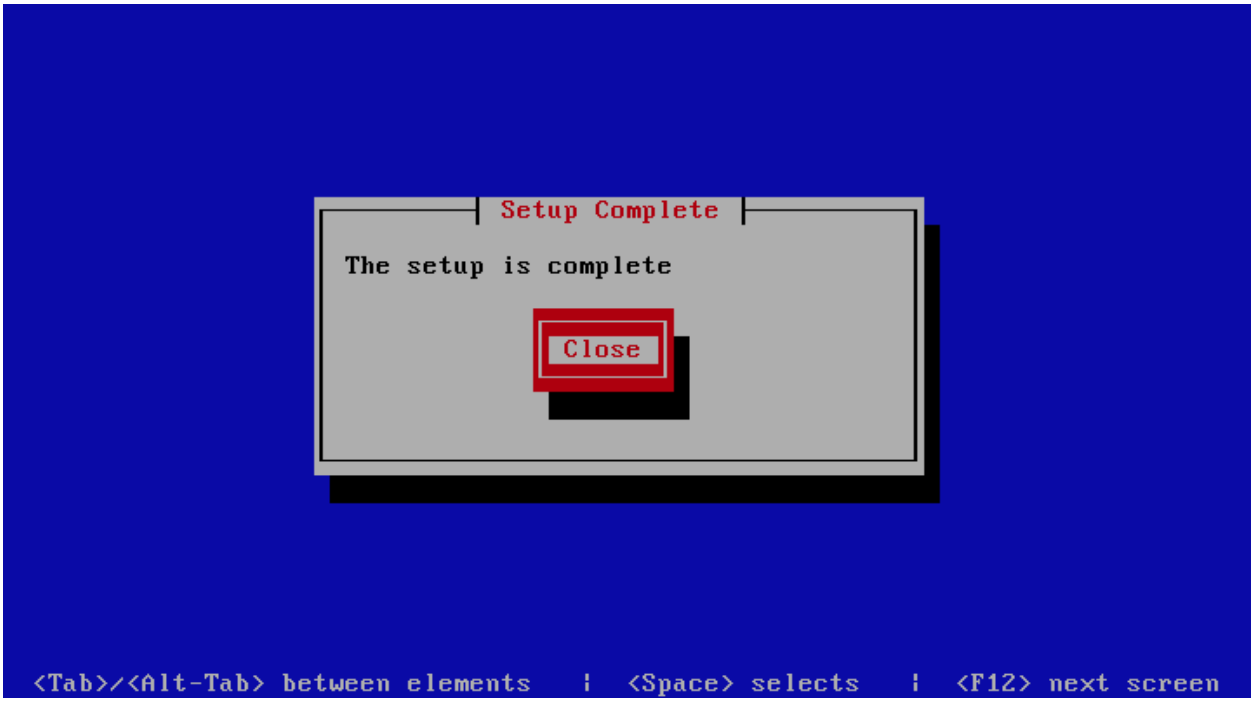
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

> **Warning:** If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.2 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

Servers setup using this profile can be setup as a *Bootstrap server*.

8.2.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

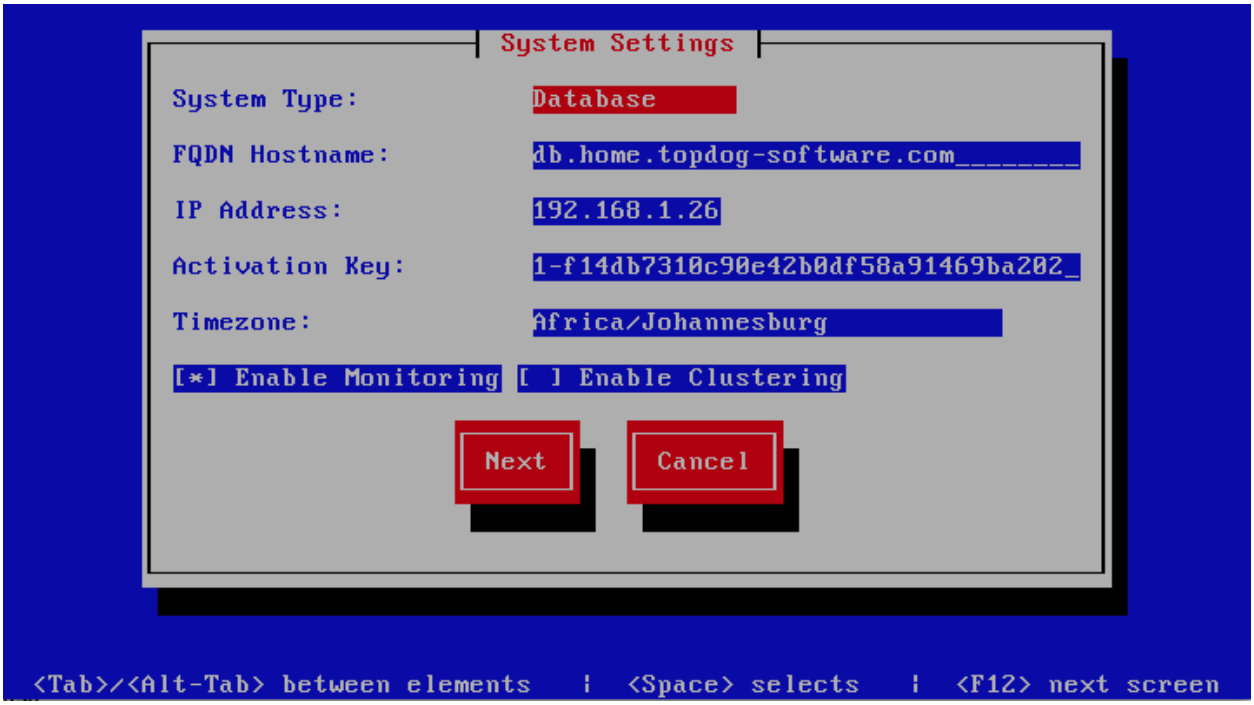
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

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	Check/Uncheck this to enable or disable backend segment *Clustering*
Enable Monitoring	Check this to enable the *Monitoring*

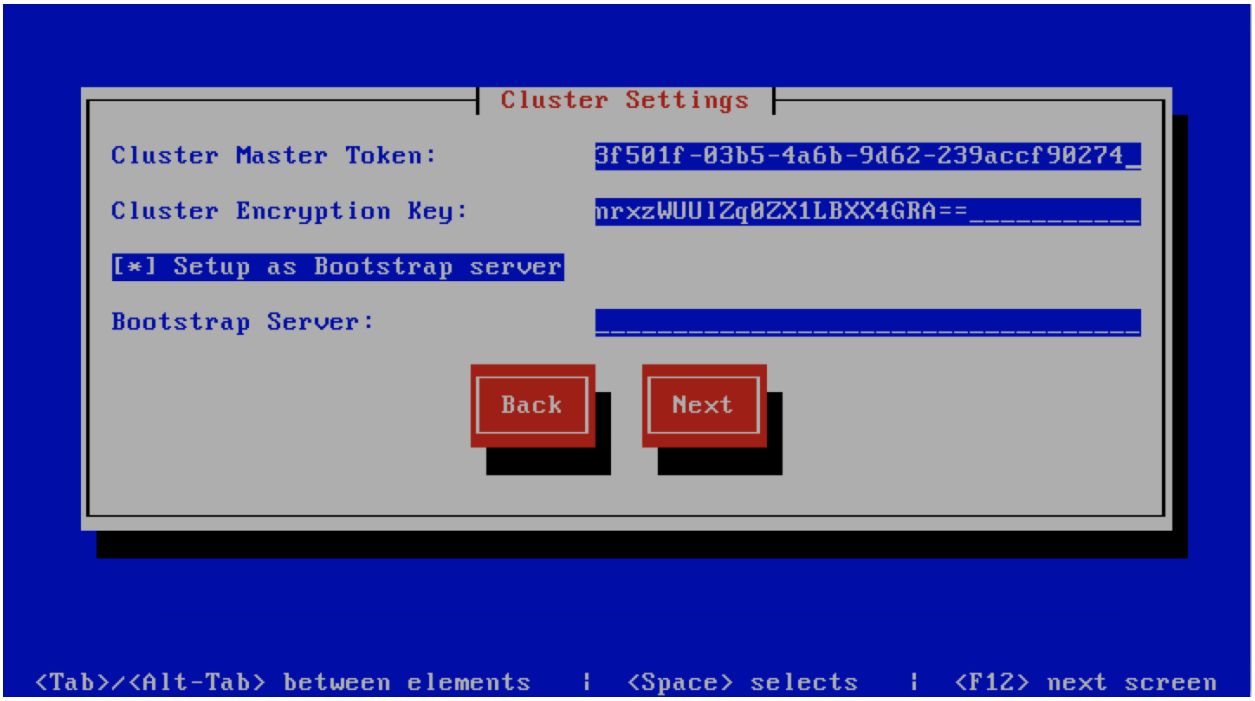


Cluster Settings

Note: This screen is only displayed if `enable clustering` is checked on the `System Settings` page.

This screen sets backend segment cluster settings. The description of the options is as follows:

Option	Description
Cluster Master Token	The cluster's master token, this is generated on the bootstrap server and it should be copied to other members in the cluster.
Cluster Encryption Key	The cluster's encryption key, this is generated on the bootstrap server and it should be copied to the other members in the cluster.
Setup as Bootstrap server	Check this on the first server to set it up as the bootstrap server. You can only have one server setup as a bootstrap server in a cluster.
Bootstrap server	The IP address of the bootstrap server, this is used on the subsequent servers that are setup after the first server.

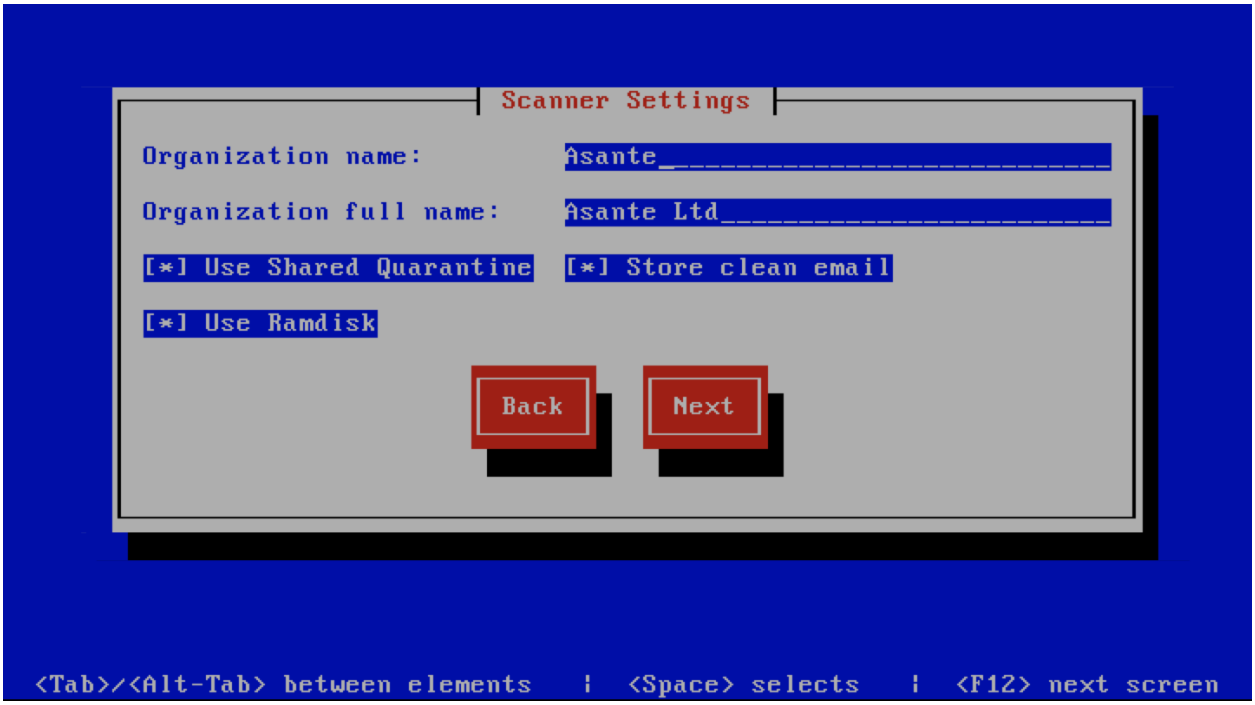


Scanner Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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 to enable *Shared quarantine* This option is only displayed if `enable clustering` is checked on the `System Settings` page.
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
Use Ramdisk	Check this to enable using a RAM disk for mail scanning This makes scanning more efficient, but it uses 1GB of RAM. Make sure you provision sufficient RAM.

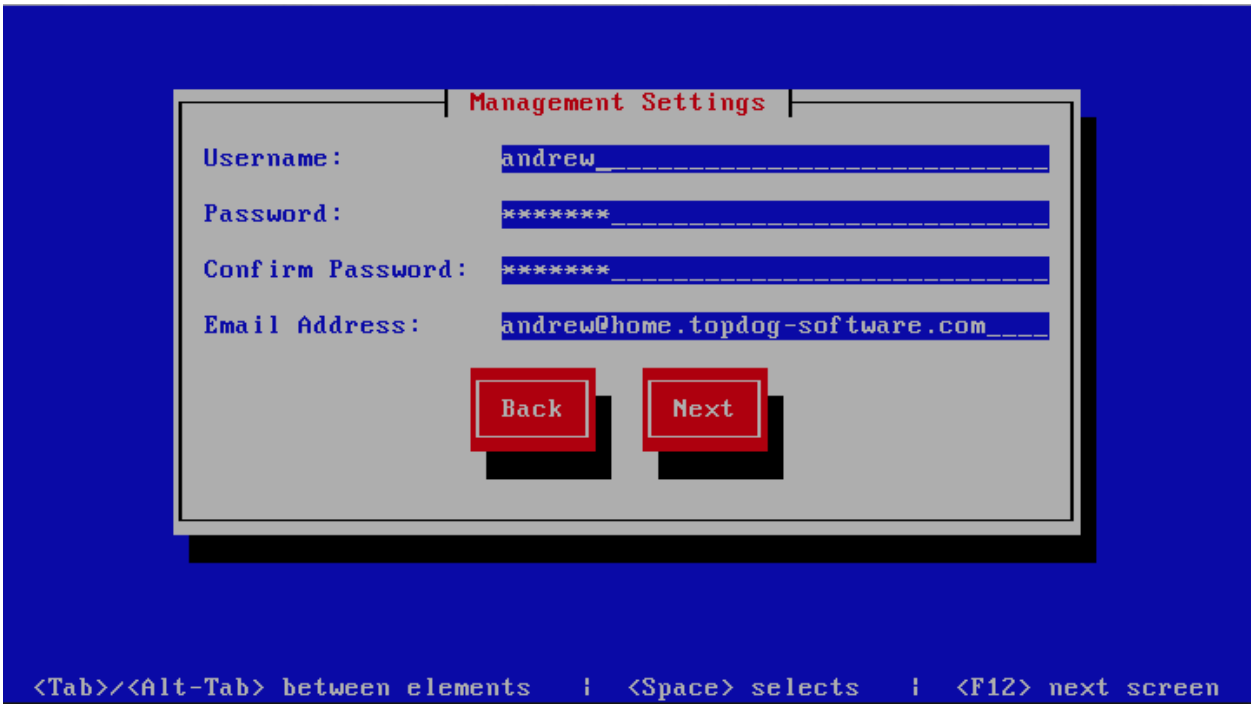


Management Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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 passwordsgenerator.net to generate strong passwords
Confirm Password	Renter the Administrator password
Email Address	Administrator email address

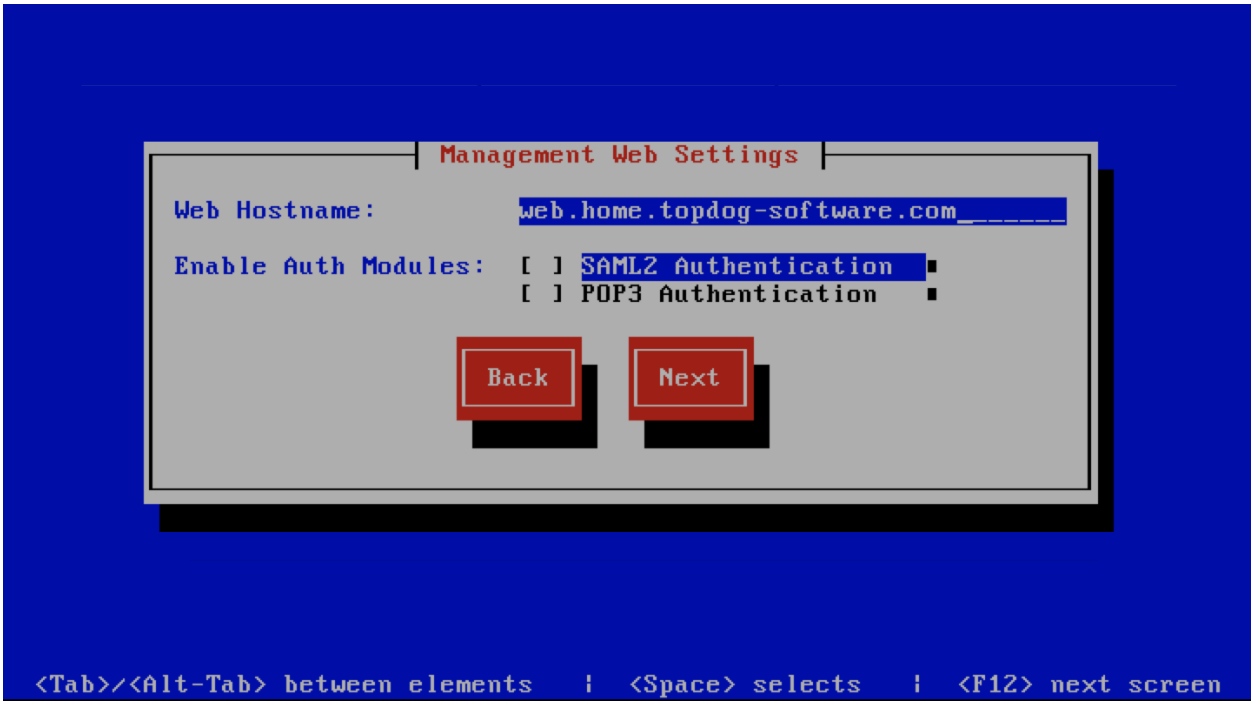


Management Web Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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
Enable Auth Modules	The external authentication modules to enable

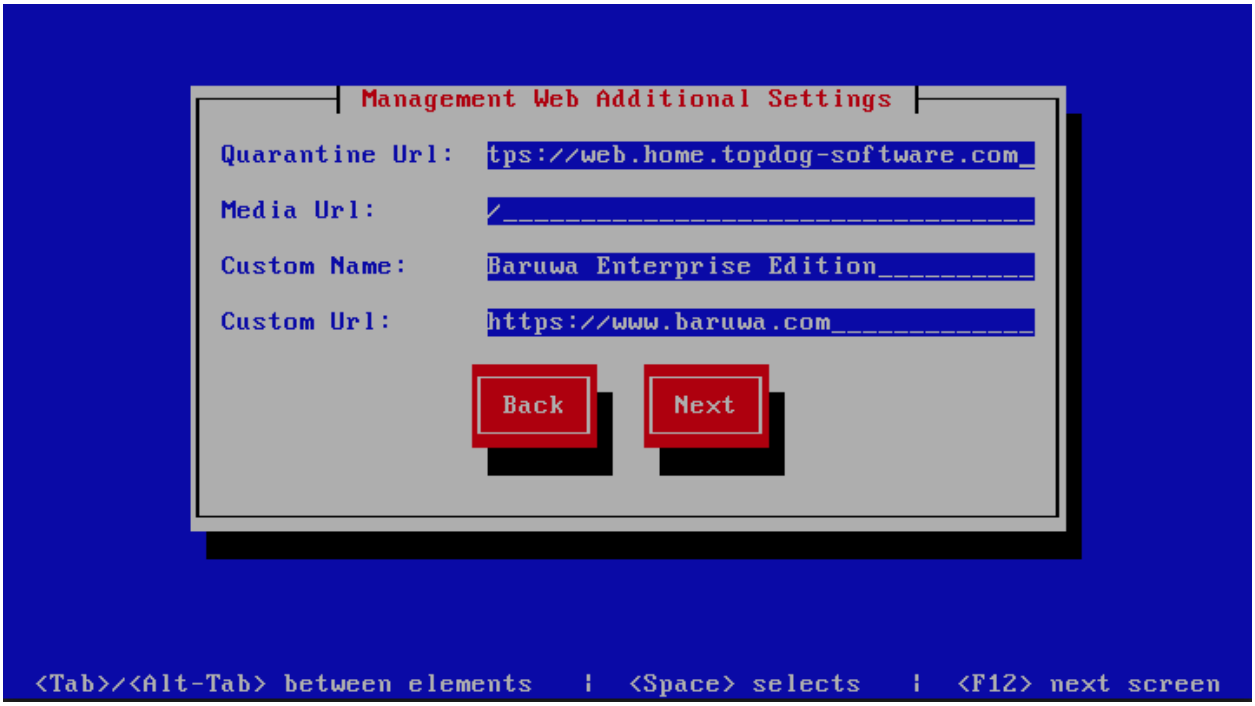


Management Web Additional Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
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.

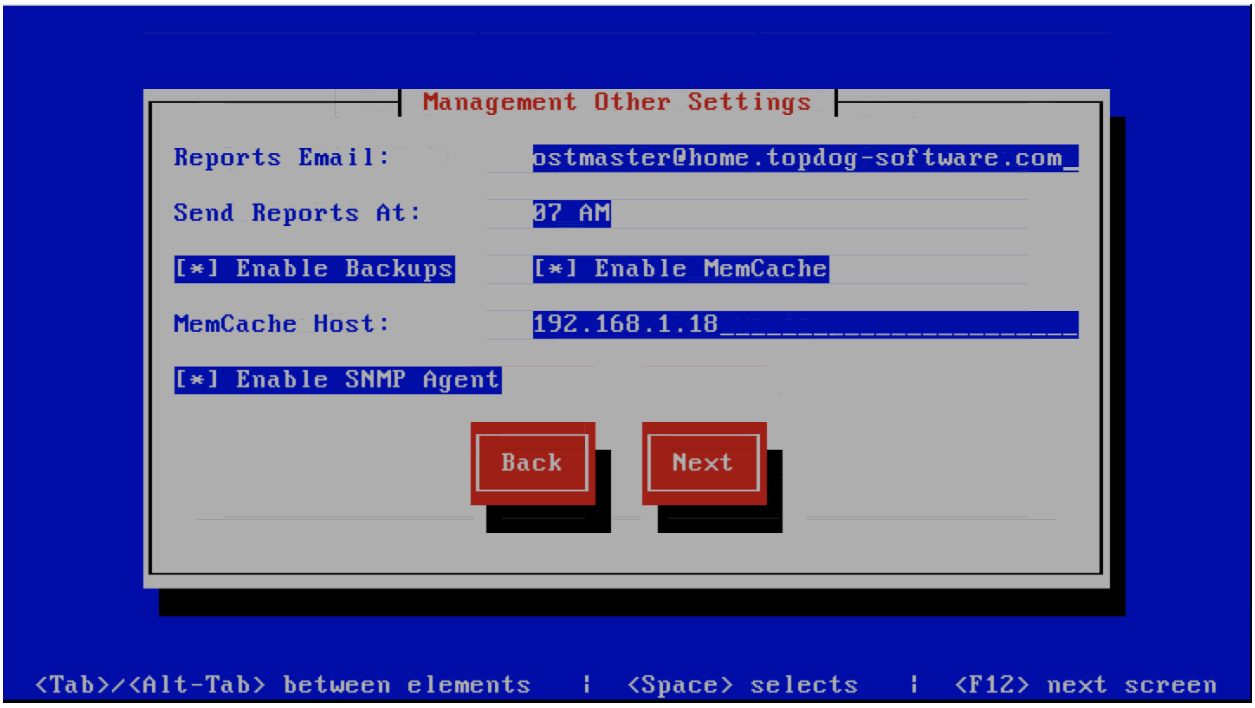


Management Other Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable Memcache	Enables or disables the Memcached cache system, when disabled the builtin cache system will be used. The builtin cache system is more efficient on standalone systems
MemCache Host	The IP address of the Memcached server
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.

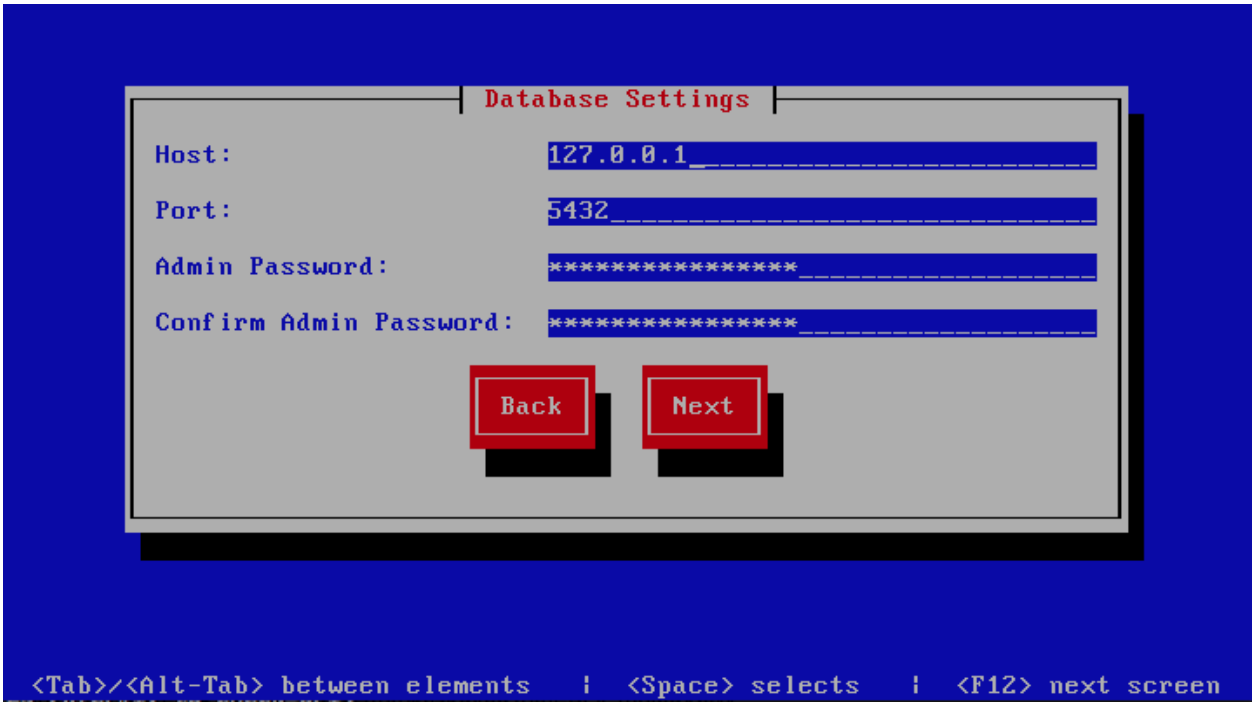


Database Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

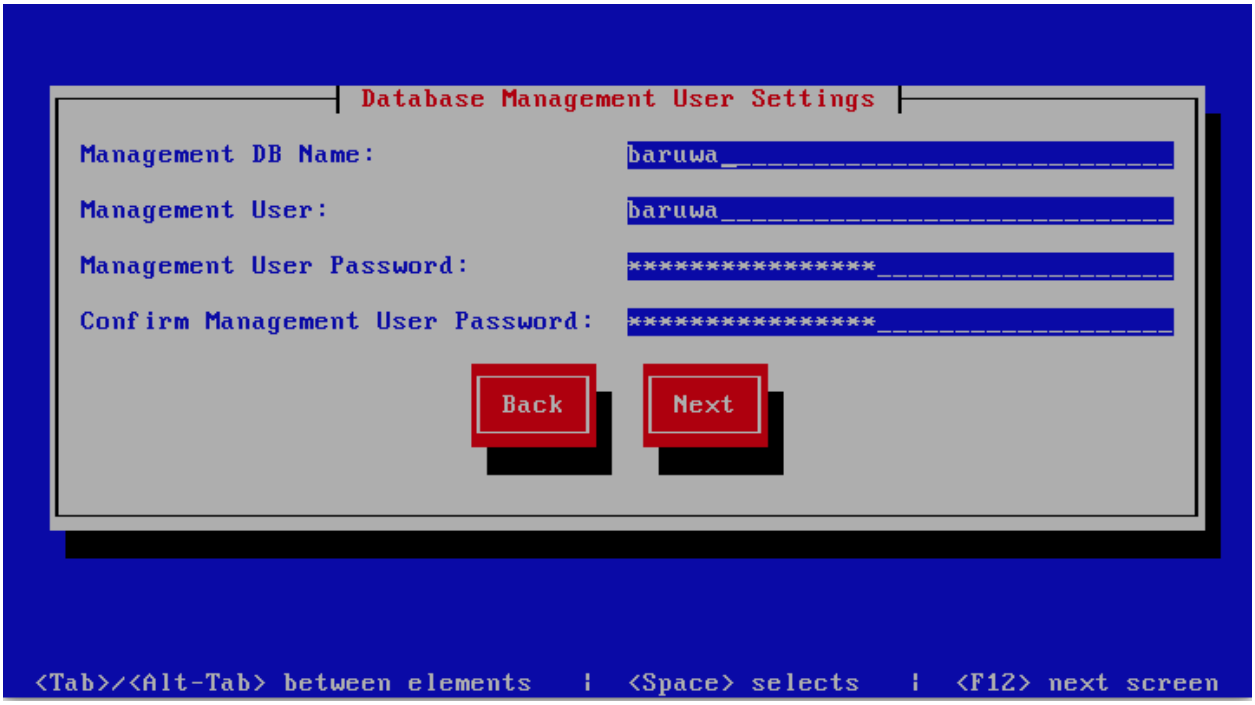


Database Management User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

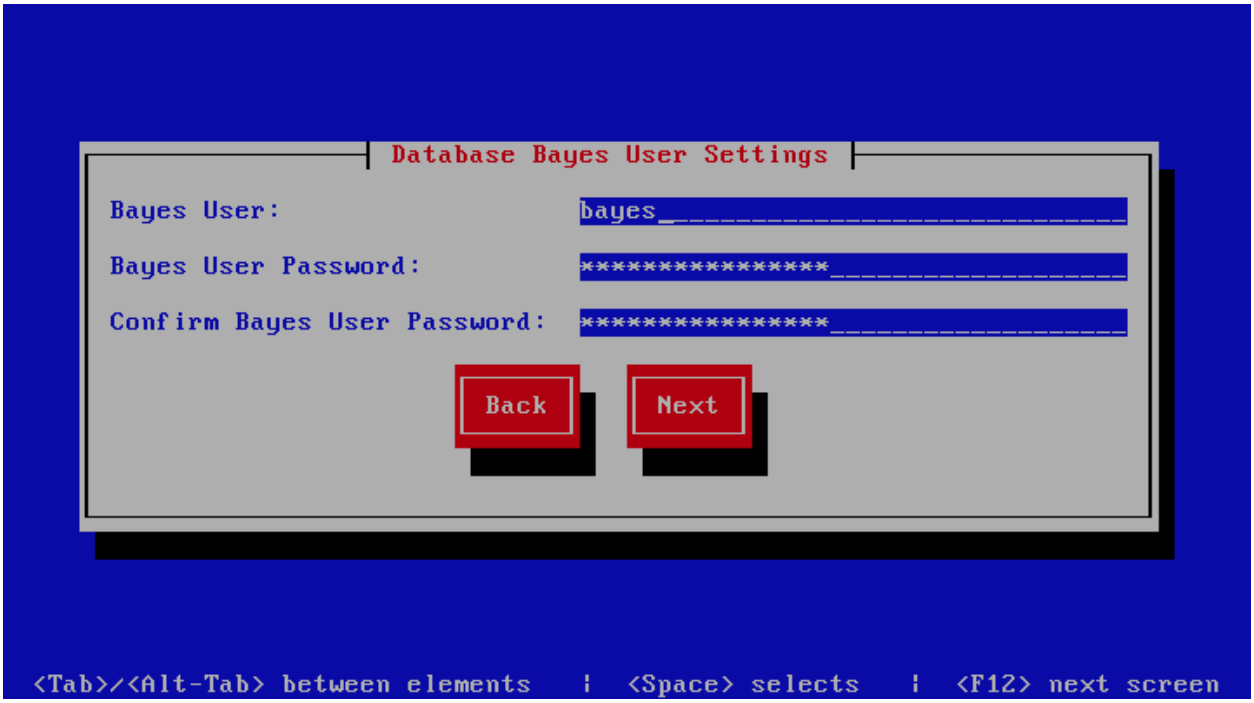


Database Bayes User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

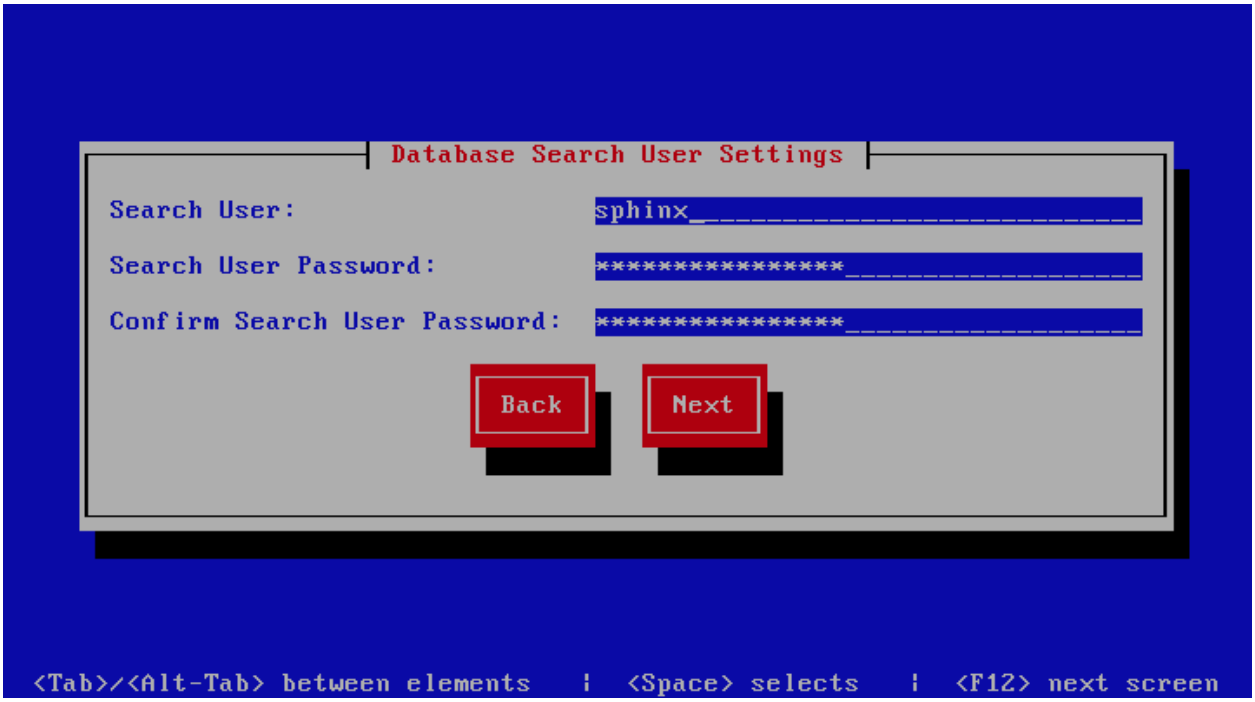


Database Search User Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

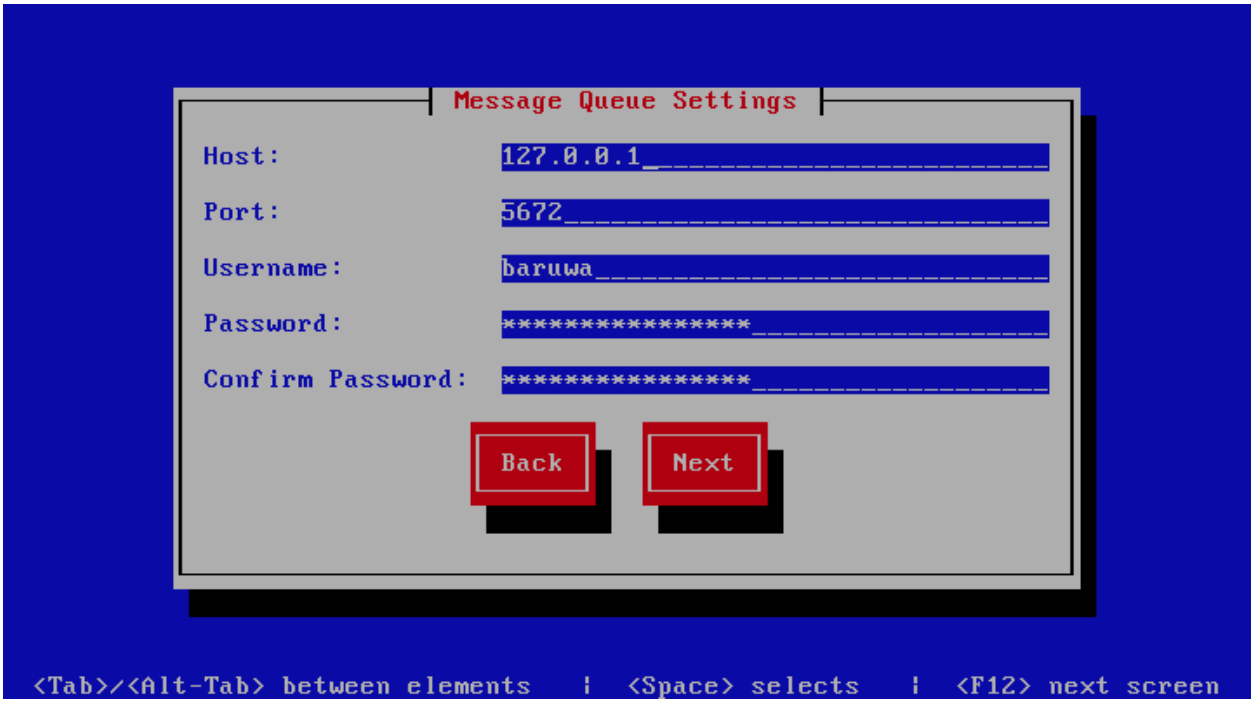


Message Queue Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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

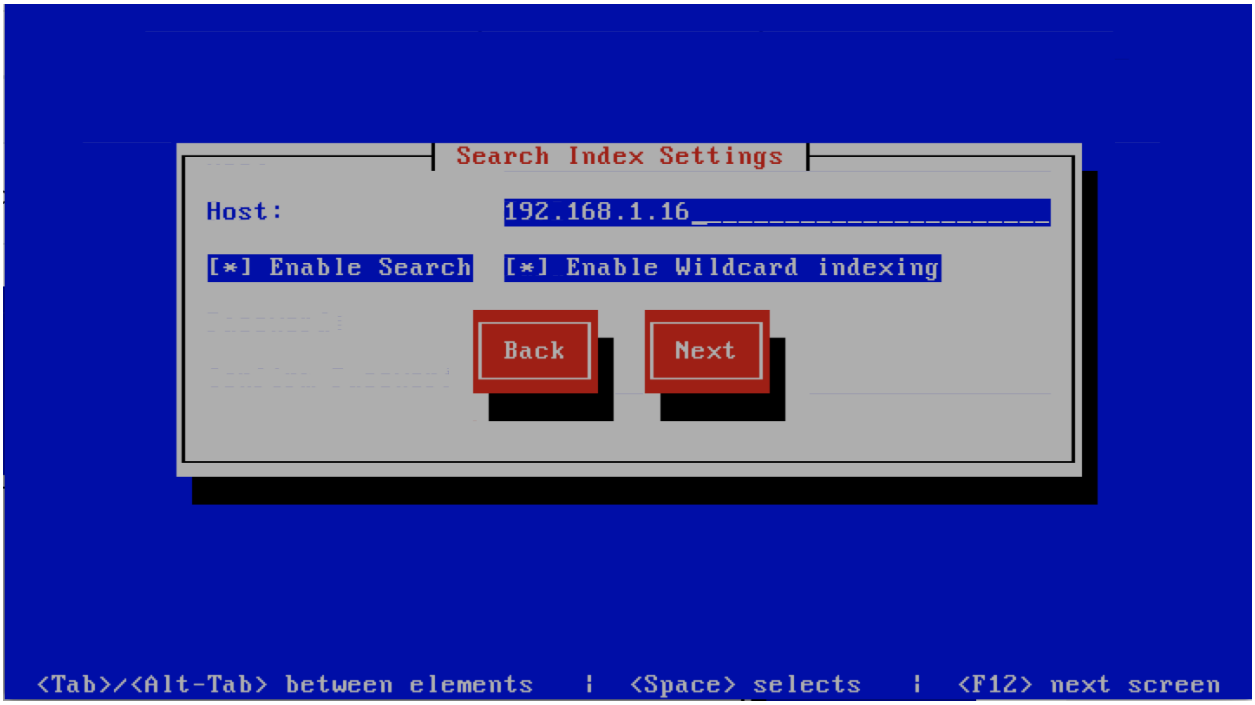


Search Index Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

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

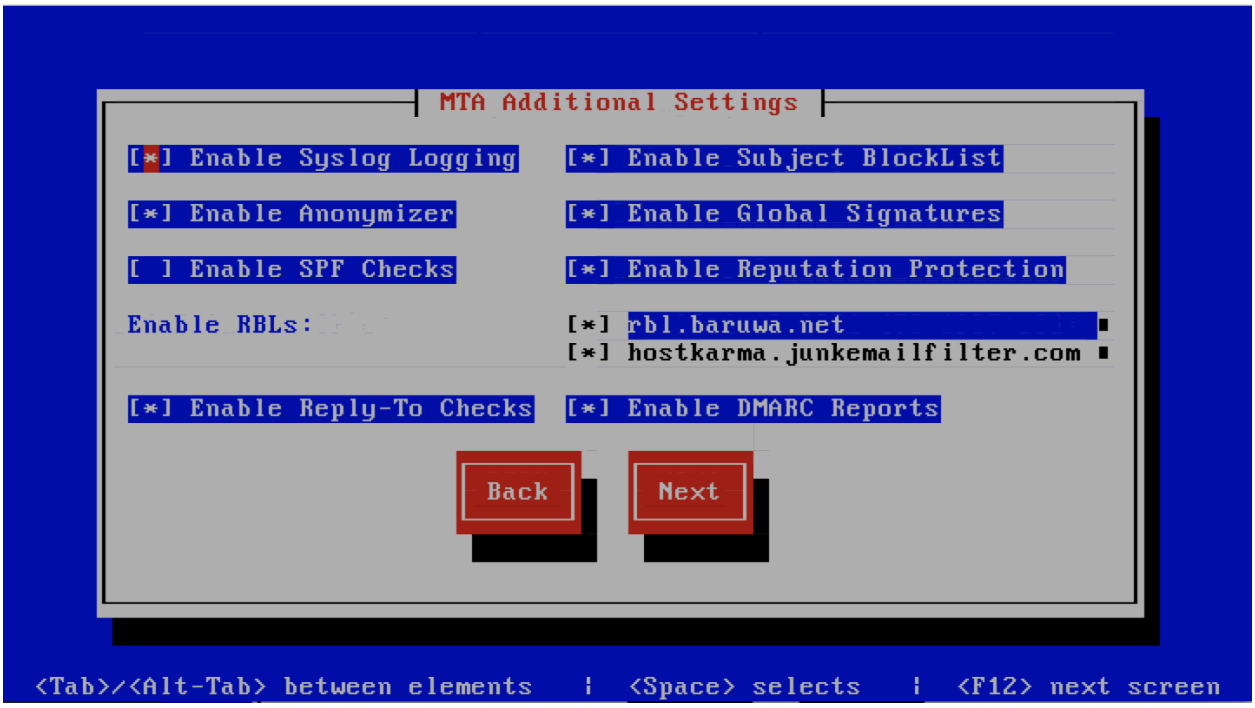


MTA Additional Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

This 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
Enable Reply-To Checks	Enable Empty Reply-To Checks
Enable DMARC Reports	Enable DMARC Reports

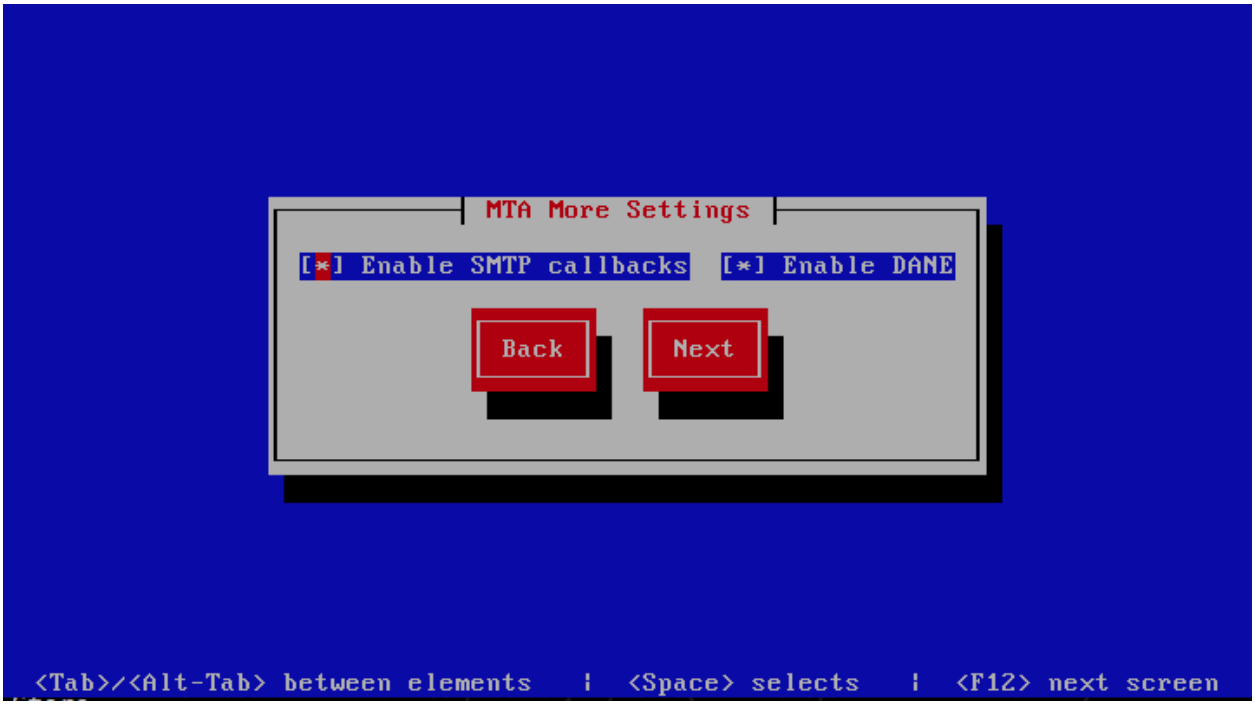


MTA More Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
Enable SMTP callbacks	Enable SMTP Callback verification for senders who do not have reverse DNS records configured.
Enable DANE	Enable the DANE protocol support.

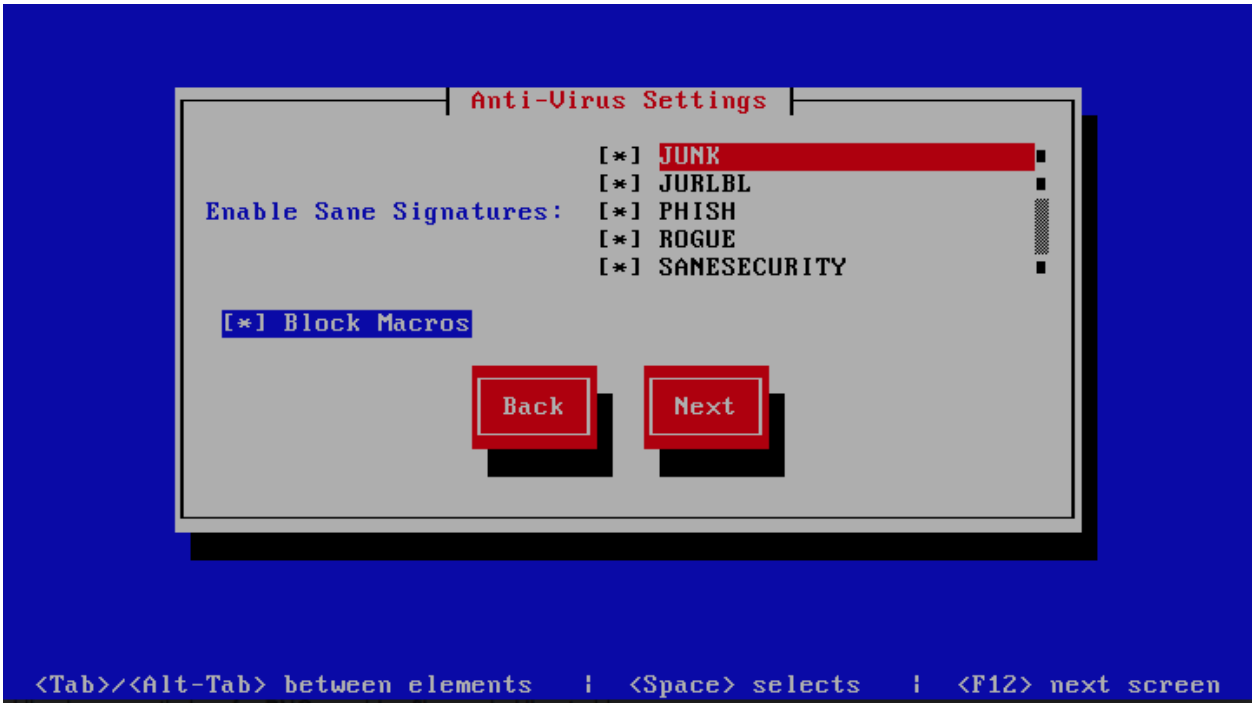


Anti Virus Settings

Note: This screen is only displayed if `Setup as Bootstrap server` is checked on the `Cluster Settings` page or `Enable clustering` is unchecked on the `System Settings` page.

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

Option	Description
Enable Sane Signatures	ClamAV Unofficial Sane signatures to enable
Block Macros	Block documents that contain macros

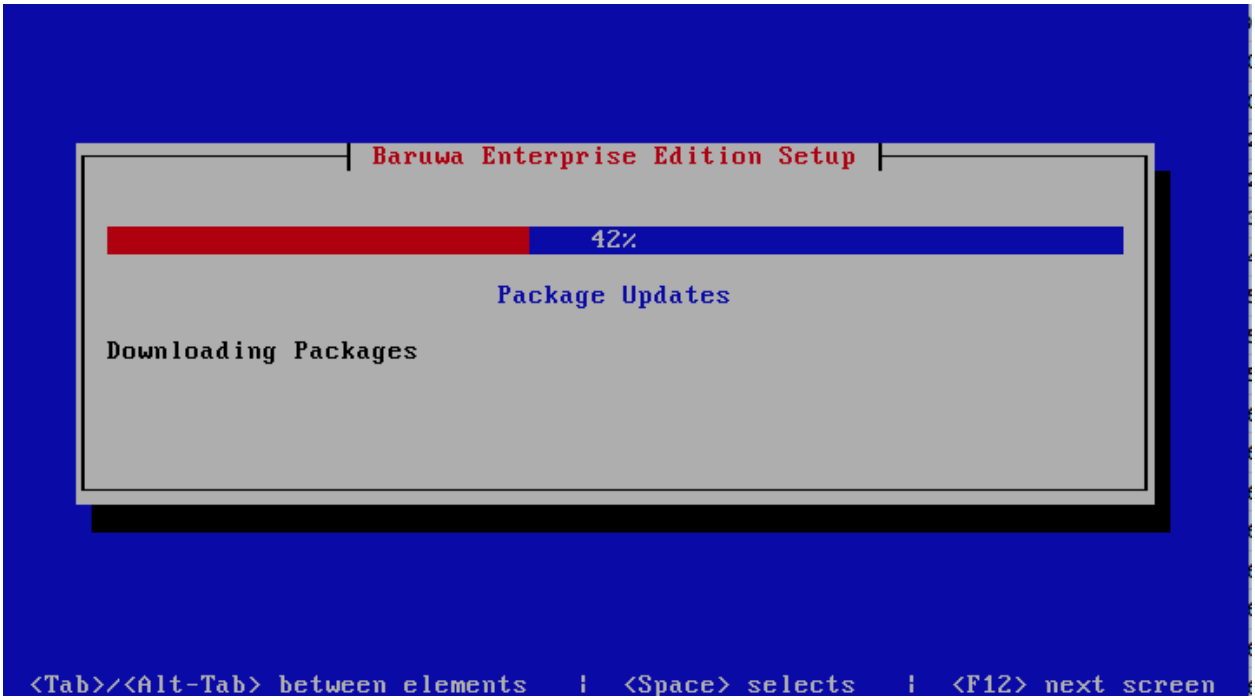


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

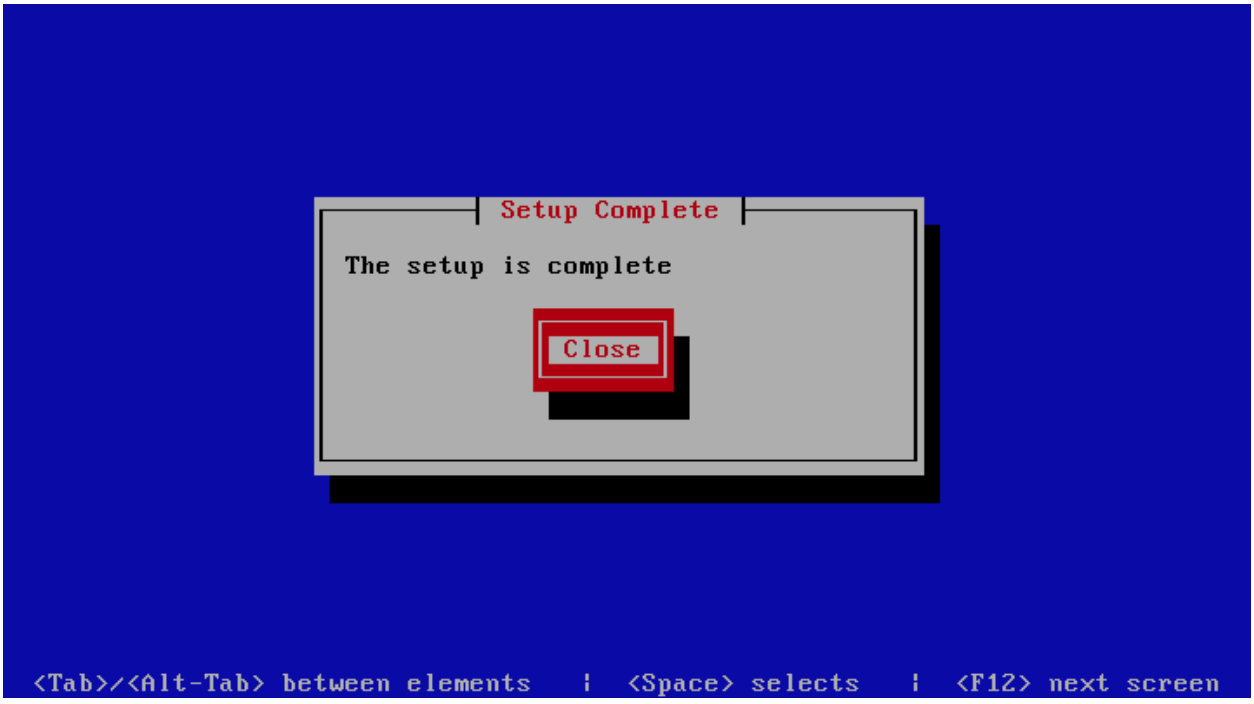
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

> **Warning:** If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.3 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

8.3.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

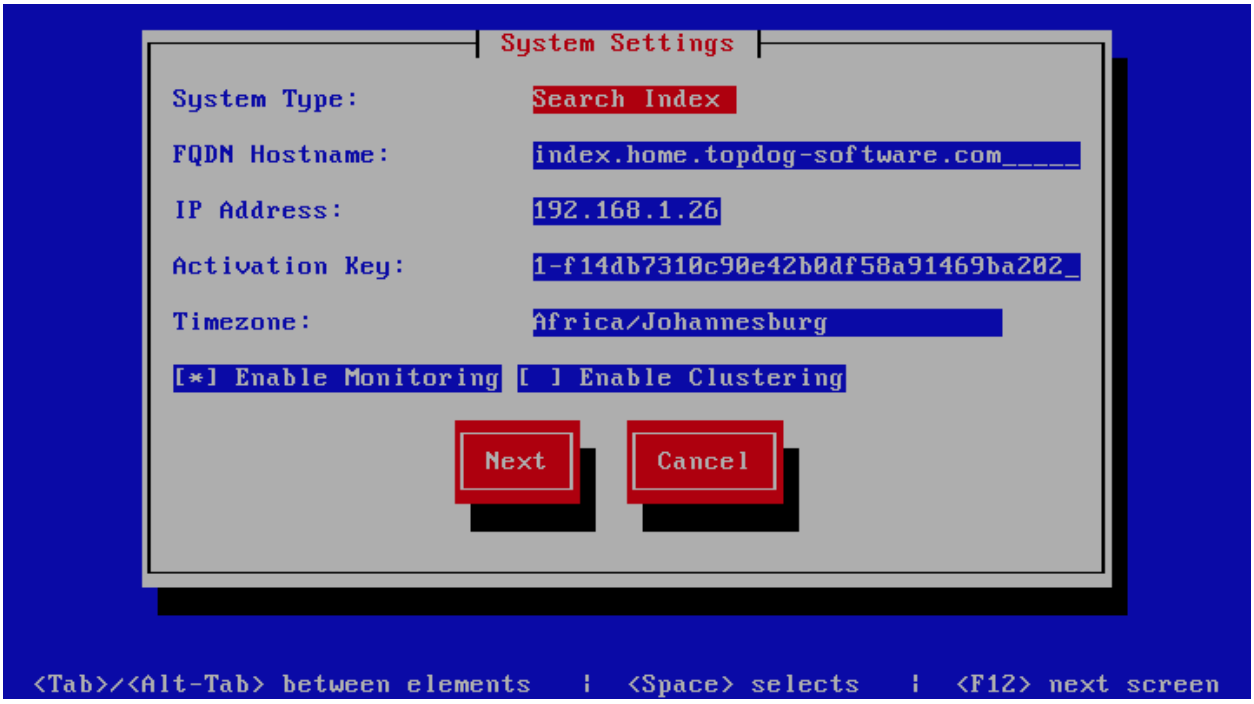
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

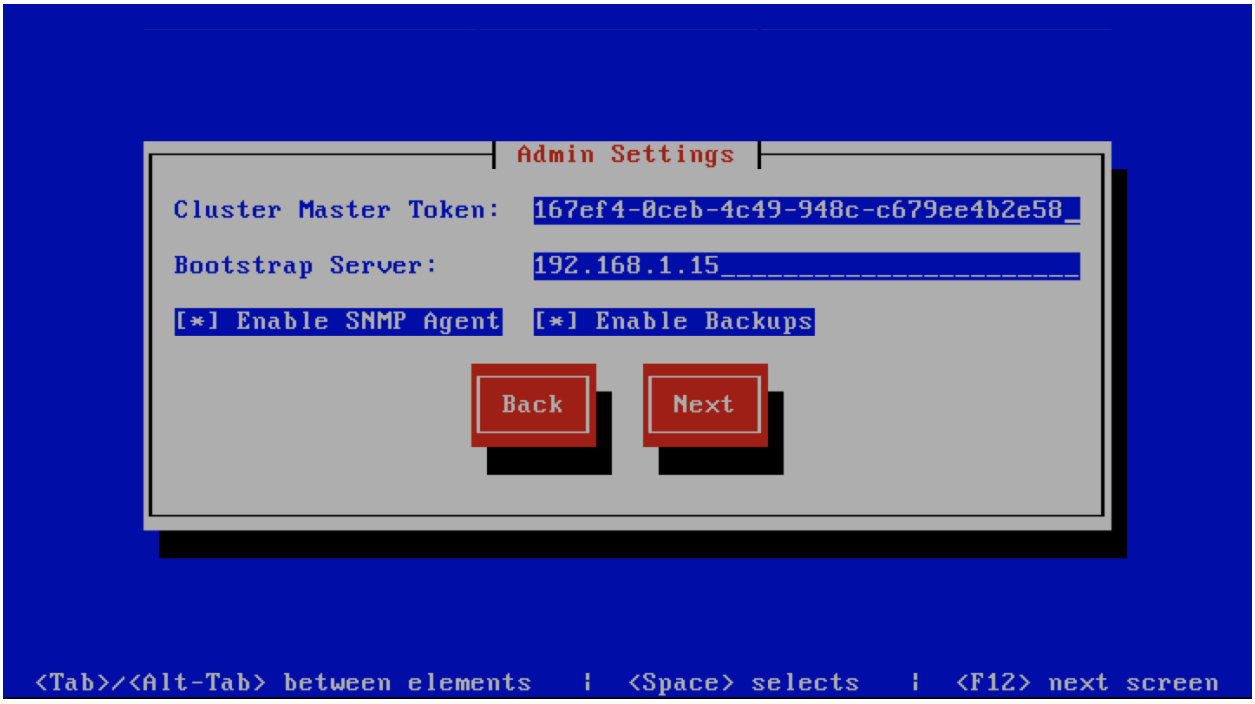
Option	Description
System Type	Set this to Search Index
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check/Uncheck this to enable or disable backend segment *Clustering*
Enable Monitoring	Check this to enable the *Monitoring*



Admin Settings

This screen sets backend segment cluster settings. The description of the options is as follows:

Option	Description
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the *Bootstrap server*.
Bootstrap server	The IP address of the *Bootstrap server*
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]

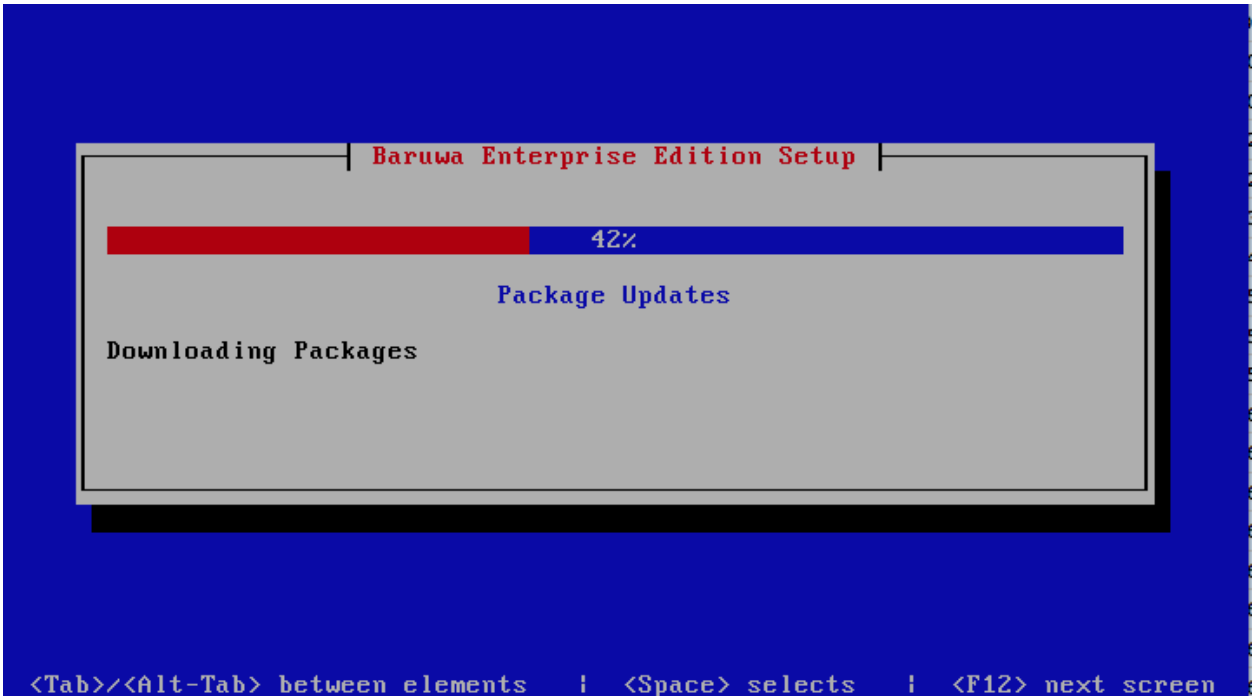


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

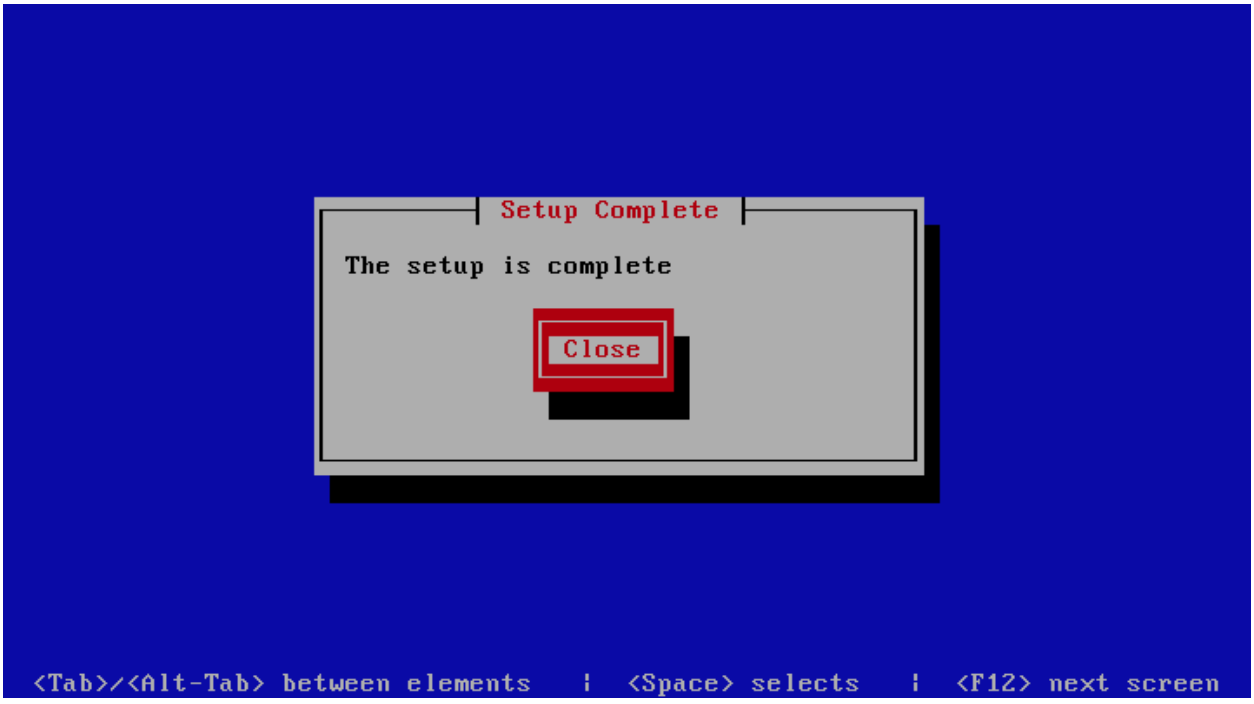
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

> **Warning:** If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.4 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

8.4.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

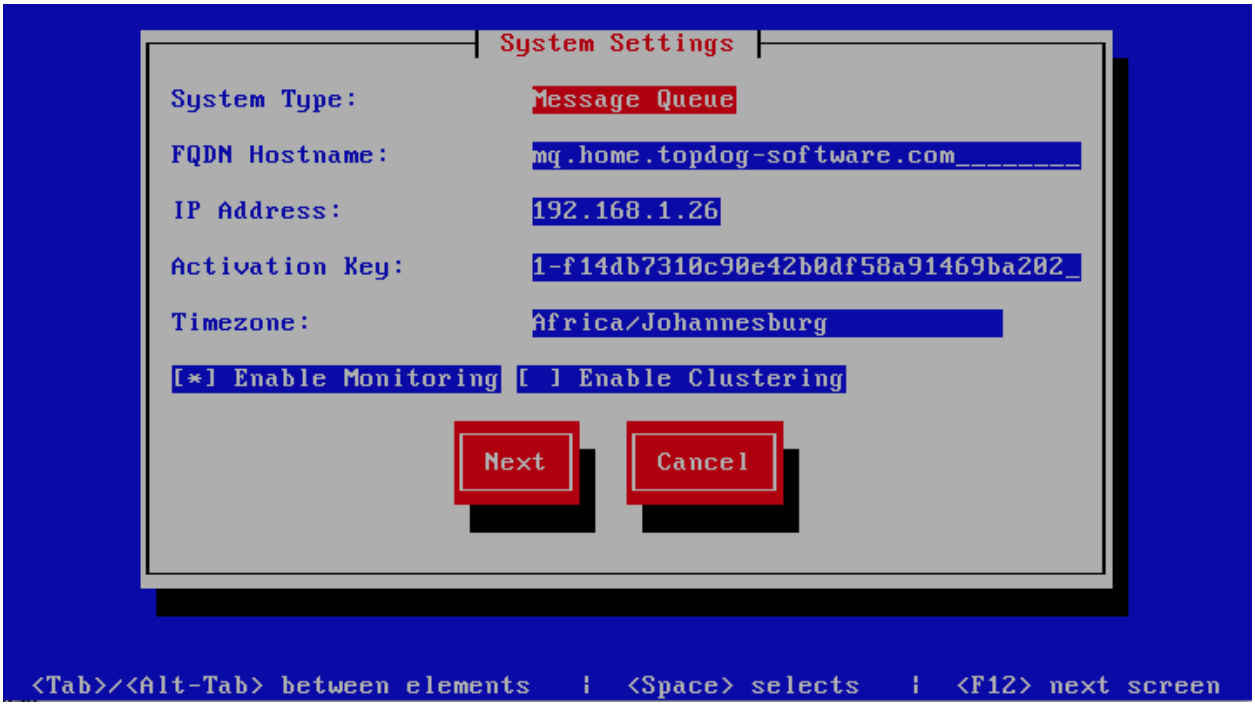
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

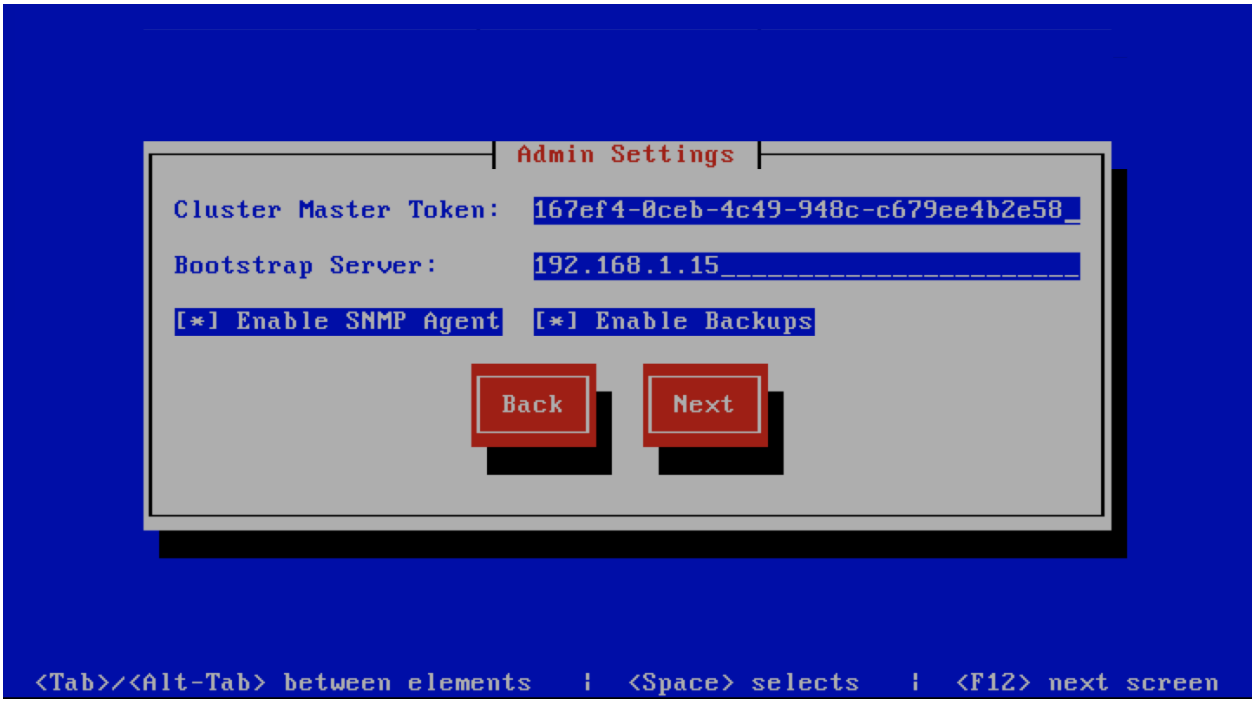
Option	Description
System Type	Set this to Message Queue
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check/Uncheck this to enable or disable backend segment *Clustering*
Enable Monitoring	Check this to enable the *Monitoring*



Admin Settings

This screen sets backend segment cluster settings. The description of the options is as follows:

Option	Description
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the *Bootstrap server*.
Bootstrap server	The IP address of the *Bootstrap server*
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]

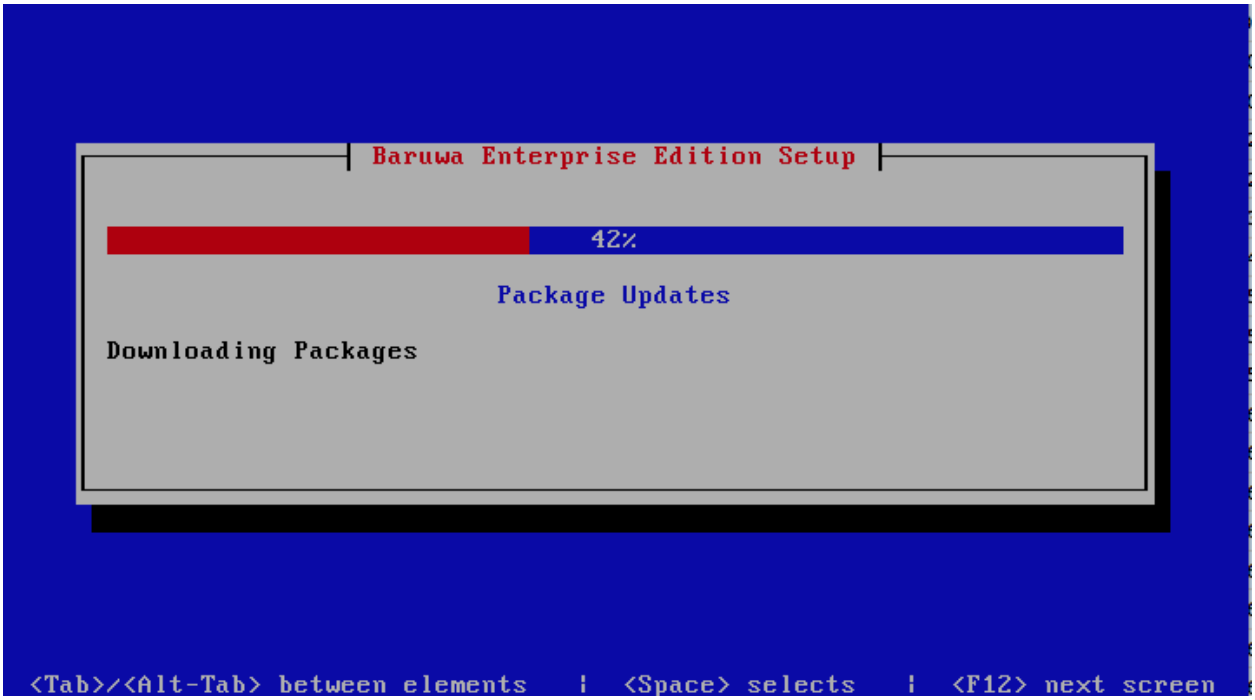


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

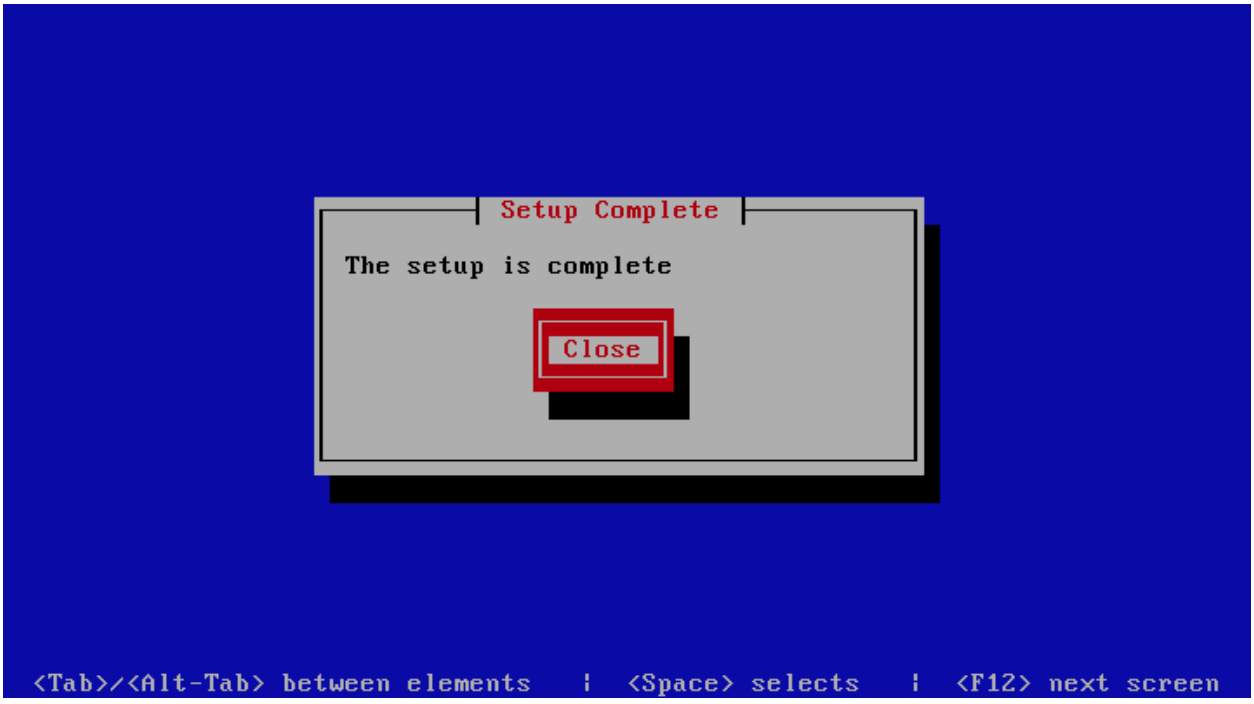
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

> **Warning:** If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.5 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Distributed Backend Hybrid Frontend* topologies.

8.5.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

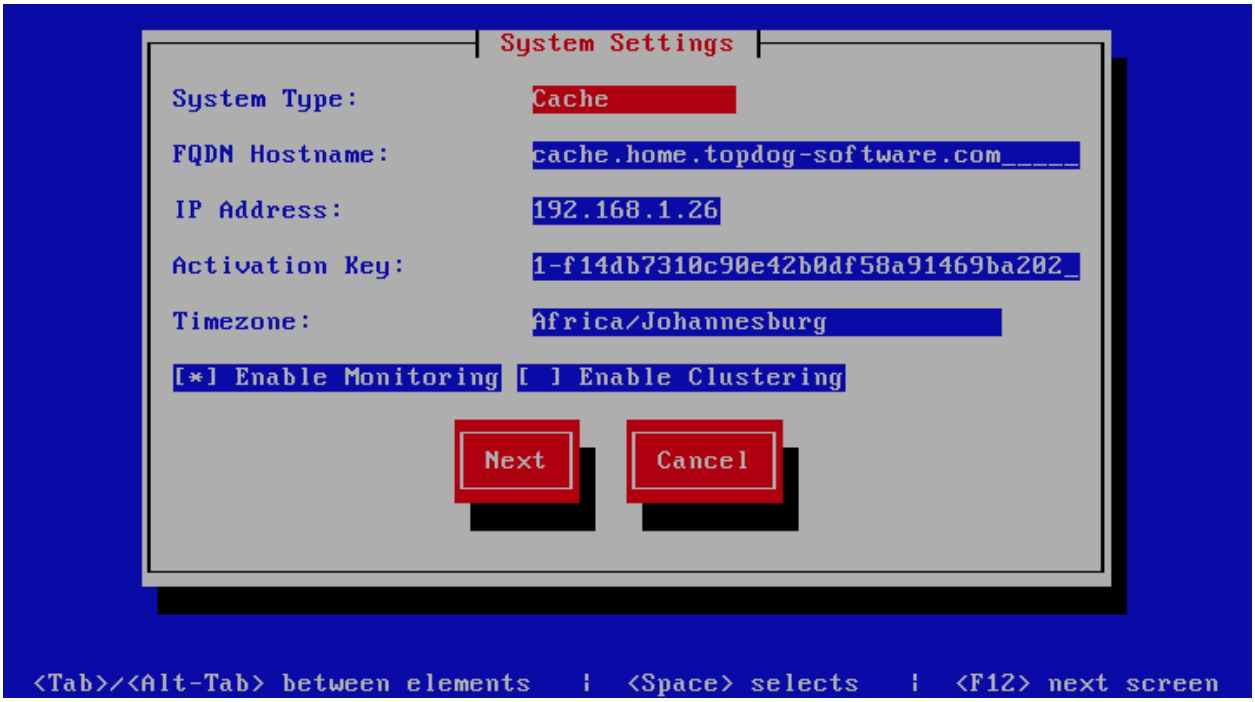
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

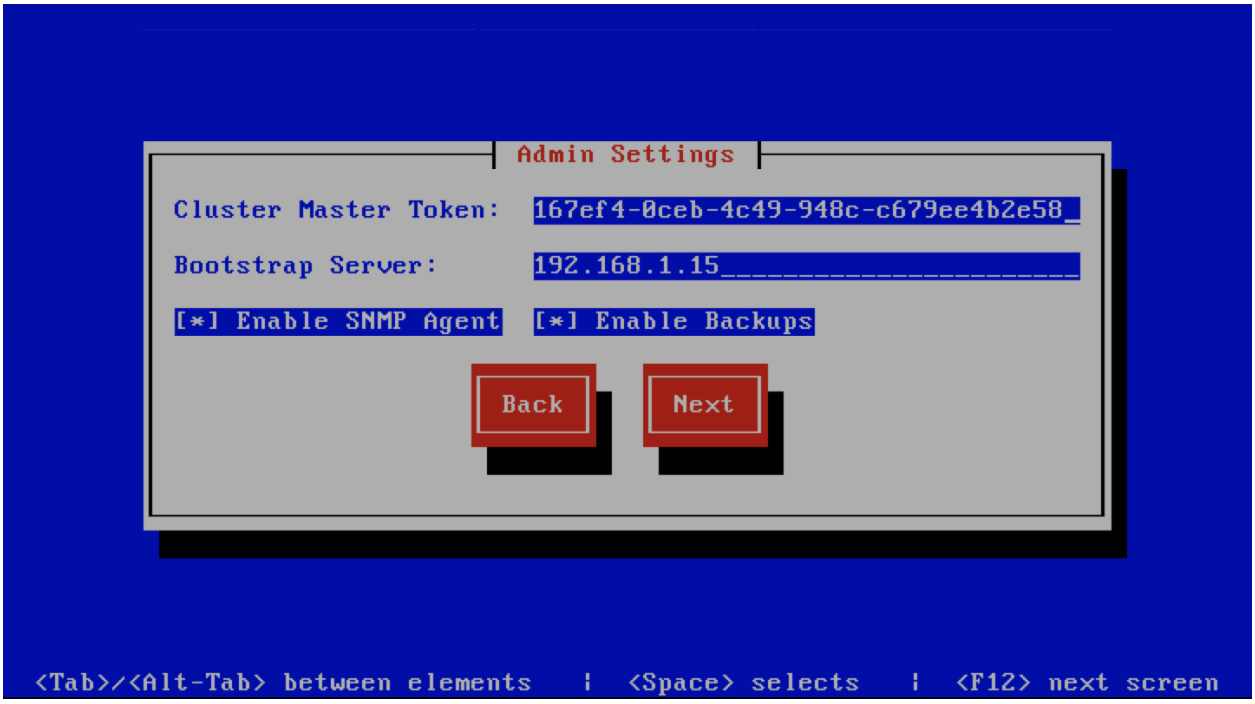
Option	Description
System Type	Set this to Cache
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.
Enable clustering	Check/Uncheck this to enable or disable backend segment *Clustering*
Enable Monitoring	Check this to enable the *Monitoring*



Admin Settings

This screen sets backend segment cluster settings. The description of the options is as follows:

Option	Description
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the *Bootstrap server*.
Bootstrap server	The IP address of the *Bootstrap server*
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]

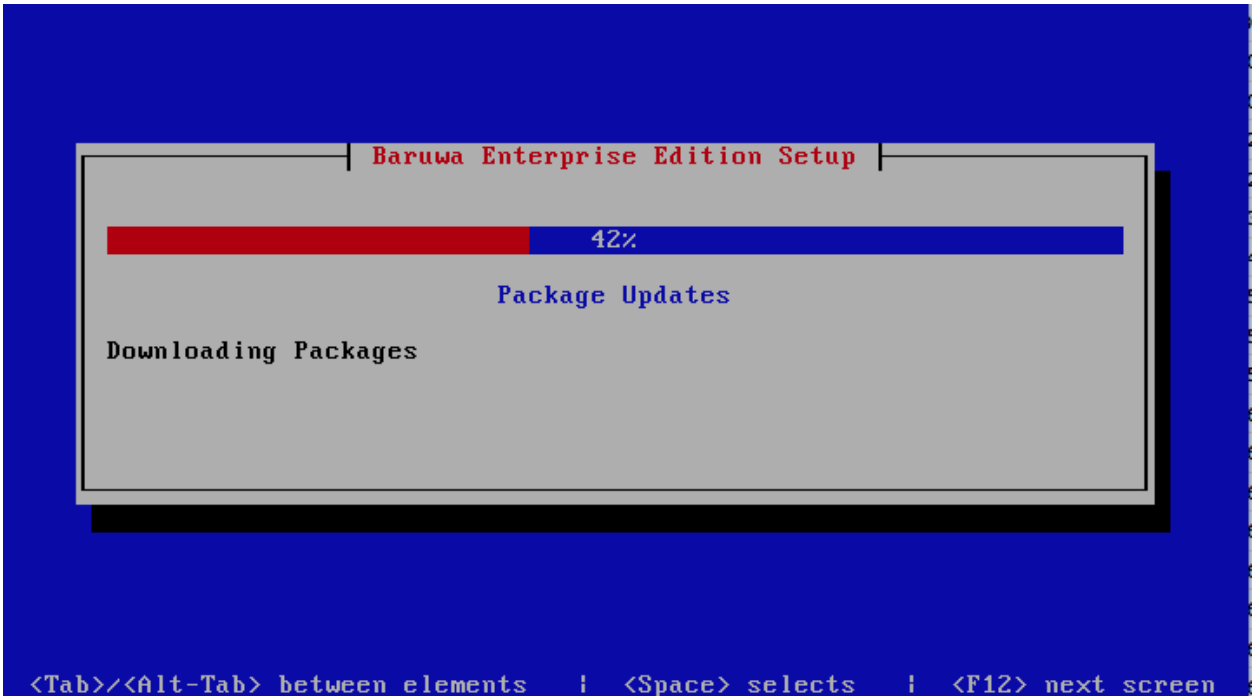


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

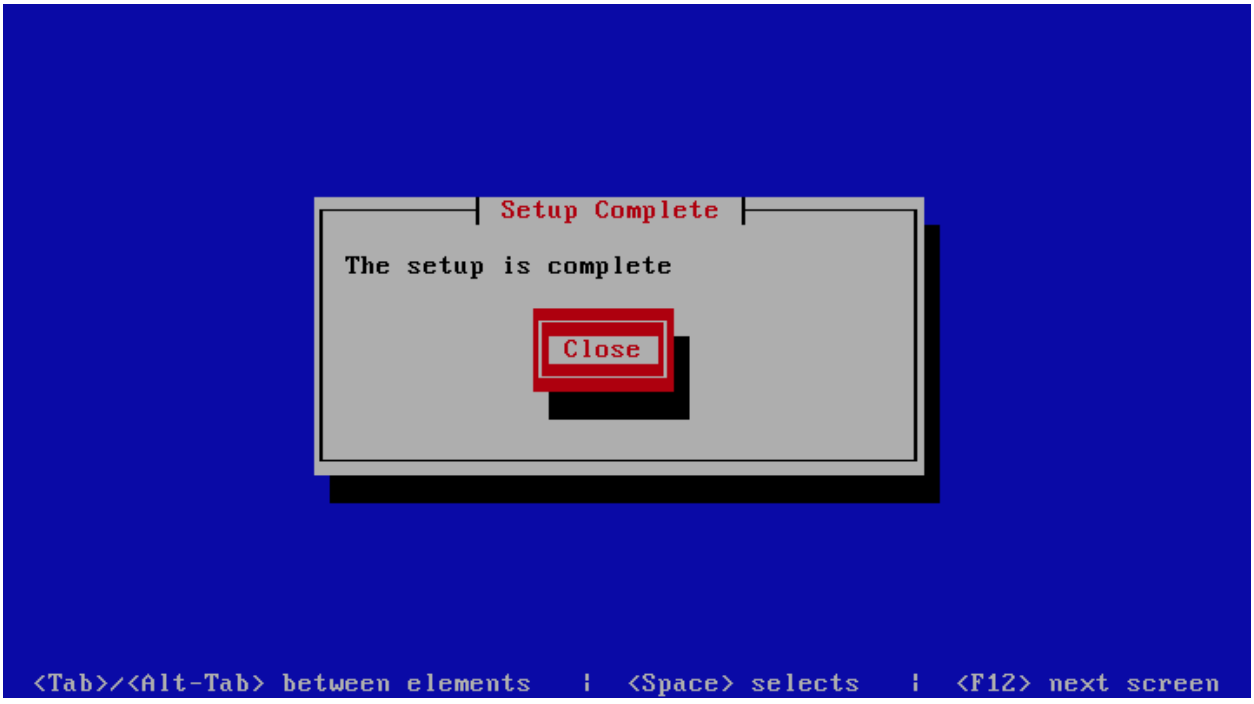
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

> **Warning:** If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.6 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.

This profile is used in the *Distributed Backend Hybrid Frontend* and *Single Backend Hybrid Frontend* topologies.

8.6.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

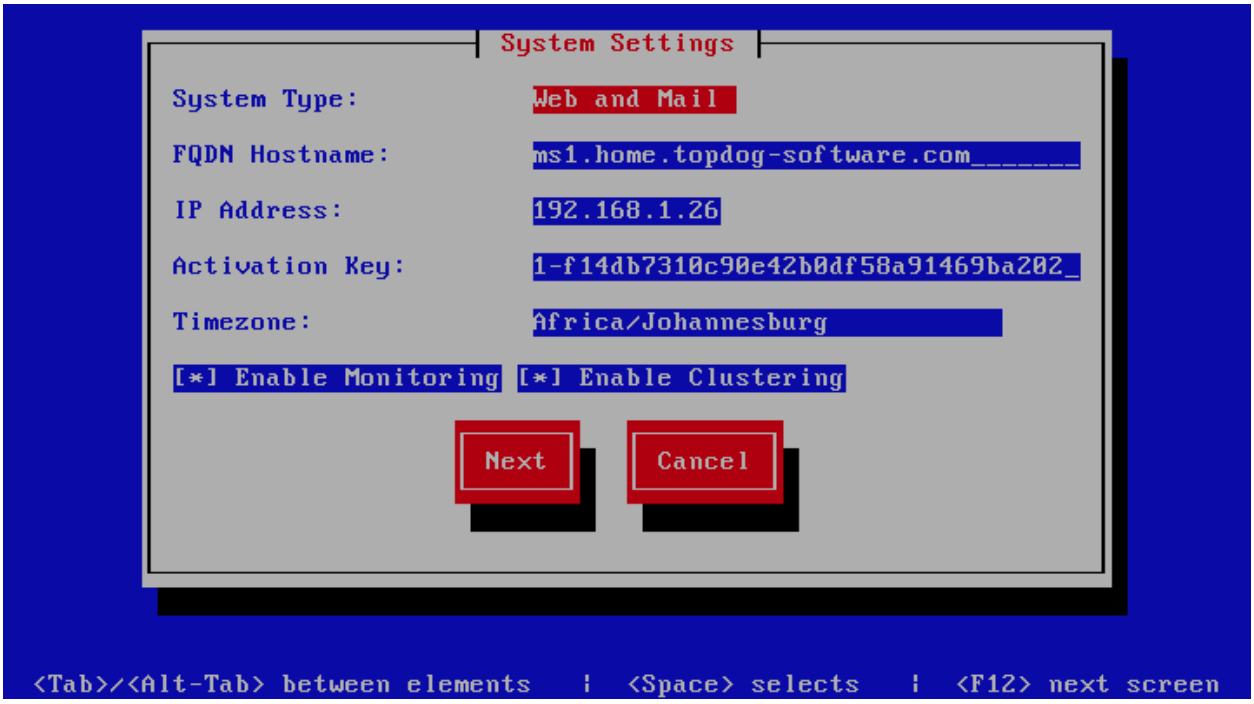
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

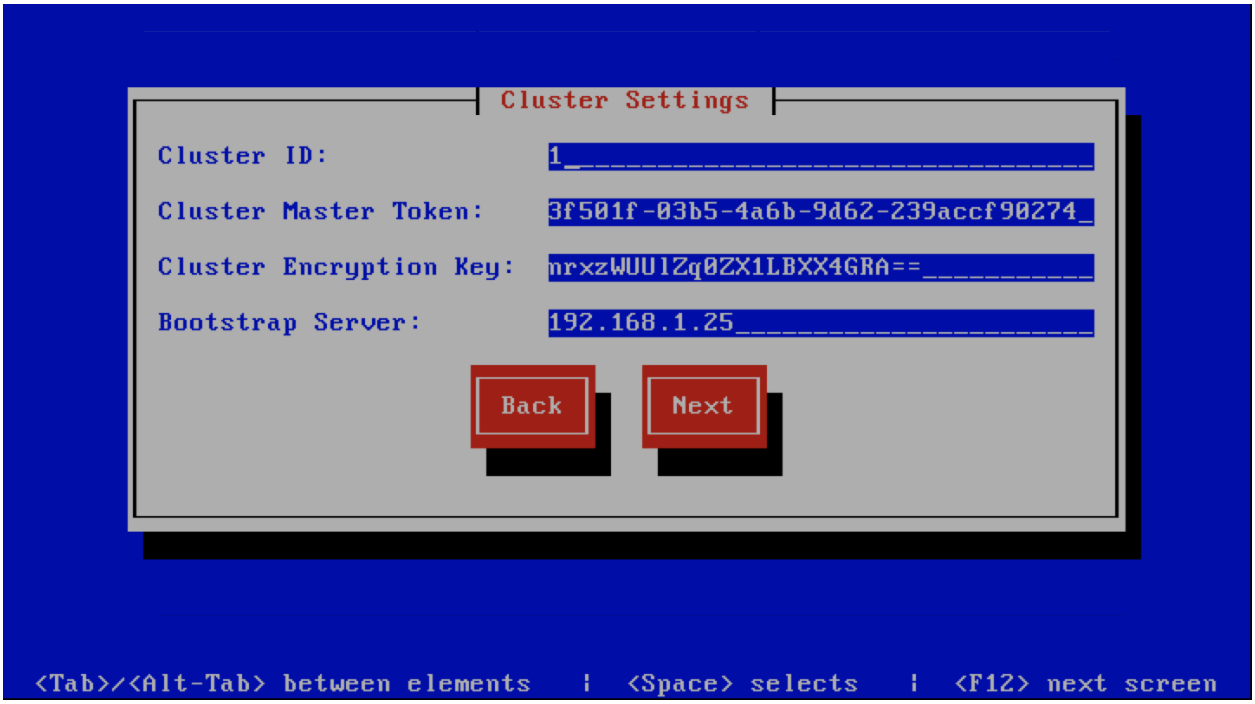
Option	Description
System Type	Set this to Web and Mail
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system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



Cluster Settings

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

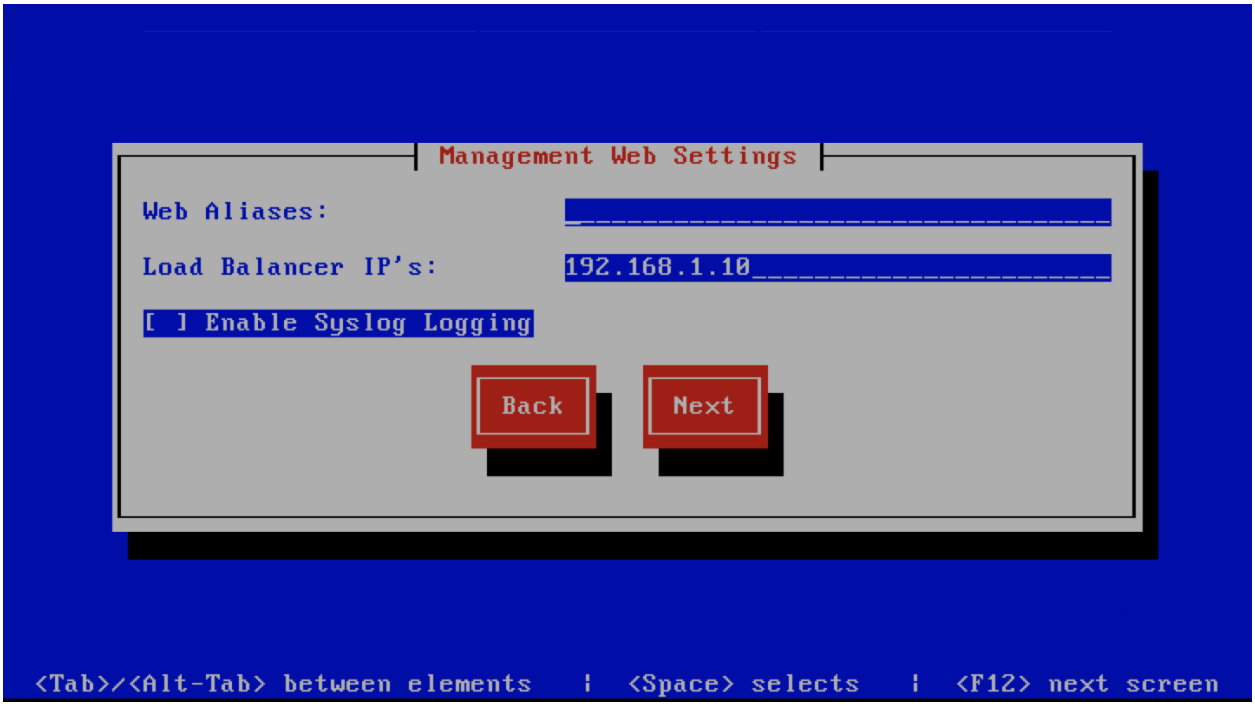
Option	Description
Cluster ID	An integer number unique to each node
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the bootstrap server.
Cluster Encryption Key	The cluster's encryption key, you can get it by running `baruwa-setup -e cluster_secret` on the bootstrap server
Bootstrap server	The IP address of the bootstrap server



Management Web Settings

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

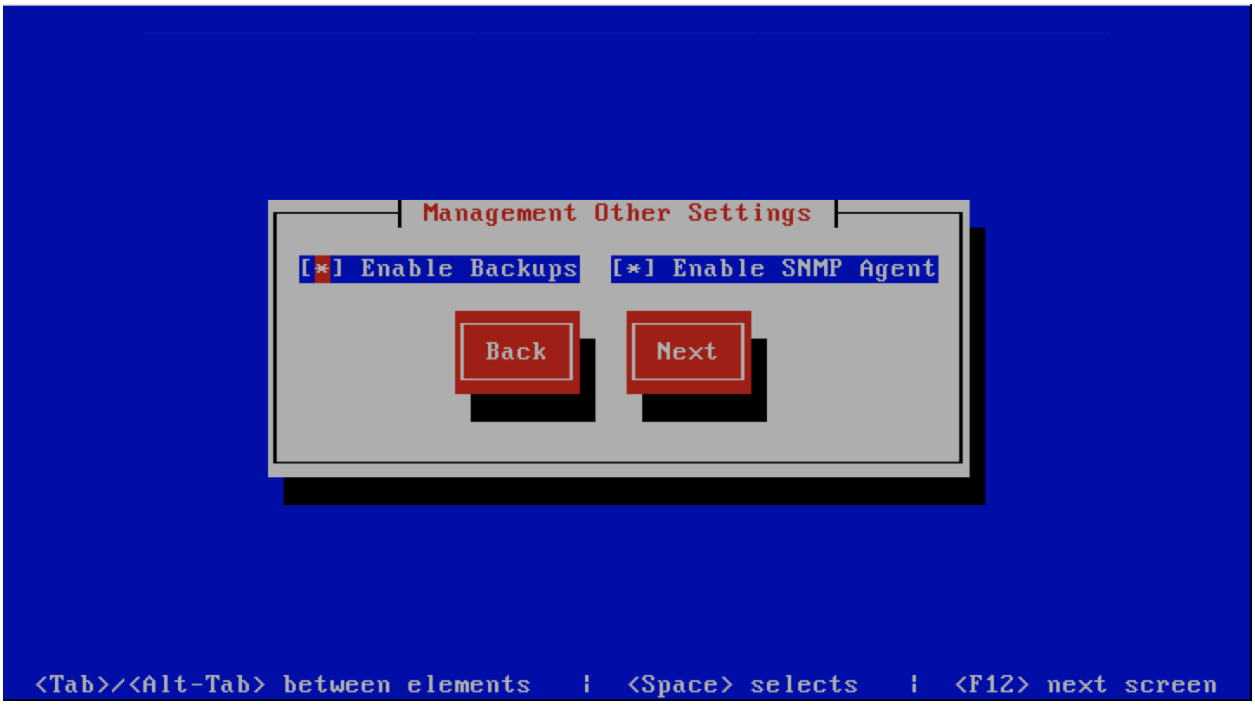
Option	Description
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable Syslog Logging	Turns on Web logging to syslog



Management Other Settings

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

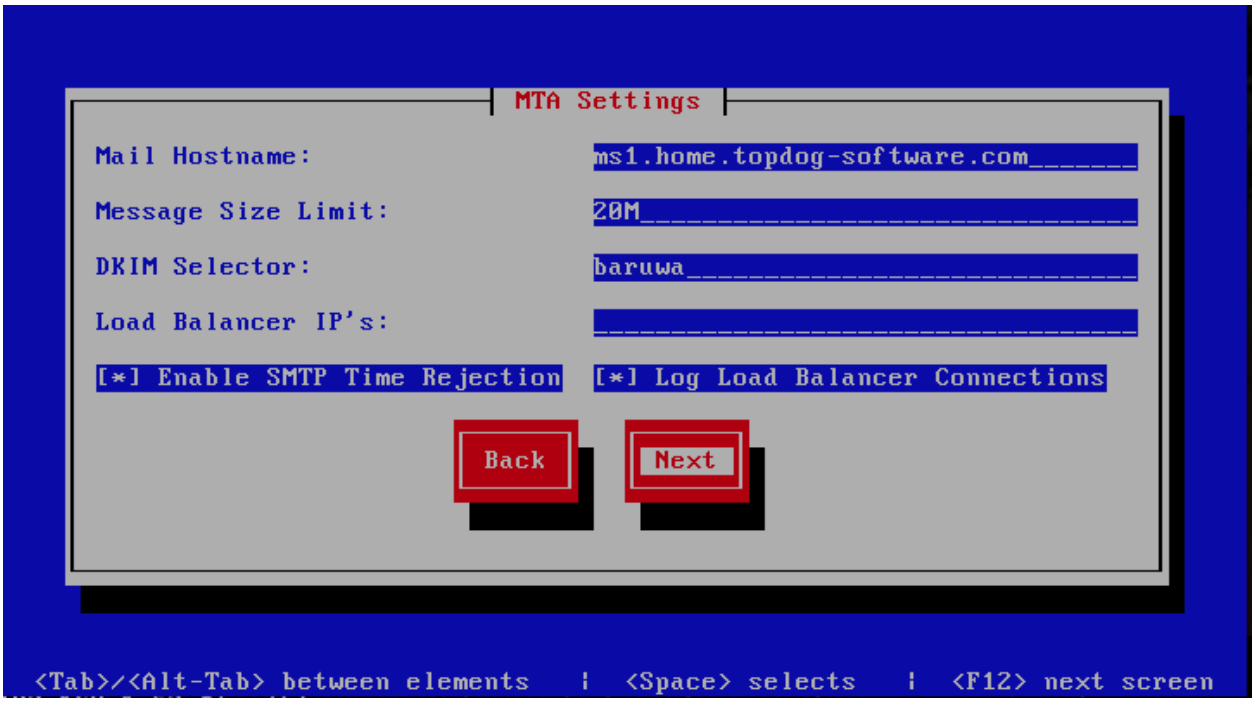
Option	Description
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.



MTA Settings

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

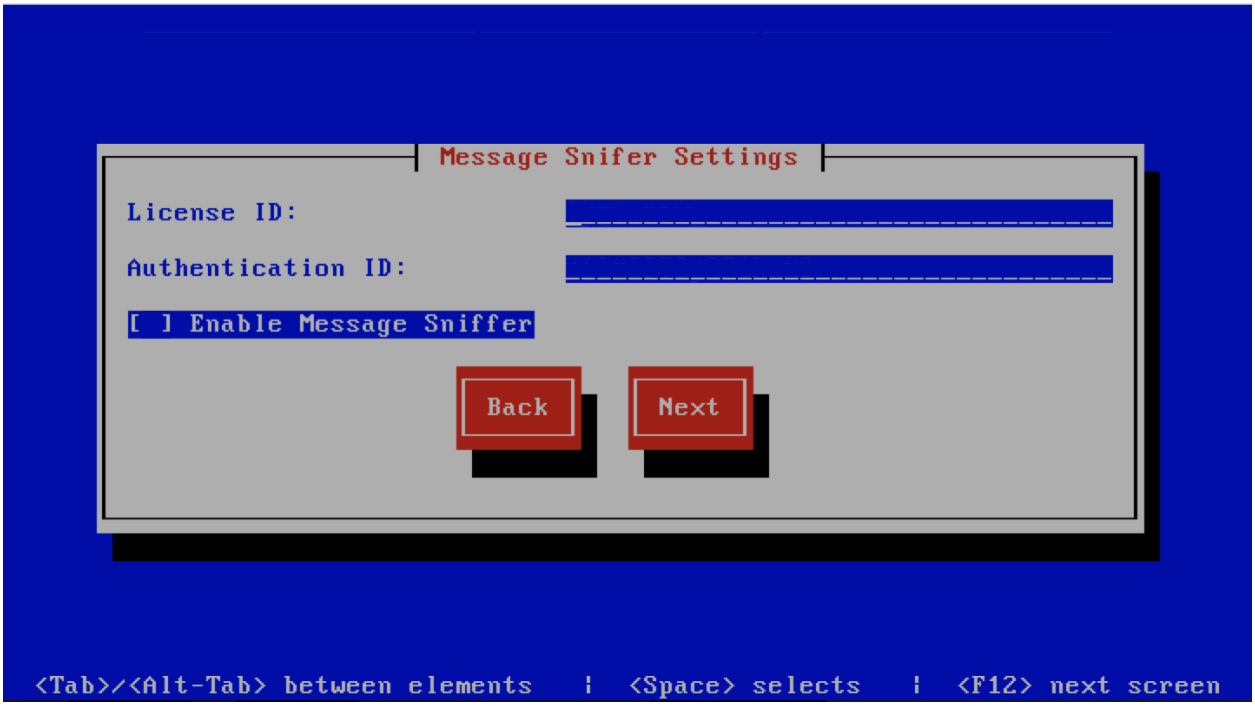
Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable SMTP Time Rejection	Enable SMTP rejection of messages which either match Anti-Virus signatures or exhibit definite SPAM like charactaristics at SMTP Time without queueing or logging the message.
Log Load Balancer Connections	Log Load Balancer connections to the MTA log



Message Sniffer Settings

This 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 ran 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 request a CertBot certificate or generate a non recognised Builtin 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.

Certbot certificate

The issuance of a CertBot certificate is based on an automated check that verifies that the hostnames specified are under your control. Baruwa performs a precheck to verify that the hostnames resolve to a public IP address on the host

itself. If this check fails then the Certbot certificate will not be requested. This check will fail if your public IP address is on another device and you are forwarding connections to a private address on your Baruwa system. To work around that you need to create a check file:

```
touch /etc/baruwa/acme.enable
```

For the validation process to succeed, Certbot systems need to be able to connect to port 80 on your system, ensure that that is allowed on your network devices.

Certbot certificates are only issued to systems of the *Standalone System*, *Web and Mail System* and *Web Interface System* profiles.

Certbot certificates are issued only to the web hostname, web aliases and the mail hostname. Cluster members names are not included in the certificate.

Support for CertBot certificates was added in BaruwaOS 6.8, refer to the *ACME TLS Certificates* section of the release notes for more information.

Note: It is currently not possible to issue or syncronize certificates in a cluster that uses the same hostname. If you are operating a cluster you should either purchase a Commercial CA issued certificate or use Builtin certificates.

Commercial CA issued certificate

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

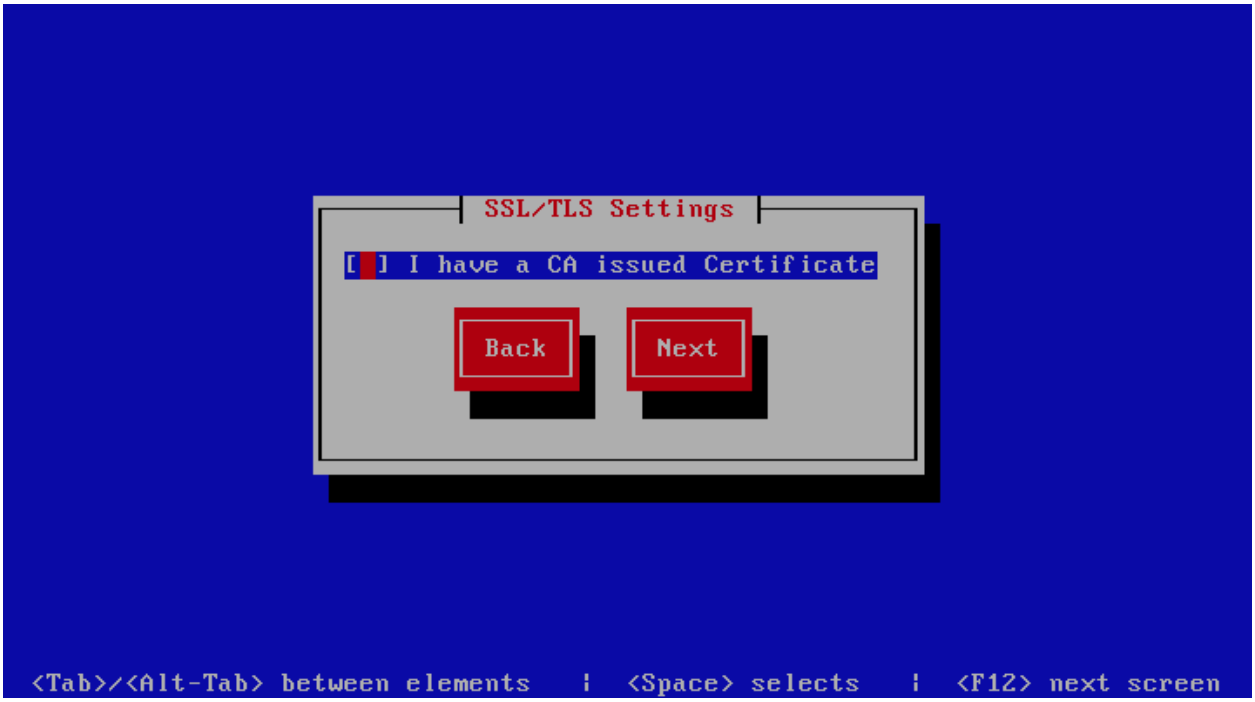
If your SSL certificate is signed using an intermediate certificate, you need to append the intermediate certificate to the file `/etc/pki/baruwa/certs/baruwa.pem`. The server certificate must appear before the intermediate certificate in the combined file.

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.

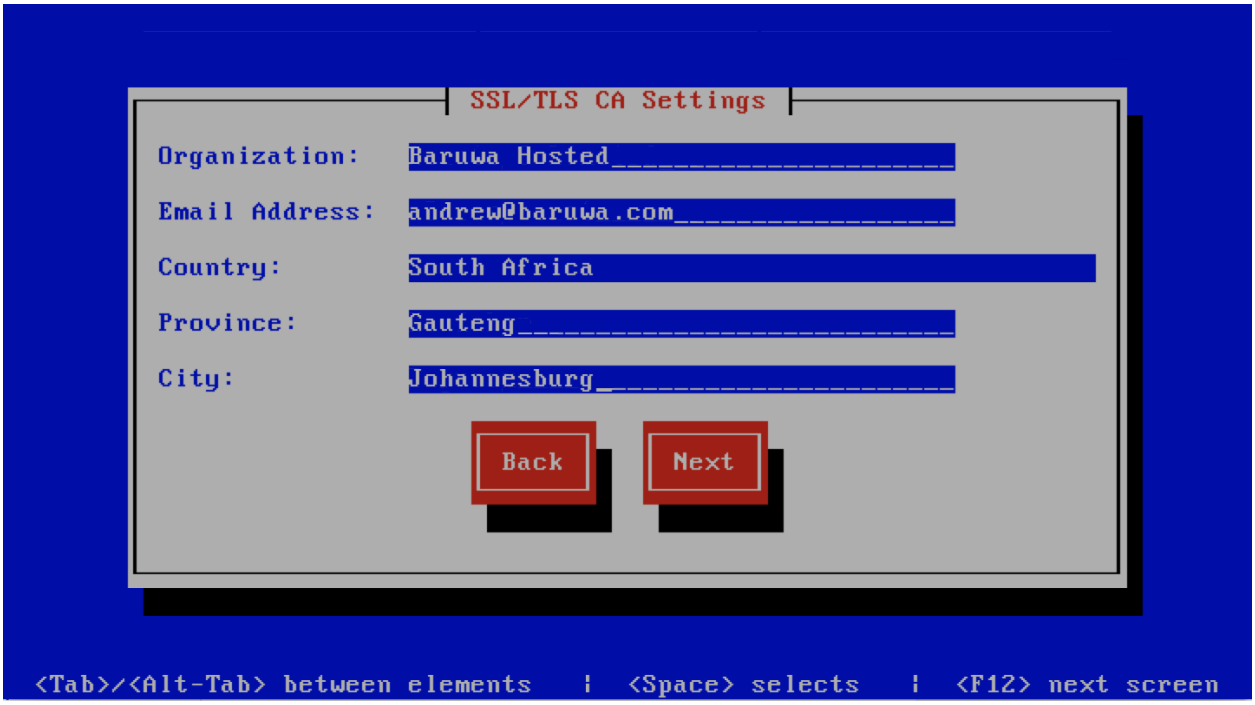
Builtin certificate

The certificate that `baruwa-setup` generates contains all the relevant system names. The downside to the builtin certificates is that they are signed by the BaruwaCA meaning they will not be recognized by browsers and will generate unknown CA errors in browsers.



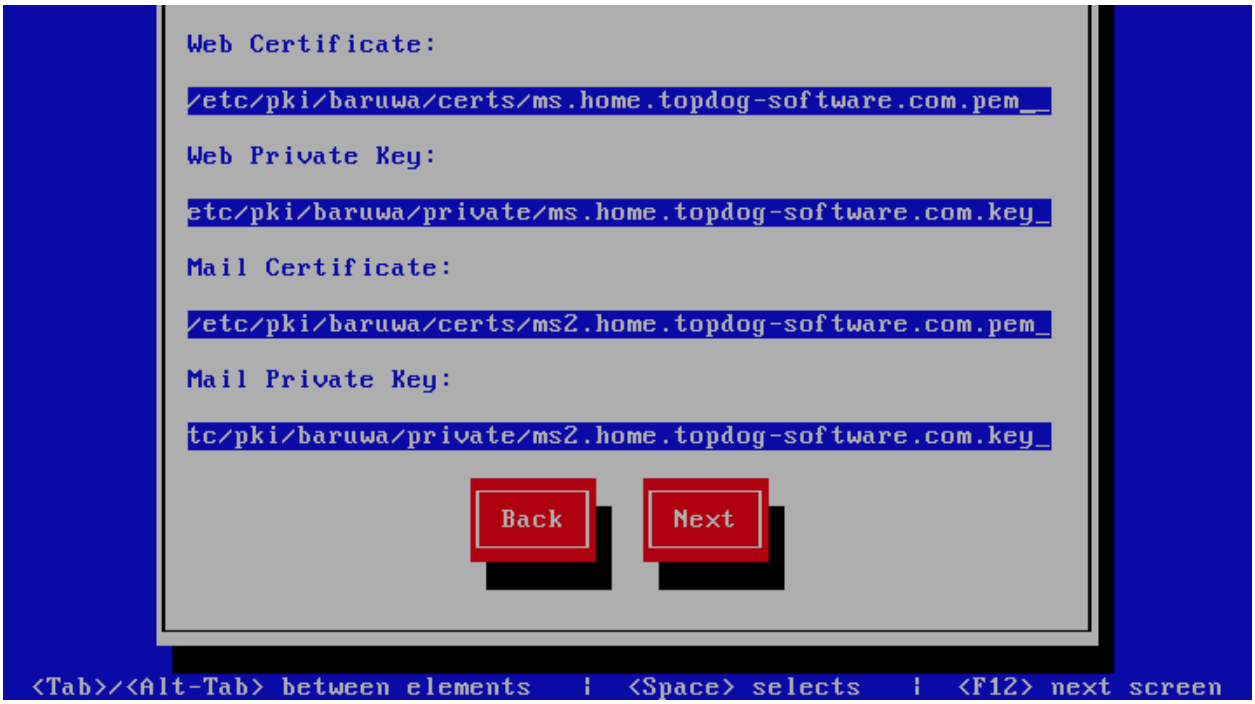
If you left `I have a CA issued Certificate` unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

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

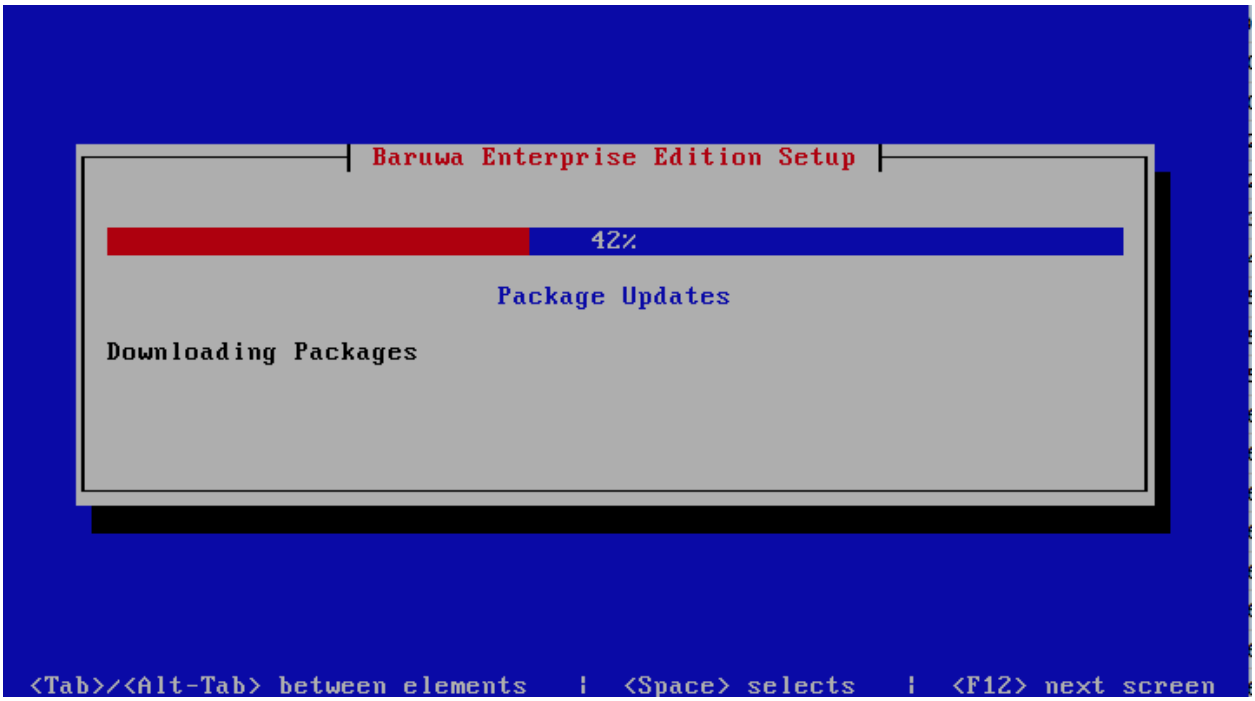


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

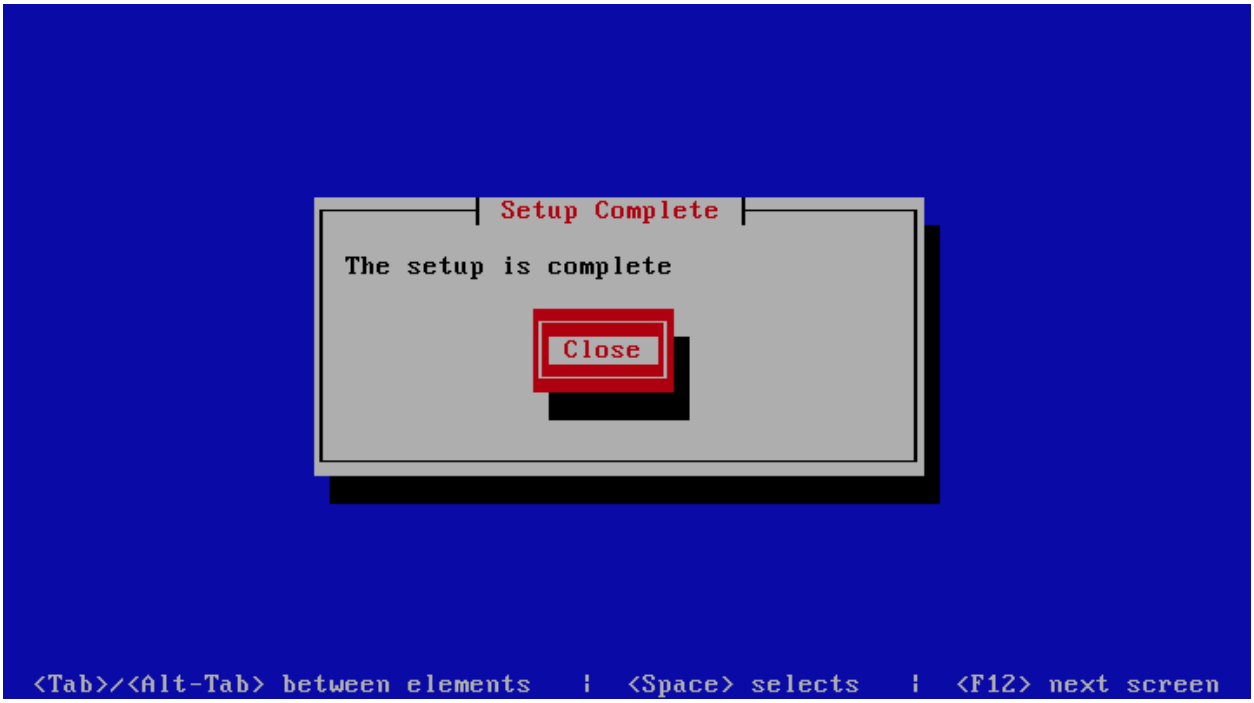
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

Warning: If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.6.2 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a Scanning Node*, *Adding 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 to the Organization
- Add a delivery server for the Domain
- Add a Domain Administrator Account for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add any user accounts to the Domain if not using external authentication

Review the *DNS*, *Administrators guide*, *Email Protection Best Practices* and *Advanced configuration* sections for other configuration and setup options available.

8.7 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Single Backend Distributed Frontend* topologies.

8.7.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

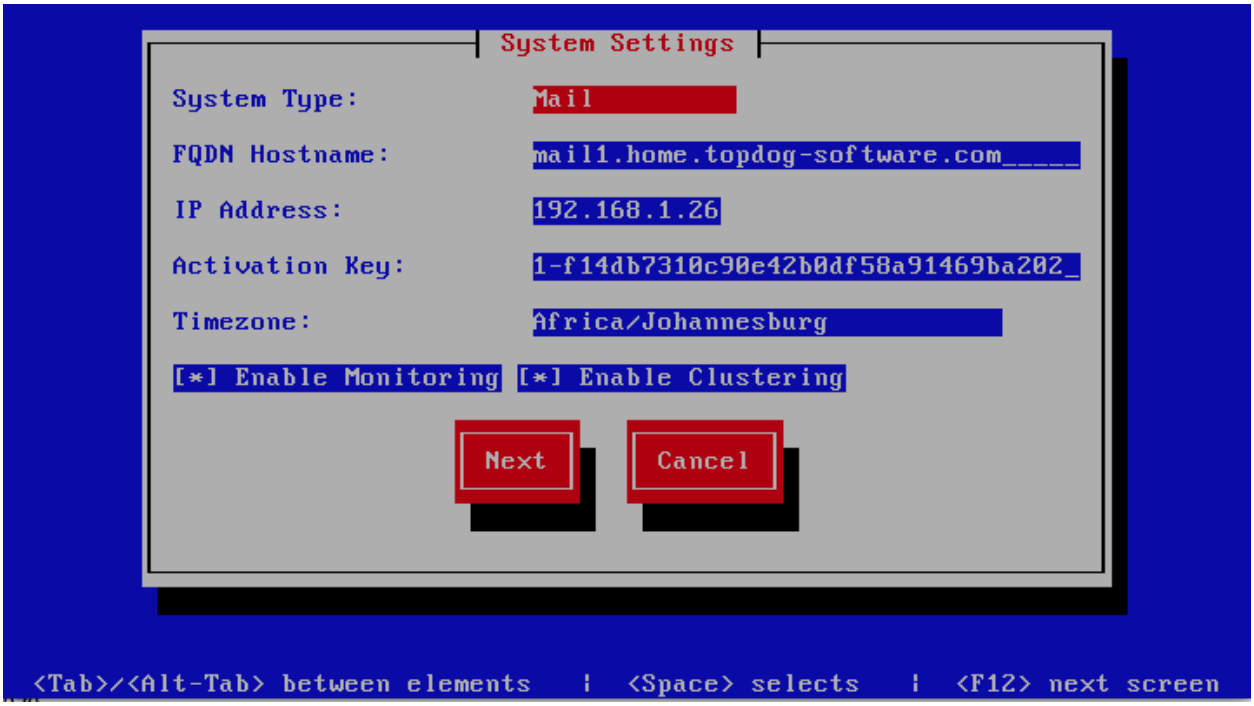
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

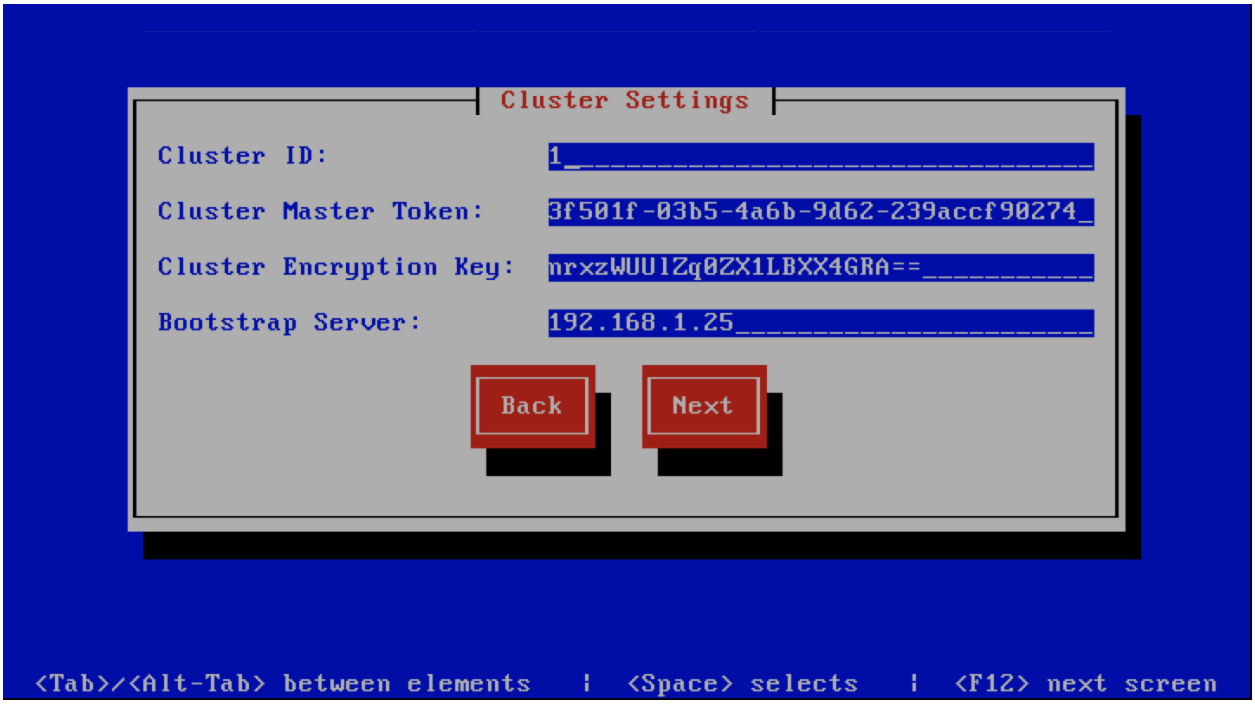
Option	Description
System Type	Set this to Mail
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system configuration.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



Cluster Settings

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

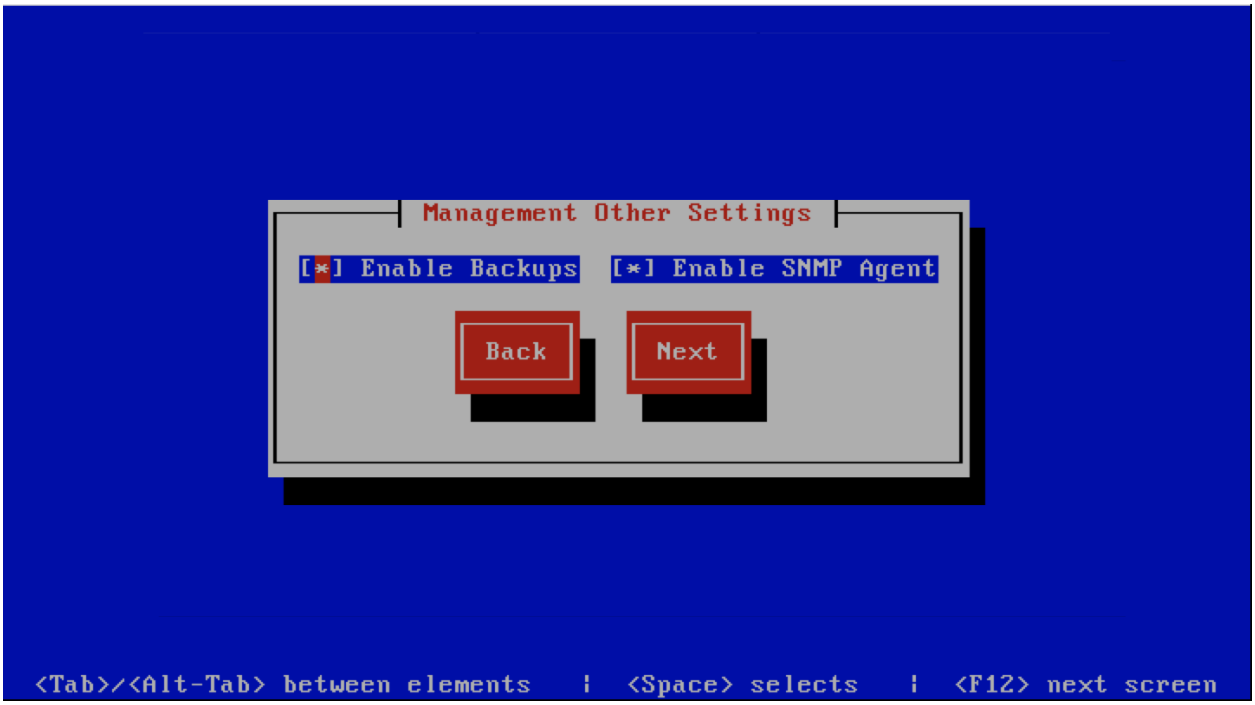
Option	Description
Cluster ID	An integer number unique to each node
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the bootstrap server.
Cluster Encryption Key	The cluster's encryption key, you can get it by running `baruwa-setup -e cluster_secret` on the bootstrap server
Bootstrap server	The IP address of the bootstrap server



Management Other Settings

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

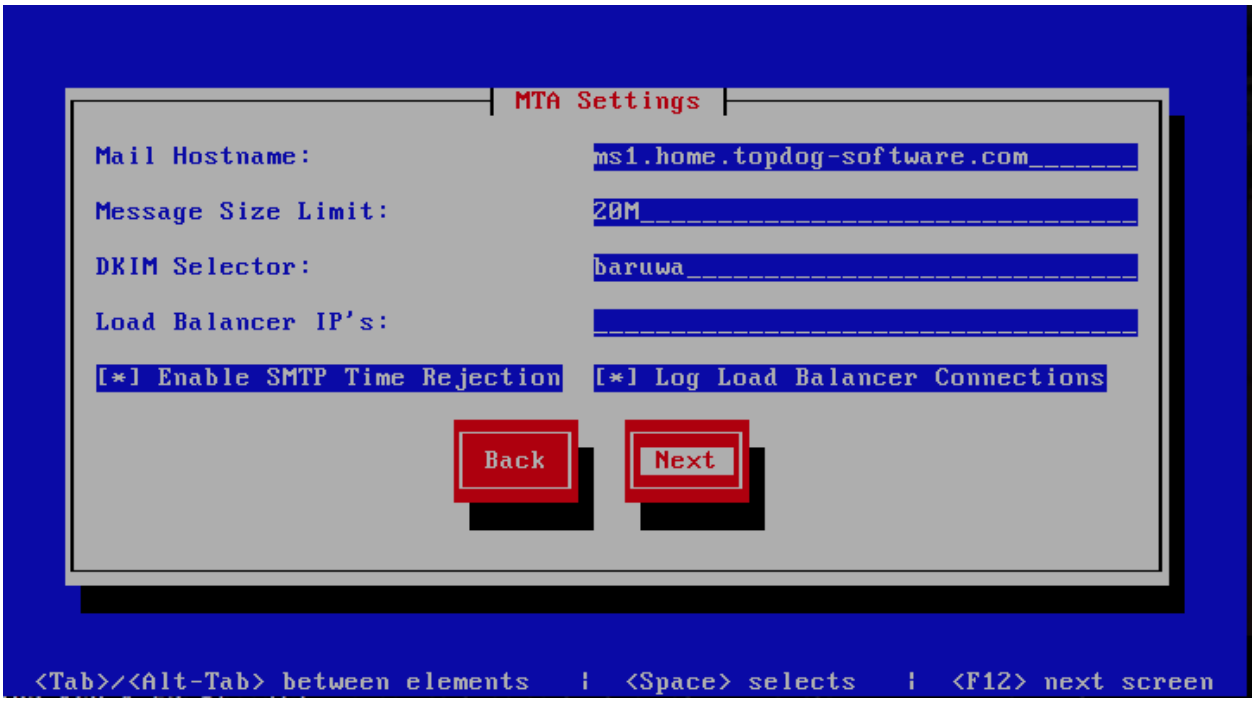
Option	Description
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.



MTA Settings

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

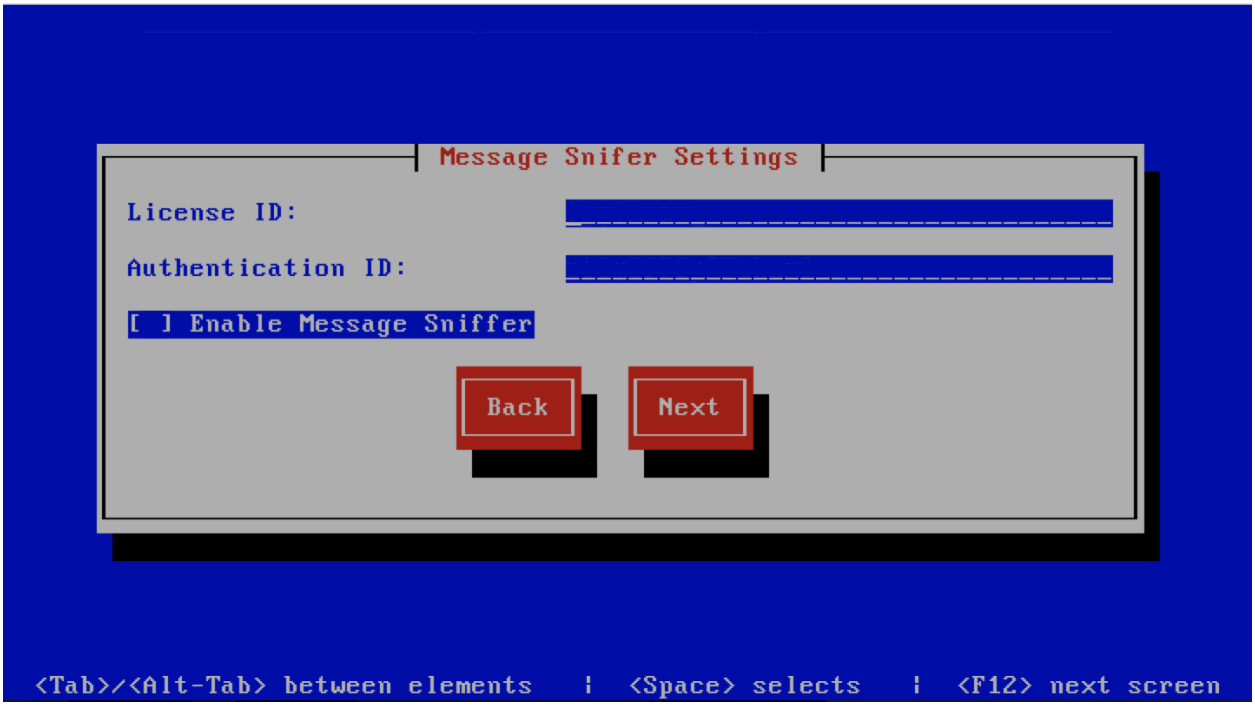
Option	Description
Mail Hostname	The mail server hostname
Message Size Limit	The max message size to accept
DKIM Selector	Sets the DKIM selector name, used to configure DKIM signing.
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable SMTP Time Rejection	Enable SMTP rejection of messages which either match Anti-Virus signatures or exhibit definite SPAM like charactaristics at SMTP Time without queueing or logging the message.
Log Load Balancer Connections	Log Load Balancer connections to the MTA log



Message Sniffer Settings

This 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 ran 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 request a CertBot certificate or generate a non recognised Builtin 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.

Certbot certificate

The issuance of a CertBot certificate is based on an automated check that verifies that the hostnames specified are under your control. Baruwa performs a precheck to verify that the hostnames resolve to a public IP address on the host

itself. If this check fails then the Certbot certificate will not be requested. This check will fail if your public IP address is on another device and you are forwarding connections to a private address on your Baruwa system. To work around that you need to create a check file:

```
touch /etc/baruwa/acme.enable
```

For the validation process to succeed, Certbot systems need to be able to connect to port 80 on your system, ensure that that is allowed on your network devices.

Certbot certificates are only issued to systems of the *Standalone System*, *Web and Mail System* and *Web Interface System* profiles.

Certbot certificates are issued only to the web hostname, web aliases and the mail hostname. Cluster members names are not included in the certificate.

Support for CertBot certificates was added in BaruwaOS 6.8, refer to the *ACME TLS Certificates* section of the release notes for more information.

Note: It is currently not possible to issue or syncronize certificates in a cluster that uses the same hostname. If you are operating a cluster you should either purchase a Commercial CA issued certificate or use Builtin certificates.

Commercial CA issued certificate

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

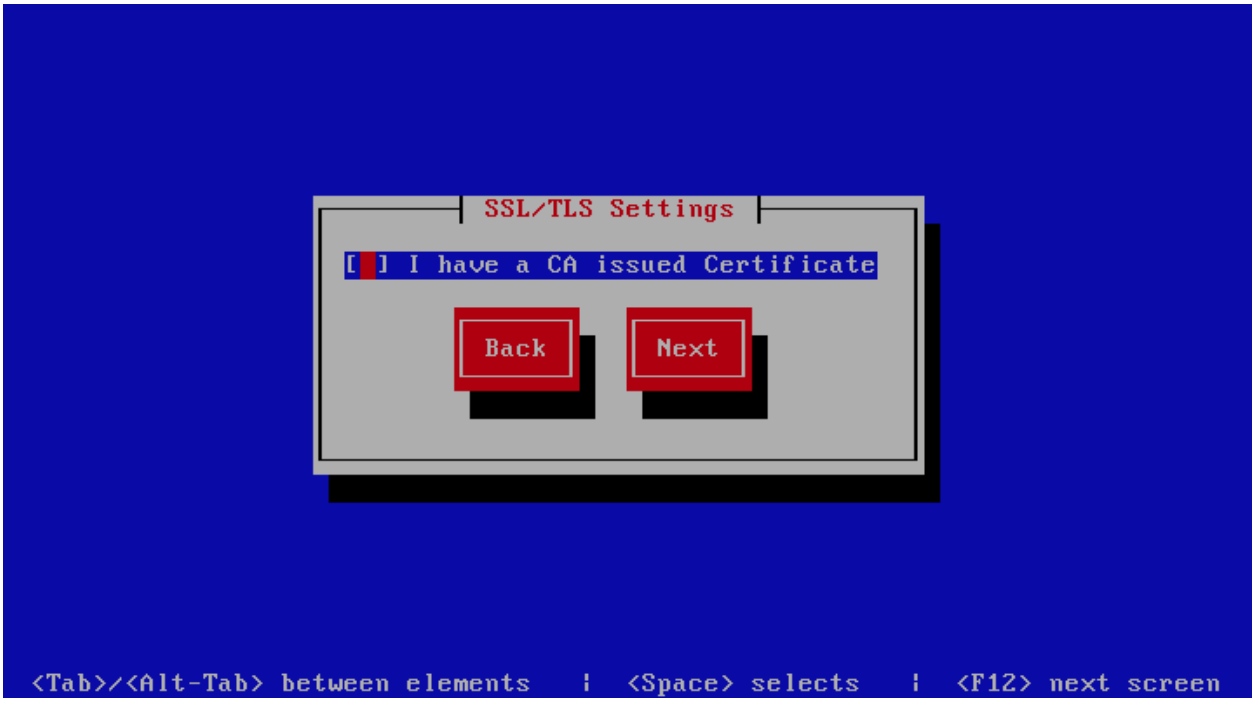
If your SSL certificate is signed using an intermediate certificate, you need to append the intermediate certificate to the file `/etc/pki/baruwa/certs/baruwa.pem`. The server certificate must appear before the intermediate certificate in the combined file.

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.

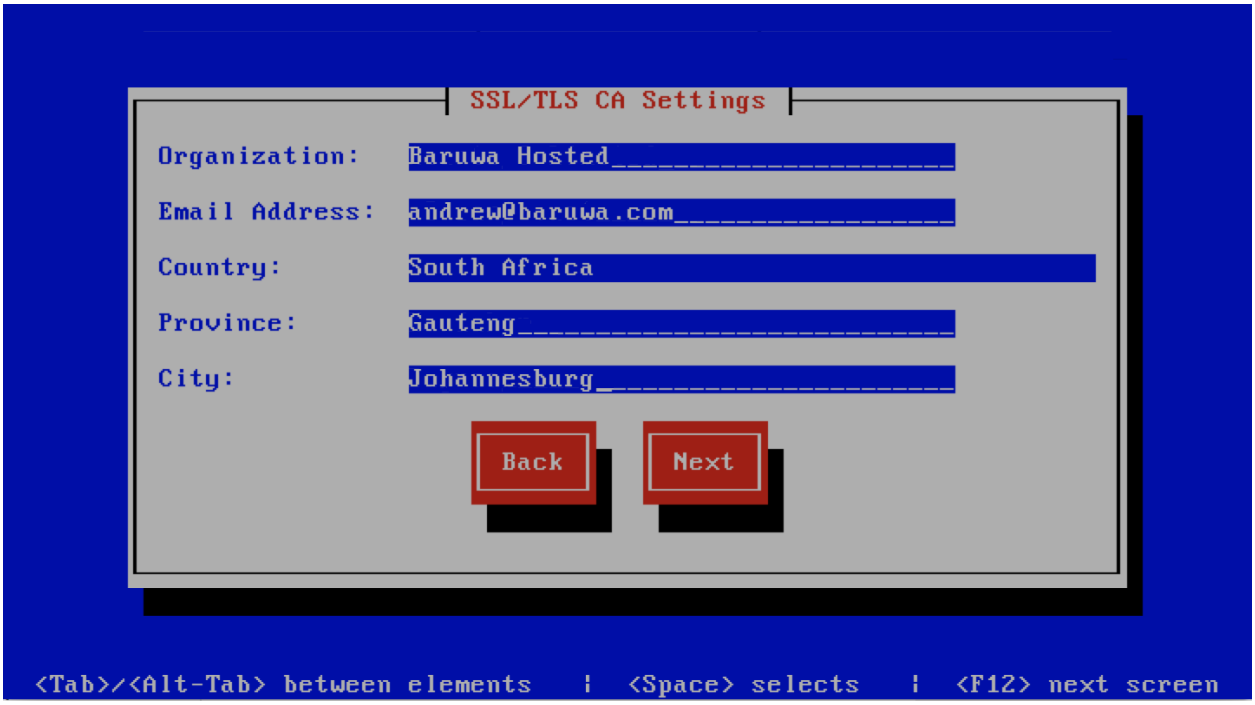
Builtin certificate

The certificate that `baruwa-setup` generates contains all the relevant system names. The downside to the builtin certificates is that they are signed by the BaruwaCA meaning they will not be recognized by browsers and will generate unknown CA errors in browsers.



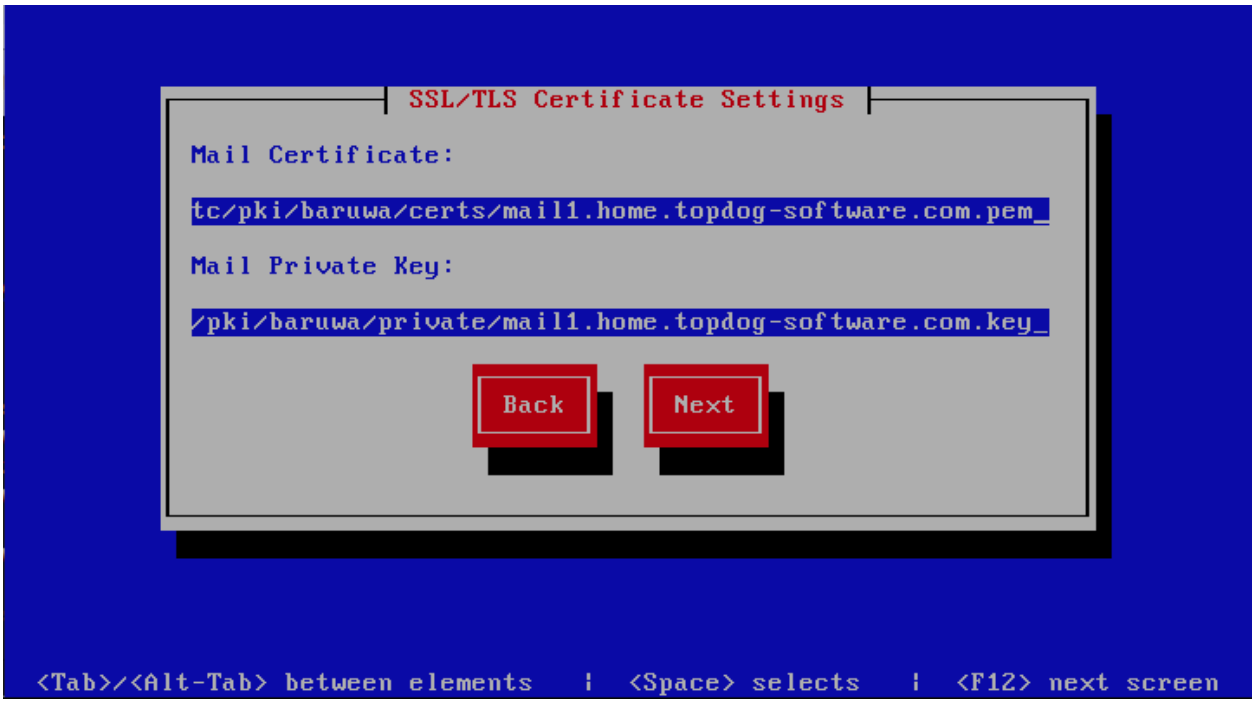
If you left `I have a CA issued Certificate` unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

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 certificate and key. The description of the options is as follows:

Option	Description
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

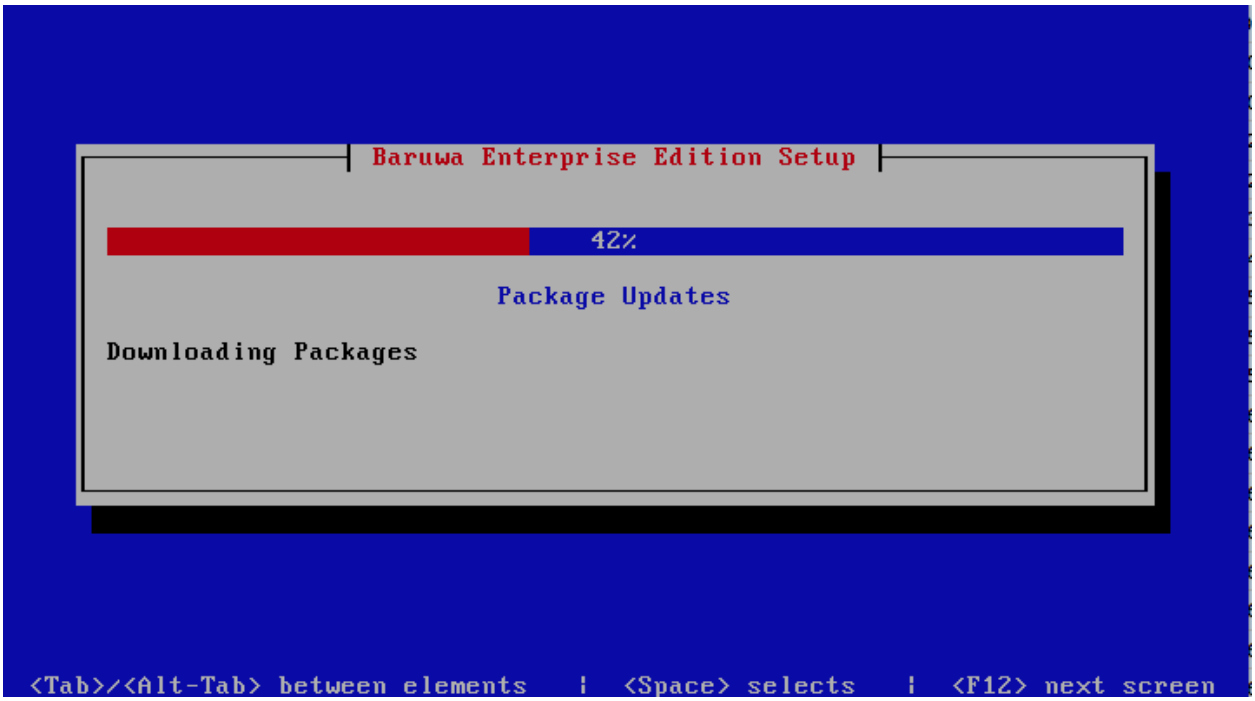


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

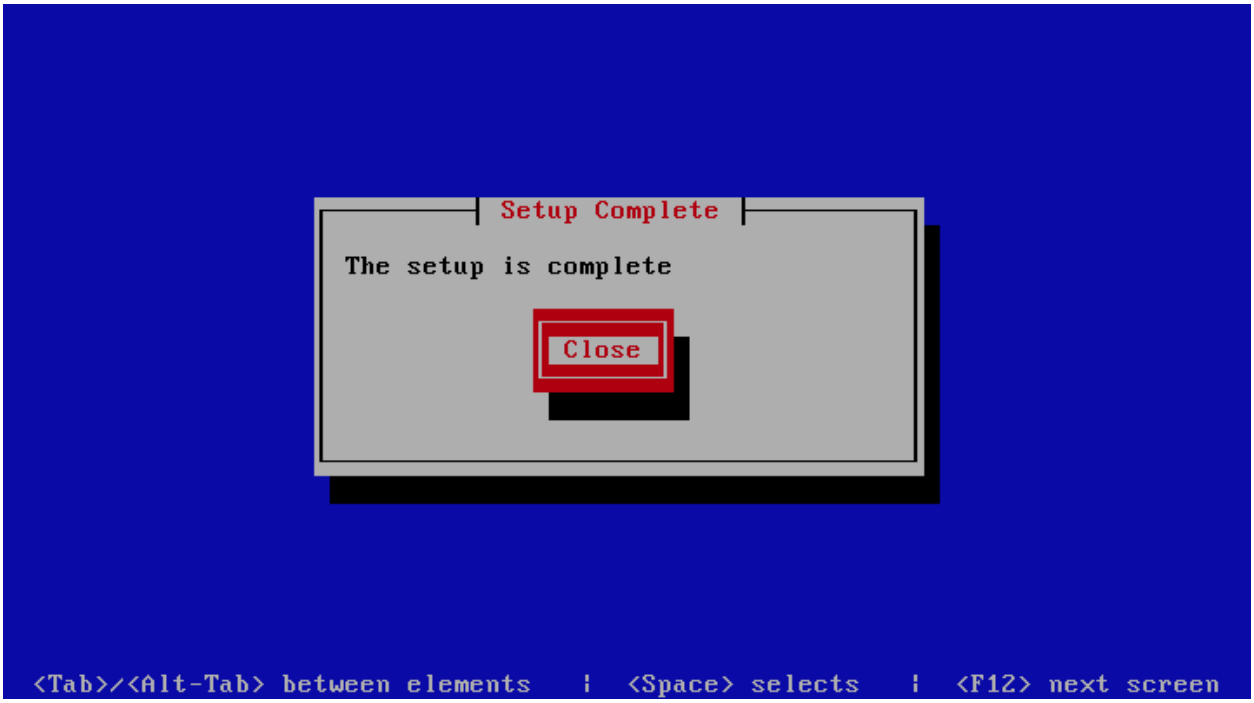
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

Warning: If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.8 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.

This profile is used in the *Distributed Backend Distributed Frontend* and *Single Backend Distributed Frontend* topologies.

8.8.1 Automated Configuration

Baruwa Enterprise Edition >= 2.0.7 uses an automated wizard based utility called *baruwa-setup* to configure, update and manage the system. On the first run 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 and management process so the user does not have to manually edit any configuration files.

The *baruwa-setup* command is idempotent, meaning it safe to run multiple times and will only make changes if they are required. All future updates and configuration changes to the system should be done using the *baruwa-setup* command. The utility has a man page that documents all the options available.

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.

Then issue the *baruwa-setup* command at the command prompt:

```
baruwa-setup
```

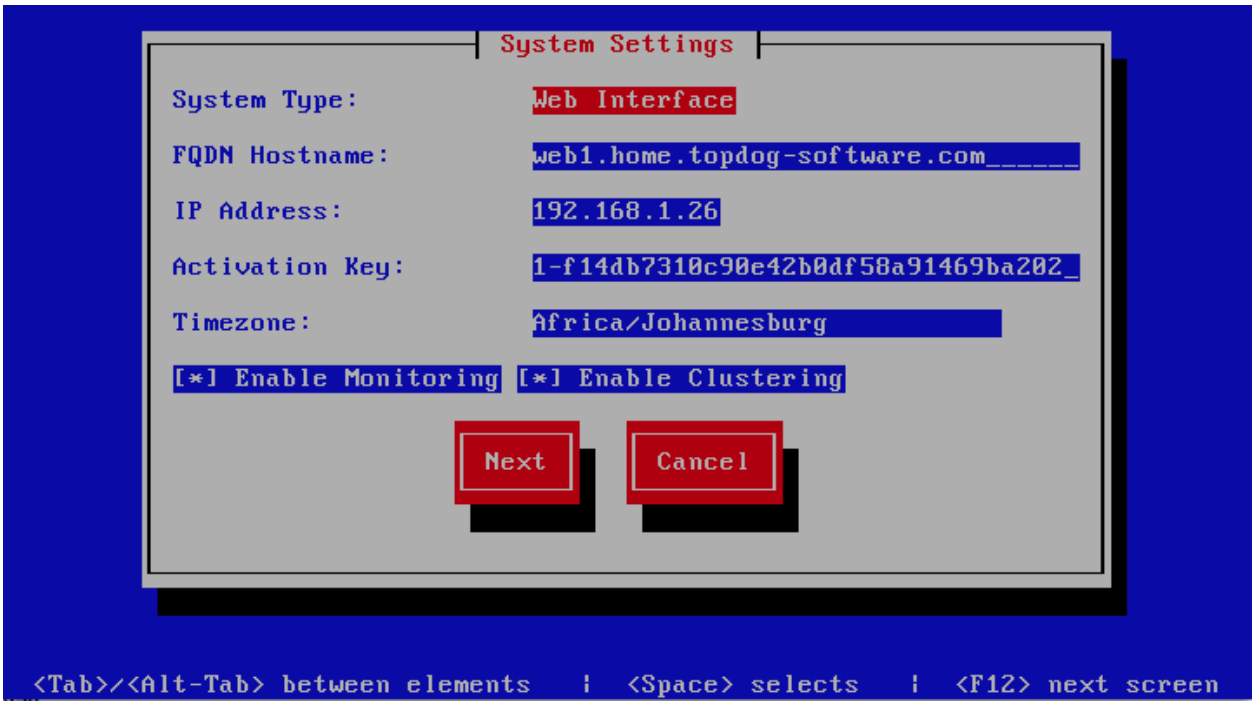
The program will ask you to set a passphrase, enter the passphrase and press enter re-enter the same passphrase again to confirm. If the passphrase is accepted the System settings screen below will be displayed.

Warning: Do not loose this passphrase, there is no way to recover it. A reinstallation will be required if you loose the passphrase.

System Settings

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

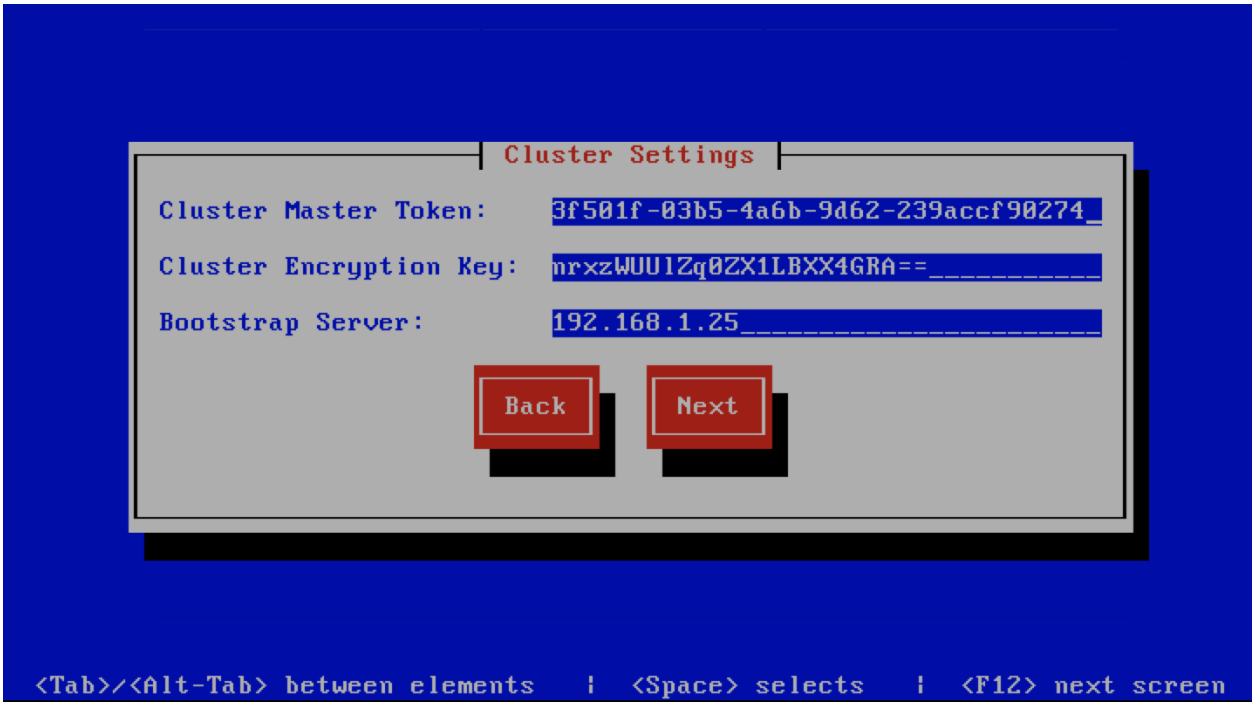
Option	Description
System Type	Set this to Web Interface
FQDN Hostname	This is the Fully qualified domain name This cannot be set to localhost
IP Address	The system IP address usually detected
Activation Key	Baruwa Enterprise Edition Activation Key
Timezone	The system timezone, detected from the system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



Cluster Settings

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

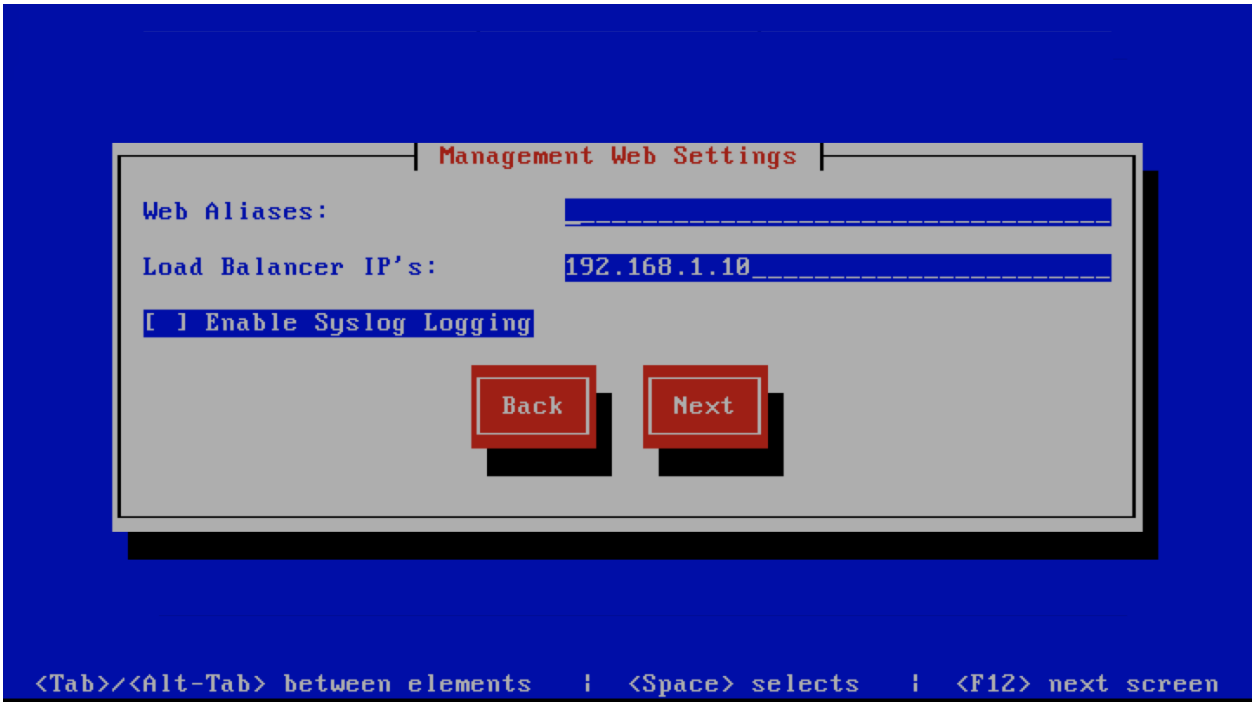
Option	Description
Cluster Master Token	The cluster's master token, you can get it by running `baruwa-setup -e master_token` on the bootstrap server.
Cluster Encryption Key	The cluster's encryption key, you can get it by running `baruwa-setup -e cluster_secret` on the bootstrap server
Bootstrap server	The IP address of the bootstrap server



Management Web Settings

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

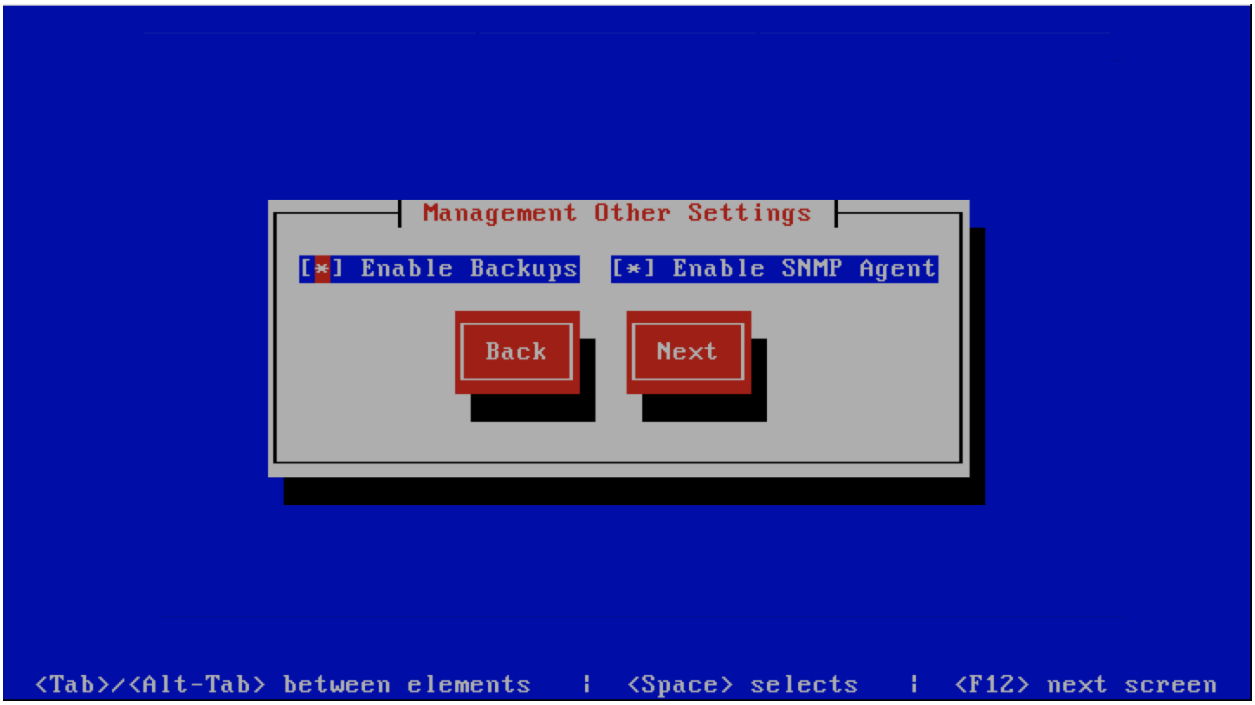
Option	Description
Web Aliases	Alternative hostnames to use to access the web interface. Use a space to separate multiple entries
Load Balancer IP's	Proxy-Protocol load balancers, space separated IP Address list
Enable Syslog Logging	Turns on Web logging to syslog



Management Other Settings

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

Option	Description
Enable Backups	Enables or disabled the backup system [*Baruwa Backups*]
Enable SNMP Agent	Enables the SNMP Agent which makes the system status available via SNMP. This option is ineffective if monitoring has not been enabled.



SSL/TLS Settings

The Baruwa web interface MUST ran 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 request a CertBot certificate or generate a non recognised Builtin 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.

Certbot certificate

The issuance of a CertBot certificate is based on an automated check that verifies that the hostnames specified are under your control. Baruwa performs a precheck to verify that the hostnames resolve to a public IP address on the host itself. If this check fails then the Certbot certificate will not be requested. This check will fail if your public IP address is on another device and you are forwarding connections to a private address on your Baruwa system. To work around that you need to create a check file:

```
touch /etc/baruwa/acme.enable
```

For the validation process to succeed, Certbot systems need to be able to connect to port 80 on your system, ensure that that is allowed on your network devices.

Certbot certificates are only issued to systems of the *Standalone System*, *Web and Mail System* and *Web Interface System* profiles.

Certbot certificates are issued only to the web hostname, web aliases and the mail hostname. Cluster members names are not included in the certificate.

Support for CertBot certificates was added in BaruwaOS 6.8, refer to the *ACME TLS Certificates* section of the release notes for more information.

Note: It is currently not possible to issue or syncronize certificates in a cluster that uses the same hostname. If you are operating a cluster you should either purchase a Commercial CA issued certificate or use Builtin certificates.

Commercial CA issued certificate

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

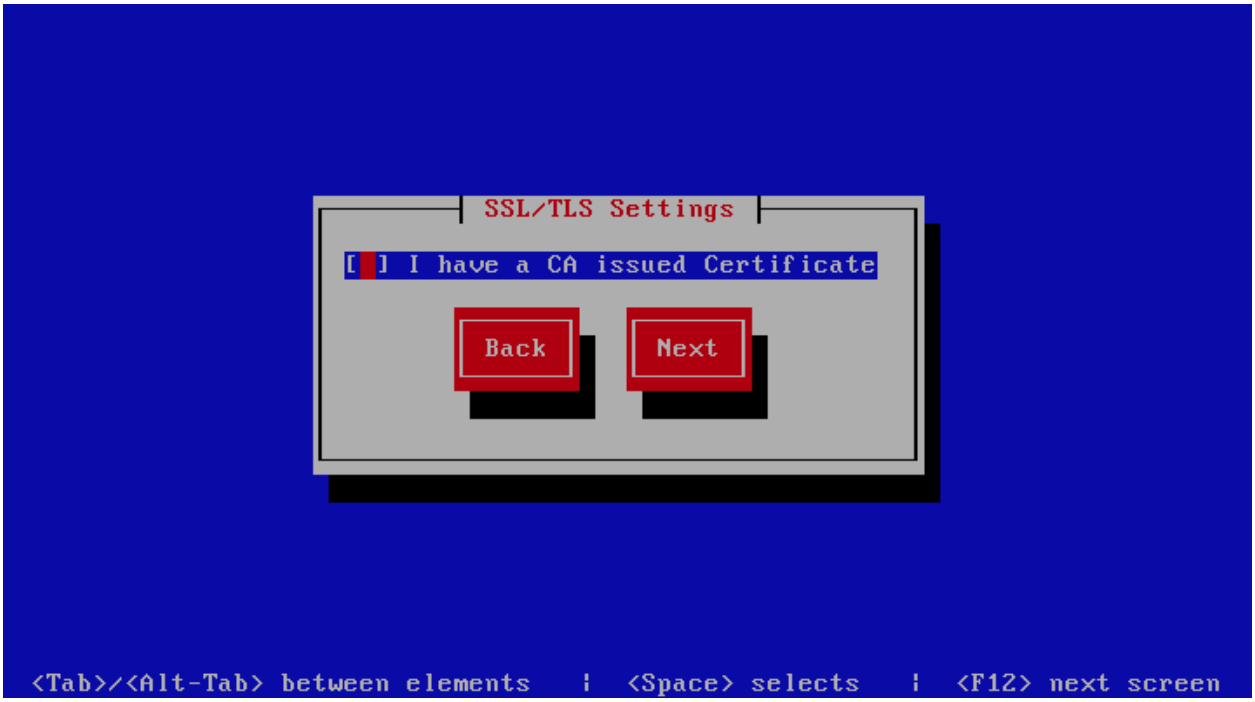
If your SSL certificate is signed using an intermediate certificate, you need to append the intermediate certificate to the file `/etc/pki/baruwa/certs/baruwa.pem`. The server certificate must appear before the intermediate certificate in the combined file.

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.

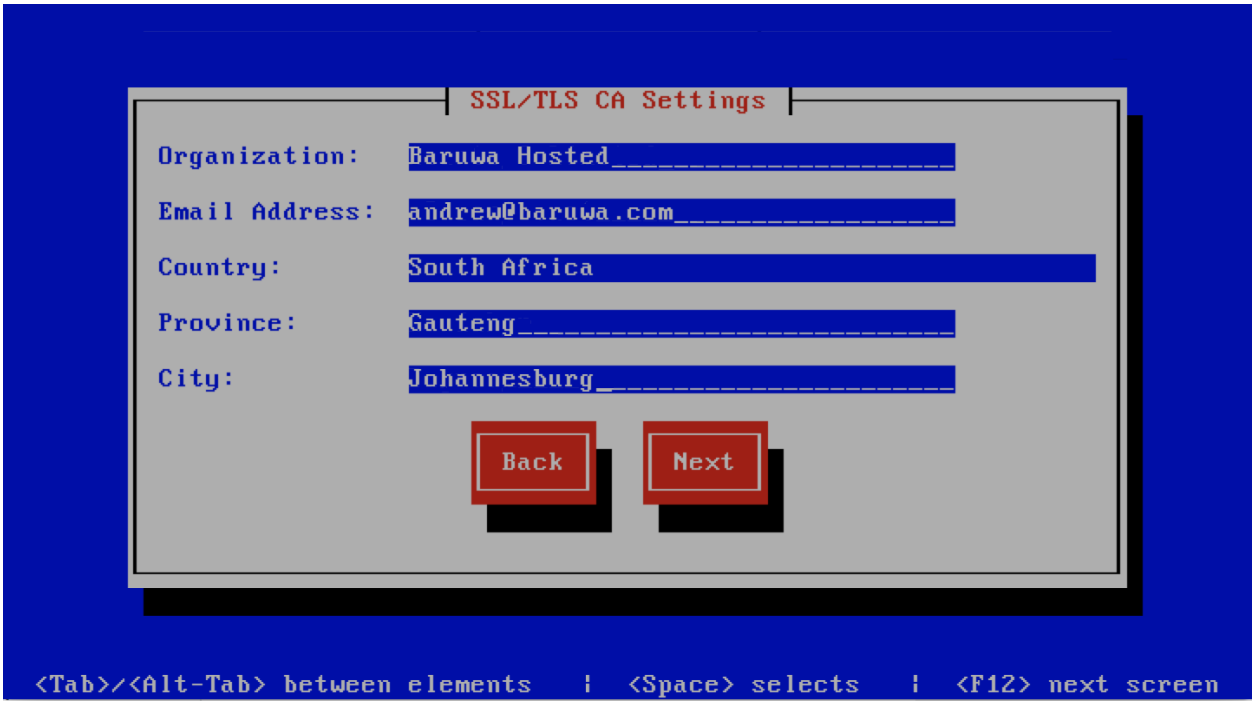
Builtin certificate

The certificate that `baruwa-setup` generates contains all the relevant system names. The downside to the builtin certificates is that they are signed by the BaruwaCA meaning they will not be recognized by browsers and will generate unknown CA errors in browsers.



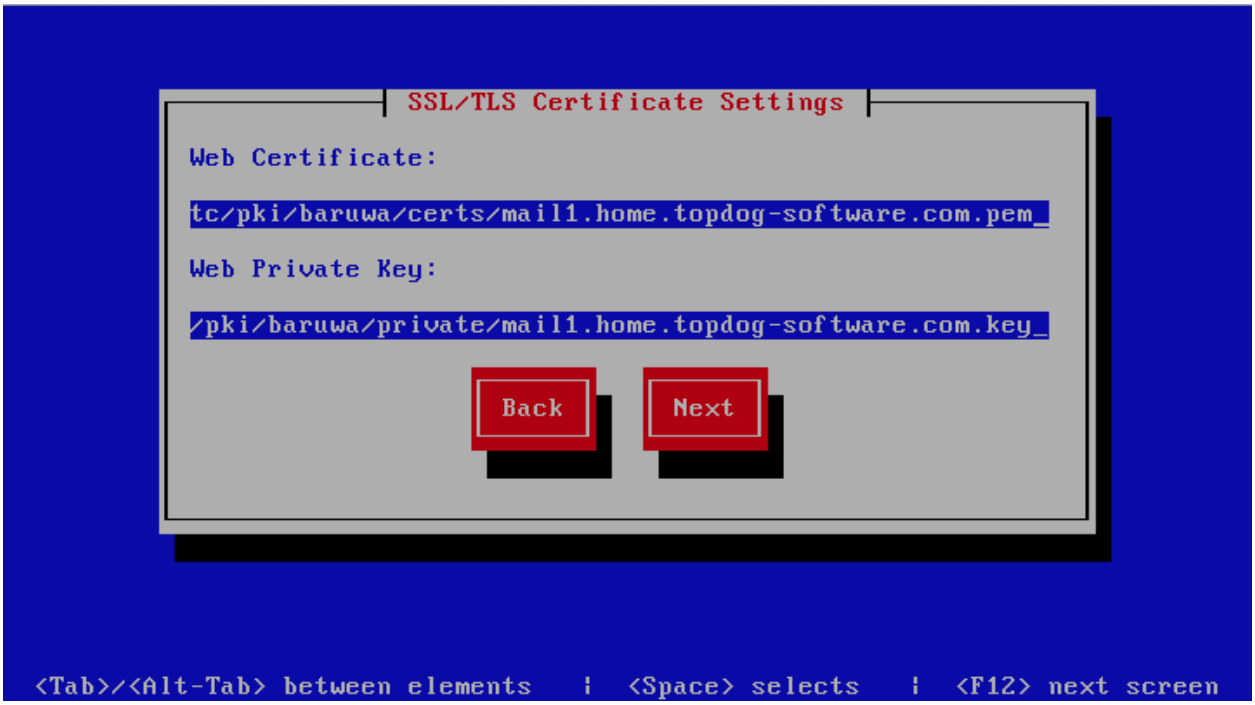
If you left `I have a CA issued Certificate` unchecked you will be presented with the following screen. You need to fill in the details which are used to create a CA from which the certificate will be issued. The description of the options is as follows:

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 certificate and key. 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

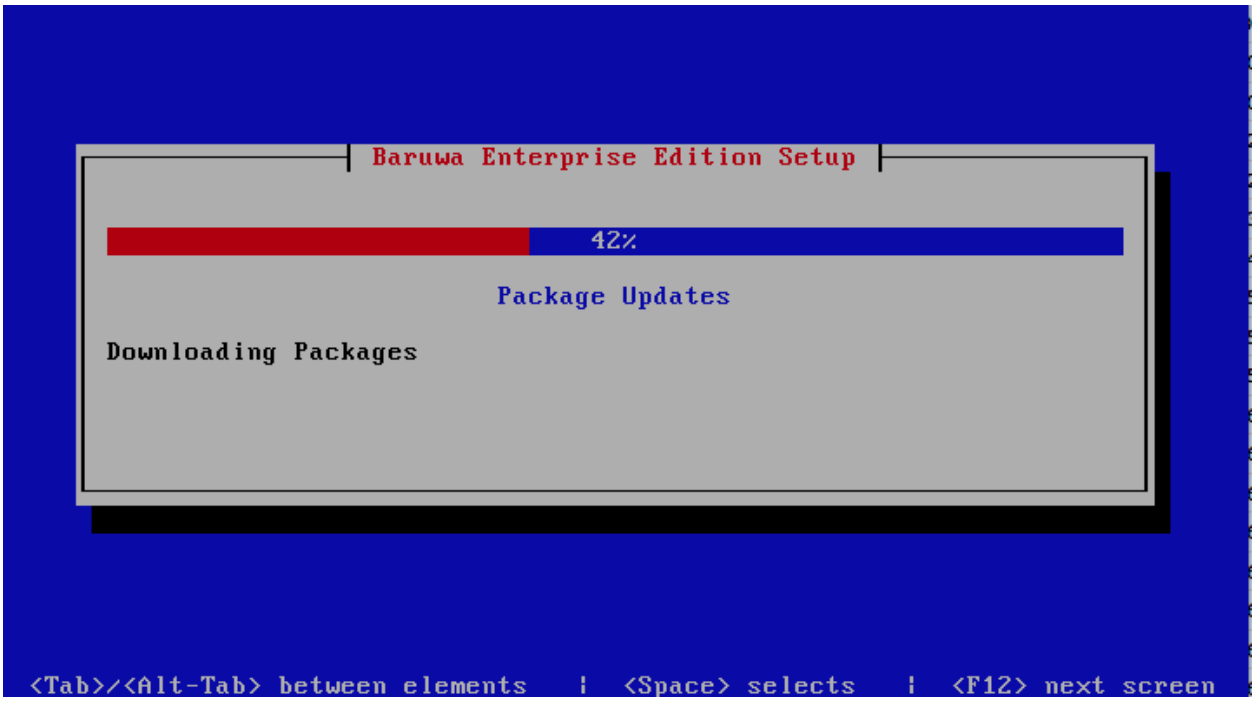


Setup Running

The `baruwa-setup` program will now ran the setup processes to configure the system. The processes include updating all the packages on the system. If a newer version of `baruwa-setup` is downloaded and installed, the process will reload the `baruwa-setup` command. When this happens a notification message with a 30 second countdown timer will be displayed and the `baruwa-setup` command will reload and display the initial (`System Settings`) screen. If this happens simply press the `next` button or the `F12` key until you get to the `Setup Running` screen again.

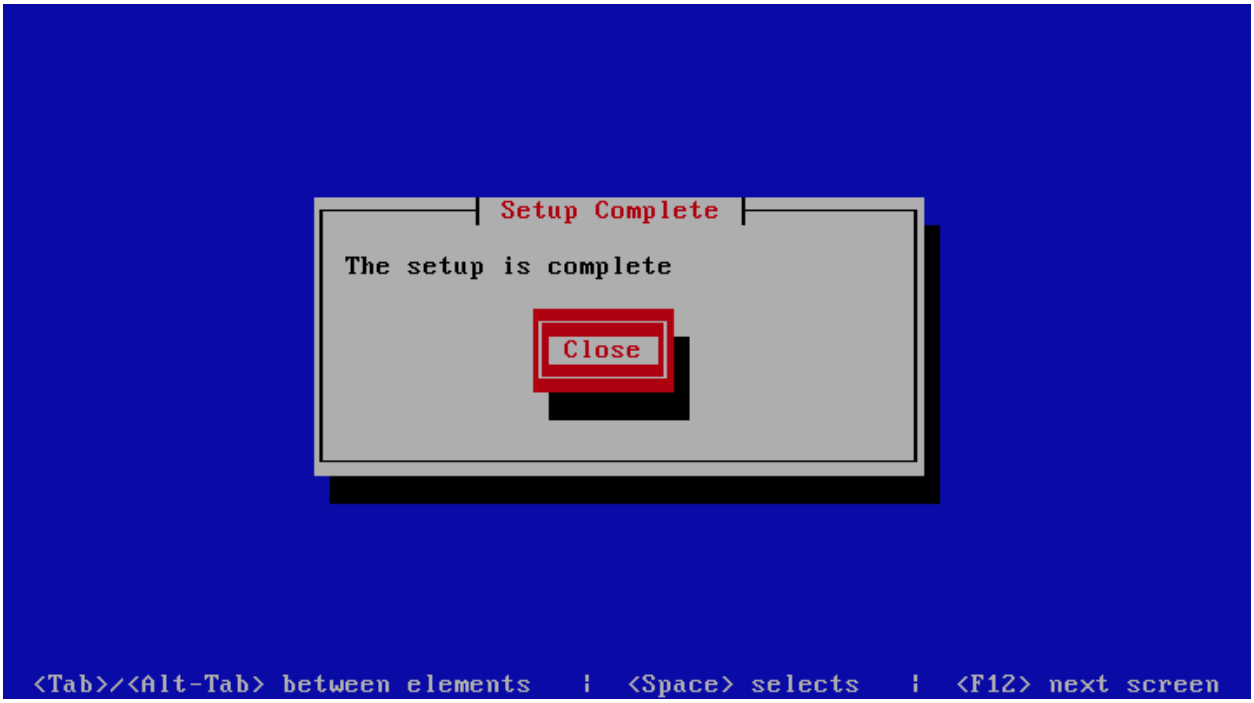
At this point there is nothing left for you to do until the setup is complete. The program will update the screen with status information as well as logging it to `/var/log/messages`. If an error occurs the error information will be displayed until you press the enter button and the program will exit.

Warning: If an error occurs while running setup, `DO NOT REINSTALL` the system copy the error and contact support.



Setup Complete

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



To ensure that all the settings are correctly applied `reboot` the server from the command line using the command:

```
reboot
```

8.8.2 Post Configuration

Now that the installation and setup are complete, you need to finalize the setup by *Adding a Scanning Node*, *Adding 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 to the Organization
- Add a delivery server for the Domain
- Add a Domain Administrator Account for the organization
- Edit the Organization and assign Domain Administrator to the organization
- Add any user accounts to the Domain if not using external authentication

Review the *DNS*, *Administrators guide*, *Email Protection Best Practices* and *Advanced configuration* sections for other configuration and setup options available.

CHAPTER

NINE

ADVANCED CONFIGURATION

9.1 Content Protection

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.1.4 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.

9.1.5 Configuration

The content protection system is configured using the Settings menu of the web interface. The instructions are available via *Content Protection*

9.2 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.

Administrative accounts can not be configured to use external authentication.

9.2.1 Supported Mechanisms

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

- LDAP
- RADIUS
- IMAP
- POP3
- SMTP
- SAML2

9.2.2 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*

9.2.3 Planned Mechanisms

Future support is planned for the following

- OAUTH

9.3 Clustering

9.3.1 Functionality available

Baruwa is capable of running in a cluster. The cluster is divided into the frontend and backend segments. Backend clustering is available in versions >= `2.1.7`.

Full Frontend Baruwa functionality is available from any member within a Baruwa Frontend segment cluster and all Frontend segment 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*

9.3.2 Requirements

Network quality

High quality network links are required between the front end and backend segments in a cluster.

Cluster Quoram

Warning: Do not setup a backend segment cluster with `even number servers` or `one server` as you may loose your data if you do. The impact is not as severe on front end servers.

To setup an efficient cluster you should have an odd number for each system type. So if you are setting up a cluster of database servers for example you need to have `3`, `5`, `7`, `9` etc servers of database type.

Server location

For backend segment systems the systems should be installed in different locations. If you install the systems in the same locations you will experience issues restoring the service if there is a location wide power failure that takes down all your servers.

Bootstrap server

A bootstrap server is required to setup a cluster. A bootstrap server is the initial server used to bring up the cluster. It can be of the `backend` or `database` profiles. You only need `one` bootstrap server per cluster. The bootstrap server is the first server that you should setup.

Note: For backwards compartibility with previous non clustered backend systems, existing systems of `backend` or `database` profile are automatically configured as bootstrap servers during upgrade to `BaruwaOS 6.9.1`.

Root CA Key

A root CA is created on the bootstrap server, the public key of that CA is stored at `/etc/pki/BaruwaCA/certs/BaruwaCA.pem`. This public key must be copied to all the members of a cluster prior to starting configuration.

Cluster Master Token and Cluster Encryption Key

During configuration of the bootstrap server, a `Cluster Master Token` and a `Cluster Encryption Key` is generated on the bootstrap server. These two should then be used on other cluster members that require these parameters.

9.3.3 Shared quarantine

Since version `2.1.0` Baruwa now has built in shared quarantine syncronization without a shared storage system. Quarantined messages are now syncronized between all the cluster nodes. This eliminates the need for a shared filesystem as was previously required. Because messages are syncronized between the cluster members any of the cluster members can process requests to release, learn delete quarantined messages. Users are able to access messages even when the specific host that processed the message via SMTP is not accessible.

Note: Note this is a technology preview and at the moment could have performance degradation issues in mail high volume environments.

When you select `use shared quarantine` in *baruwa-setup*, built in syncronization is automatically enabled, if you wish to use a shared filesystem on Baruwa versions >= 2.1.0 you need to overide the built in syncronization by creating the file `/etc/baruwa/sync.disable`. You can do that by running the following command:

```
touch /etc/baruwa/sync.disable
```

In order for the cluster hosts to be able to locate each other you need to add them as nodes under `Settings` and provide the correct IP address. The cluster nodes perform syncronization on port `TCP 1027`. If some of your cluster nodes are behind a port forwarded firewall, you need to forward port `1027` to the actual cluster node. If you have multiple nodes behind the same firewall you should use different ports to portforward to `1027` on each internal server. You then need to modify the scanning node under settings and set the port to the port you have configured for this specific server on the firewall.

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 with a shared storage system 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*

9.3.4 Limitations

Host specific quarantines

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.

Management traffic

Note: This limitation is not present when using a clustered backend, available in versions >= `2.1.7`.

Given that the primary function of the Baruwa System is processing of email, full high availability is limited to the mail processing function.

In event of backend server connectivity or functionality failure, email processing will NOT be disrupted and will continue functioning normally.

The management interface how ever will be unaccessible in event of backend server connectivity or functionality failure.

When the backend server connectivity or functionality is restored, resyncronization of the system will take place and the management interface will return to normal functionality.

9.3.5 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*

To use Baruwa Enterprise Edition HTTP servers with these load balancers you need to specify the load balancer IP addresses in the `Load Balancer IP's` field on the `Management Web 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 send-proxy
        server web2 192.168.1.23:80 check send-proxy

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

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
```

9.4 Customization

Baruwa Enterprise Edition configuration is done via a configuration management system, this means that manual changes to files are overwritten by the configuration management system.

In some cases end users would like to make local customizations which should not be overwritten. This section provides information on the supported customization mechanisms within Baruwa.

9.4.1 Configuration system customization

From BaruwaOS version 6.7.3, the entire configuration management system can be customized with local changes that are not overwritten when the system is upgraded or baruwa-setup is run.

Configuration system customization is supported by the salt configuration engine not the puppet configuration engine. The salt configuration engine is the default engine in BaruwaOS versions >= 6.7.3.

To customize a configuration module make a copy of the module from */srv/baruwa/salt/base* into */srv/baruwa/salt/custom*. You can then make changes to the module within the */srv/baruwa/salt/custom* directory. This changes will override the default configuration module.

Note: Please note that you will be responsible for syncing any changes made to the upstream module to your own custom module when ever the upstream module is updated.

9.4.2 MTA Customization

The MTA configuration provides a number of hooks to allow the user to merge their own configuration into the running configuration managed by the configuration management system.

The following hooks are available.

Config file name	Purpose
/etc/exim/macros.conf.local	Redefine the macros in /etc/exim/macros.conf
/etc/exim/custom-lists.post	Add lists to lists section
/etc/exim/custom-vars.post	Add additional config options
/etc/exim/custom-acl_check_auth.pre	Add ACL's before the acl_check_auth ACL
/etc/exim/custom-acl_check_auth.post	Add ACL's after the acl_check_auth ACL
/etc/exim/custom-acl_check_quit.pre	Add ACL's before the acl_check_quit ACL
/etc/exim/custom-acl_check_quit.post	Add ACL's after the acl_check_quit ACL
/etc/exim/custom-acl_check_notquit.pre	Add ACL's before the acl_check_notquit ACL
/etc/exim/custom-acl_check_notquit.post	Add ACL's after the acl_check_notquit ACL
/etc/exim/custom-acl_check_mail.pre	Add ACL's before the acl_check_mail ACL
/etc/exim/custom-acl_check_mail.post	Add ACL's after the acl_check_mail ACL
/etc/exim/custom-acl_check_rcpt.pre	Add ACL's before the acl_check_rcpt ACL
/etc/exim/custom-acl_check_rcpt-rbls	Add RBL ACL's before the builtin RBL ACL's in the acl_check_rcpt ACL
/etc/exim/custom-acl_check_rcpt.post	Add ACL's after the acl_check_rcpt ACL
/etc/exim/custom-acl_check_data.pre	Add ACL's before the acl_check_data ACL
/etc/exim/custom-acl_check_data.post	Add ACL's after the acl_check_data ACL
/etc/exim/custom-acl_check_mime.pre	Add ACL's before the acl_check_mime ACL
/etc/exim/custom-acl_check_mime.post	Add ACL's after the acl_check_mime ACL
/etc/exim/custom-acl_check_connect.pre	Add ACL's before the acl_check_connect ACL
/etc/exim/custom-acl_check_connect.post	Add ACL's after the acl_check_connect ACL
/etc/exim/custom-acl_check_helo.pre	Add ACL's before the acl_check_helo ACL
/etc/exim/custom-acl_check_helo.post	Add ACL's after the acl_check_helo ACL
/etc/exim/custom-acl_check_dkim.pre	Add ACL's before the acl_check_dkim ACL
/etc/exim/custom-acl_check_dkim.post	Add ACL's after the acl_check_dkim ACL
/etc/exim/custom-routers.pre	Add routers before the default routers
/etc/exim/custom-routers-post-split.pre	Add routers before the split router
/etc/exim/custom-routers.post	Add routers after the default routers
/etc/exim/custom-transports.pre	Add transports before the default transports

Continued on next page

Table 9.1 – continued from previous page

/etc/exim/custom-transports.post	Add transports after the default transports
/etc/exim/custom-routers-out.pre	Add Outbound routers before the default routers
/etc/exim/custom-routers-out.post	Add Outbound routers after the default routers
/etc/exim/custom-transports-out.pre	Add Outbound transports before the default transports
/etc/exim/custom-transports-out.post	Add Outbound transports after the default transports

9.4.3 Scanner Customization

The Mail Scanning system configuration can be overridden by creating .local settings files in */etc/MailScanner/baruwa/rules* The following configuration files can be customized using the *filename.local* system.

Settings Filename	Purpose
approved.senders.rules	Approved senders ruleset
archives.filename.rules	Archives filenames ruleset
archives.filetype.rules	Archives filetype ruleset
banned.senders.rules	Banned senders ruleset
deletedcontentmessage.rules	Deleted content message ruleset
deletedfilenamemessage.rules	Deleted filename message ruleset
deletedsizemessage.rules	Deleted message size message ruleset
deletedvirusmessage.rules	Deleted virus message ruleset
disinfectedreport.rules	Disinfected report ruleset
filename.rules	Blocked filename ruleset
filetype.rules	Blocked filetype ruleset
highspam.actions.rules	Definate spam actions ruleset
highspam.score.rules	Definate spam score ruleset
html.sigs.rules	HTML signature ruleset
inlinespamwarning.rules	Inline SPAM warning html message ruleset
inlinewarninghtml.rules	Inline SPAM warning text message ruleset
inlinewarningtxt.rules	Inline warning text message ruleset
languages.rules	Languages ruleset
message.size.rules	Message size ruleset
recipientspamreport.rules	Spam report ruleset
rejectionreport.rules	Rejection report ruleset
sendercontentreport.rules	Content protection report ruleset
sendererrorreport.rules	Sender Error report ruleset
senderfilenamereport.rules	Sender filename report ruleset
sendersizereport.rules	Sender message size report ruleset
senderspamrblreport.rules	Sender RBL blocked report ruleset
senderspamreport.rules	Sender SPAM blocked report ruleset
senderspamsareport.rules	Sender SPAM report ruleset
sendervirusreport.rules	Sender Virus Blocked report ruleset
sig.imgs.names.rules	Signature image names ruleset
sig.imgs.rules	Signature images ruleset
sign.clean.msgs.rules	Sign clean messages ruleset
spam.actions.rules	Possible spam actions ruleset
spam.checks.rules	Spam checks ruleset
spam.score.rules	Spam score ruleset
storedcontentmessage.rules	Stored content message ruleset

Continued on next page

Table 9.2 – continued from previous page

storedfilenamemessage.rules	Stored filename message ruleset
storedsizemessage.rules	Stored size message ruleset
storedvirusmessage.rules	Stored virus message ruleset
text.sigs.rules	Text signature ruleset
virus.checks.rules	Virus checks ruleset

9.5 Addons

9.5.1 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.

9.6 Additional Anti Virus Engines

By default Baruwa Enterprise Editions runs the ClamAV Anti Virus engine at SMTP time. You can on a per domain basis change this behaviour to have Anti Virus checks run after you have accepted the message.

You can also ran additional Anti Virus Engines both at SMTP time within the MTA process and after accepting the message from within the scanner process.

The recommended approach is to ran Anti-Virus checks at SMTP time and reject the messages straight away.

The following Anti Virus Engines are supported.

Name	SMTP Time Scanning	POST SMTP Time Scanning
ClamAV	Yes	Yes
Sophos	Yes	Yes
F-Secure	Yes	Yes
ESET	No	Yes
F-PROT	Yes	Yes
AVAST	Yes	Yes

9.6.1 Installation and Configuration

ClamAV

ClamAV is part of the base install and is configured to run by default at SMTP time. If you want to perform scanning POST SMTP time then you need to select the `Clamav Daemon` under virus checks in the MailScanner settings section of the interface.

Sophos

To install Sophos, download the `Antivirus for Linux` package from the Sophos website. The software is free to download and use.

You need an additional 1GB of RAM to ran the Sophos Anti-Virus Engine.

Copy the tar file to the `/usr/local/src` directory on your server.

Follow the following steps to install and configure the software.

- Extact the files from the tar file.:

```
tar xvf sav-linux-free-9.tgz
```

- Run the setup script:

```
./sophos-av/install.sh
```

- The script will prompt you for information as follows.:

```
Press <return> to display Licence. Then press <spc> to scroll forward.
```

Press enter, until you get to the bottom of the License text.:

```
Do you accept the licence? Yes(Y)/No(N) [N]
```

Type `Y` if you want to accept the license or `N` if not. If you enter `N` then the script will exit.:

```
Where do you want to install Sophos Anti-Virus? [/opt/sophos-av]
```

Leave at the default and press enter.:

```
Do you want to enable on-access scanning? Yes(Y)/No(N) [Y]
```

Type `N` and press enter.:

```
Which type of auto-updating do you want? From Sophos(s)/From own server(o)/None(n) [s]
```

Press enter.:

```
Do you wish to install the Free (f) or Supported (s) version of SAV for Linux? [s]
```

Type `s` if you want the supported version or `f` for the free version.:

```
Do you need a proxy to access Sophos updates? Yes(Y)/No(N) [N]
```

Press enter.

The script will perform the installation and setup. If all goes well you should get the following message:

```
Starting Sophos Anti-Virus daemon:                         [  OK  ]
Installation completed.
```

- At this point you are now ready to configure the software. To do so run the following:

```
/opt/sophos-av/bin/savconfig UINotifier false
/opt/sophos-av/bin/savconfig EmailNotifier false
/opt/sophos-av/bin/savconfig EnableOnStart false
/opt/sophos-av/bin/savconfig UIttyNotification false
/opt/sophos-av/bin/savconfig SendThreatEmail false
/opt/sophos-av/bin/savconfig UpdatePeriodMinutes 30
/opt/sophos-av/bin/savconfig EmailDemandSummaryIfThreat false
/opt/sophos-av/bin/savupdate
/opt/sophos-av/bin/savdctl --daemon disable
service sav-protect restart
```

Sophos Integration

There are two ways in which Sophos can be integrated into Baruwa Enterprise Edition:

- *Sophos SAVID*
- *Sophos Command line*

Sophos SAVID is the most efficient way to integrate, however it is only available to Sophos paying customers. If you are not a paying customer then you need to select the *Sophos Command line* option.

Sophos SAVID

To enable the `SAVID` integration method, you need to download and install the SAV Dynamic Interface Linux 64 bit package (`Sophos account required`).

Copy the tar file to the /usr/local/src directory on your server.

Follow the following steps to install and configure the software.

- Extact the files from the tar file.:

```
tar xvf savdi-linux-64bit.tar
```

- Run the install script:

```
cd savdi-install/
./savdi_install.sh
```

- Create the required directories:

```
mkdir /var/lib/savdid
mkdir /var/run/savdid
chmod 0700 /var/run/savdid
chmod 0750 /var/lib/savdid
```

- Create the group and user:

```
groupadd -r savdid
useradd -r -g savdid -d /var/lib/savdid -s /sbin/nologin -c "Sophos savdid user"␣
↪savdid
```

- Change the directory ownership:

```
chown savdid.exim /var/lib/savdid
chown savdid.savdid /var/run/savdid
```

- Download and install configuration file:

```
cp /usr/local/savdi/savdid.conf /usr/local/savdi/savdid.conf.orig
curl -o /usr/local/savdi/savdid.conf https://raw.githubusercontent.com/baruwa-
↪enterprise/baruwa-misc/master/savdid.conf
```

- Download and install the init script:

```
curl -o /etc/init.d/savdid https://raw.githubusercontent.com/baruwa-enterprise/
↪baruwa-misc/master/savdid.init
chmod +x /etc/init.d/savdid
chkconfig savdid on
```

- Startup the `SAVID` service:

```
service savdid start
```

- Add a custom MTA configuration overide for SMTP Time scanning (Skip if you want to scan after SMTP time):

```
cat >> /etc/exim/custom-acl_check_data.post << 'EOF'
  warn    hosts         = 127.0.0.1
          add_header    = X-Baruwa-Virus-Checks: bypassed, quarantine release
  drop    set acl_m_av_scanner = sophie:/var/lib/savdid/savdid.sock
          malware       = ${if and { \
                                  {!eq {$sender_host_address}{127.0.0.1}} \
                                  {eq {${perl{ip_in_network}{SAVDB}{$sender_host_
↪address}}}{false}} \
                                  {eq {${if forall{<, $recipients}{match{\
                                      ${extract{smtp_av}{${lookup{$item}cdb*@{/
↪var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}{no}}}{yes}} \
                                  {eq {${if forall{<, $recipients}{\
                                      match{${extract{virus_checks}{${lookup{
↪$item}cdb*@{/var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}
↪{no}}}{yes}} \
                              }{*}{0}}
          message       = The message was rejected due to security policies -␣
↪INFO_URL#mvi
          log_message   = This message matched anti-virus signature [$malware_
↪name]
EOF
```

- Install and startup the update notification system:

```
yum install python-watcher -y
chkconfig python-watcher on
service python-watcher start
```

- To enable POST SMTP Time Scanning, select the `Sophos SAVID` under virus checks in the MailScanner settings section of the interface.

Sophos Command line

Use the command line integration option if you are not a Sophos paying customer or if you want to do POST SMTP scanning.

- Create a wrapper script for SMTP Time scanning:

```
cat > /usr/local/bin/sav-scan << 'EOF'
#!/bin/bash
#
# Wrap the savscan
/opt/sophos-av/bin/savscan -nb -sc -f -all -rec -ss -archive -loopback --no-
↪follow-symlinks --no-reset-atime -tnef -mime -oe -pua -suspicious "$1"
exit 0
EOF
```

- Make the wrapper script executable:

```
chmod +x /usr/local/bin/sav-scan
```

- Add a custom MTA configuration overide for SMTP Time scanning (Skip if you want to scan after SMTP time):

```
cat >> /etc/exim/custom-acl_check_data.post << 'EOF'
  warn    hosts         = 127.0.0.1
          add_header    = X-Baruwa-Virus-Checks: bypassed, quarantine release
  drop    set acl_m_av_scanner = cmdline:/usr/local/bin/sav-scan %s: found in␣
↪file:'(.+)'
          malware       = ${if and { \
                                    {!eq {$sender_host_address}{127.0.0.1}} \
                                    {eq {${perl{ip_in_network}{SAVDB}{$sender_host_
↪address}}}{false}} \
                                    {eq {${if forall{<, $recipients}{match{\
                                        ${extract{smtp_av}{${lookup{$item}cdb*@{/
↪var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}{no}}}{yes}} \
                                    {eq {${if forall{<, $recipients}{\
                                        match{${extract{virus_checks}{${lookup{
↪$item}cdb*@{/var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}
↪{no}}}{yes}} \
                                }{*}{0}}
          message       = The message was rejected due to security policies -␣
↪INFO_URL#mvi
          log_message   = This message matched anti-virus signature [$malware_
↪name]
EOF
```

- Restart mailscanner for the above configuration to take effect:

```
service mailscanner restart
```

- To enable POST SMTP Time Scanning, select the `Sophos` under virus checks in the MailScanner settings section of the interface.

F-Secure

To install F-Secure, download the `Linux Server Security` package from the F-Secure website. This commercial software so you need to purchase a license. If you do not have a license the software will work in evaluation mode for 30 days after which it will cease to function correctly.

You need an additional 1GB of RAM to ran the F-Secure Anti-Virus Engine.

Copy the tar file to the `/usr/local/src` directory on your server.

Follow the following steps to install and configure the software.

- Extact the files from the tar file.:

```
tar xzvf fsls-11.00.79-rtm.tar.gz
```

- F-Secure does not provide 64-bit packages so you need to install 32-bit compat packages:

```
yum install glibc.i686 libstdc++.i686
```

- Run the setup script:

```
./fsls-11.00.79-rtm/fsls-11.00.79-rtm --command-line-only --auto standalone␣
↪lang=en noremotewui nolocallogin nofirewall
```

- Edit the `/etc/opt/f-secure/fssp/fssp.conf` configuration file and make the following changes:

```
odsFileScanInsideMIME 1
odsFilePrimaryActionOnInfection 1
odsFileSecondaryActionOnInfection 2
odsAskQuestions 0
odsFollowSymlinks 1
daemonLogfileEnabled 1
daemonSocketMode 0660
socketpathGroup exim
```

- Install the `fsavd` init script:

```
cp /opt/f-secure/fssp/etc/fsavd /etc/init.d/
chmod +x /etc/init.d/fsavd
chkconfig --add fsavd
```

- Start the `fsavd` service:

```
service fsavd start
```

- Add a custom MTA configuration overide for SMTP Time scanning (Skip if you want to scan after SMTP time):

```
cat >> /etc/exim/custom-acl_check_data.post << 'EOF'
  warn    hosts         = 127.0.0.1
          add_header    = X-Baruwa-Virus-Checks: bypassed, quarantine release
  drop    set acl_m_av_scanner = fsecure:/tmp/.fsav-0
          malware       = ${if and { \
```

```
                                    {!eq {$sender_host_address}{127.0.0.1}} \
                                    {eq {${perl{ip_in_network}{SAVDB}{$sender_host_
↪address}}}{false}} \
                                    {eq {${if forall{<, $recipients}{match{\
                                        ${extract{smtp_av}{${lookup{$item}cdb*@{/
↪var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}{no}}}{yes}} \
                                    {eq {${if forall{<, $recipients}{\
                                        match{${extract{virus_checks}{${lookup{
↪$item}cdb*@{/var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}
↪{no}}}{yes}} \
                                }{*}{0}}
          message       = The message was rejected due to security policies -␣
↪INFO_URL#mvi
          log_message   = This message matched anti-virus signature [$malware_
↪name]
EOF
```

- Restart mailscanner for the above configuration to take effect:

```
service mailscanner restart
```

- To enable POST SMTP Time Scanning, select the `F-Secure` under virus checks in the MailScanner settings section of the interface.

ESET

To install ESET, download the `ESET for Linux` package from the ESET website. This is commercial software so you need to purchase a license.

You need an additional 512Mb of RAM to ran the ESET Anti-Virus Engine.

- ESET does not provide 64-bit packages so you need to install 32-bit compat packages:

```
yum install glibc.i686 libstdc++.i686
```

- Install the ESET rpm package.
- To enable POST SMTP Time Scanning, select the `ESET` under virus checks in the MailScanner settings section of the interface.

F-PROT

There is a package available for F-PROT with in our repository. This is commercial software so you need to purchase a license.

- To install the package run:

```
yum install f-prot -y
```

- Add a custom MTA configuration overide for SMTP Time scanning (Skip if you want to scan after SMTP time):

```
cat >> /etc/exim/custom-acl_check_data.post << 'EOF'
  warn    hosts         = 127.0.0.1
          add_header    = X-Baruwa-Virus-Checks: bypassed, quarantine release
  drop    set acl_m_av_scanner = f-prot6d:127.0.0.1 10200
          malware       = ${if and { \
                                    {!eq {$sender_host_address}{127.0.0.1}} \
```

```
                                    {eq {${perl{ip_in_network}{SAVDB}{$sender_host_
↪address}}}{false}} \
                                    {eq {${if forall{<, $recipients}{match{\
                                        ${extract{smtp_av}{${lookup{$item}cdb*@{/
↪var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}{no}}}{yes}} \
                                    {eq {${if forall{<, $recipients}{\
                                        match{${extract{virus_checks}{${lookup{
↪$item}cdb*@{/var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}
↪{no}}}{yes}} \
                                }{*}{0}}
          message       = The message was rejected due to security policies -␣
↪INFO_URL#mvi
          log_message   = This message matched anti-virus signature [$malware_
↪name]
EOF
```

- To enable POST SMTP Time Scanning, select the `F-prot Daemon 6` under virus checks in the MailScanner settings section of the interface.

AVAST

There is a package available for AVAST with in our repository. This is commercial software so you need to purchase a license.

Note: We are an authorized Avast reseller so you can purchase AVAST subscriptions through us at discounted list pricing.

- To install the package run:

```
yum install avast -y
```

- Install your license by copying it to `/etc/avast/license.avastlic` on your Baruwa server.
- Start the Avast daemon:

```
service avast start
```

- Add a custom MTA configuration overide for SMTP Time scanning (Skip if you want to scan after SMTP time):

```
cat >> /etc/exim/custom-acl_check_data.post << 'EOF'
  warn    hosts         = 127.0.0.1
          add_header    = X-Baruwa-Virus-Checks: bypassed, quarantine release
  drop    set acl_m_av_scanner = avast:/var/run/avast/scan.sock
          malware       = ${if and { \
                                    {!eq {$sender_host_address}{127.0.0.1}} \
                                    {eq {${perl{ip_in_network}{SAVDB}{$sender_host_
↪address}}}{false}} \
                                    {eq {${if forall{<, $recipients}{match{\
                                        ${extract{smtp_av}{${lookup{$item}cdb*@{/
↪var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}{no}}}{yes}} \
                                    {eq {${if forall{<, $recipients}{\
                                        match{${extract{virus_checks}{${lookup{
↪$item}cdb*@{/var/lib/baruwa/data/db/cleandata.cdb}}}{$value}{yes}}}{yes}}{yes}
↪{no}}}{yes}} \
                                }{*}{0}}
```

```
          message       = The message was rejected due to security policies -␣
↪INFO_URL#mvi
          log_message   = This message matched anti-virus signature [$malware_
↪name]
EOF
```

- To enable POST SMTP Time Scanning, select the `Avast` under virus checks in the MailScanner settings section of the interface.

9.7 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.

Note: Themes need to be kept up to date when changes are made to the built in templates. Ensure that you sync the changes made during each major release. If you do not keep the templates in sync you may get errors or incorrect information displayed.

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.

9.7.1 What can be customized

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

9.7.2 Guidelines

Themes `MUST` retain the copyright notice at the bottom. The copyright notice should not be obscured or hidden. Failure to comply with the rebranding guidelines will lead to termination of your subscription.

If you would like to fully rebrand the interface please purchase a rebranding license.

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

9.7.3 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>/
```

9.7.4 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
```

9.7.5 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/`

9.7.6 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 website.

9.7.7 Emails and Reports

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

9.8 Baruwa API

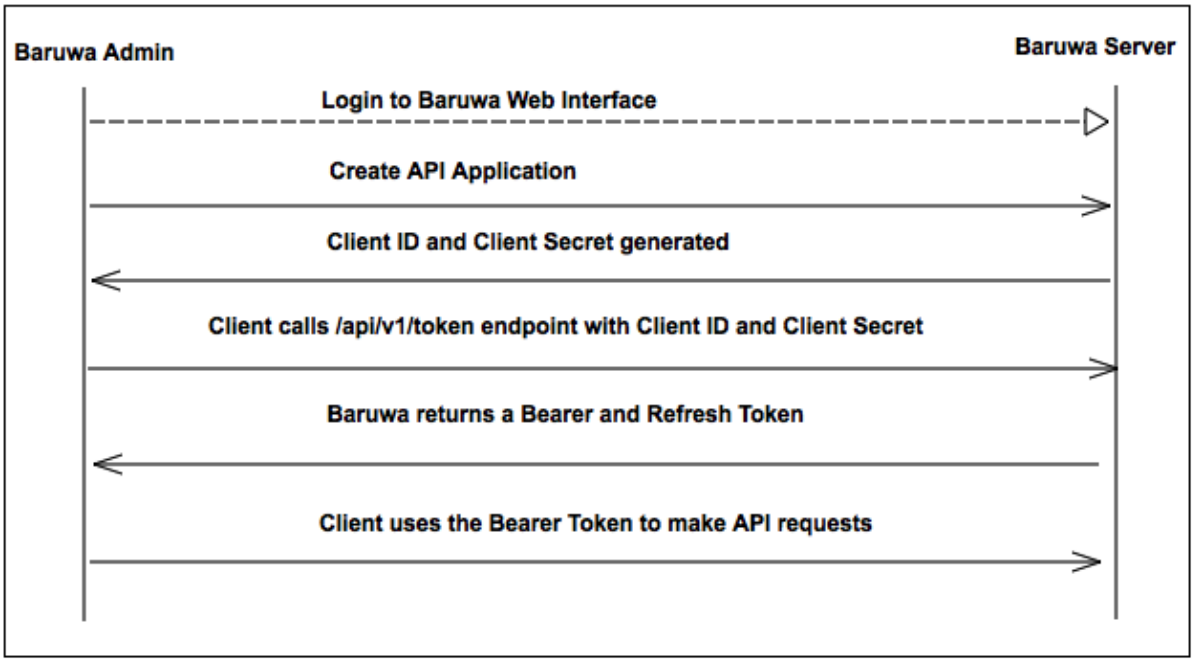
The `Baruwa API` allows you to manage a Baruwa Server in a programmatic way using conventional HTTP requests. The endpoints are intuitive and powerful, allowing you to easily make calls to retrieve information or to execute actions. The `Baruwa API` is organized around REST and uses OAUTH 2.0 authentication. 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.

9.8.1 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
```

9.8.2 Documentation

The Baruwa API documentation is available online.

9.8.3 API Libraries

Python

Available through pip:

```
pip install BaruwaAPI
```

If your system doesn't have pip, you can also use easy_install:

```
easy_install BaruwaAPI
```

The source code is in the Github BaruwaAPI repo and the package is available on PyPI

Ruby

Available as a gem:

```
gem install baruwa
```

If you use bundler, add the following line:

```
gem 'baruwa'
```

The source code is in the Github baruwa-ruby repo and the package is available on rubygems.org

Perl

Available as a cpan package:

```
cpan Net::BaruwaAPI
```

The source code is in the Github Net-BaruwaAPI repo and the package is available on cpan

Under development

The following languages are currently under development.

- Go

9.9 Email Protection Best Practices

In addition to installing and configuring Baruwa Enterprise Edition systems for your email protection you need to implement some email best practices.

Implementing these best practices will ensure, improved email performance and security.

9.9.1 Reverse DNS

The reverse DNS resolution (rDNS) maps an IP address to a hostname. Most email servers are configured to reject any email that doesn't have a valid rDNS.

You need to configure the rDNS record for your external IP address to match the mail hostname you have configured for your Baruwa servers.

9.9.2 SPF

Sender Policy Framework (SPF) is an email validation system, it is designed to detect and prevent against email spoofing.

By creating an SPF record for your domains, systems that receive email purported to be from your domain are able to verify if the system sending the email is indeed authorized to send email using that domain name.

SPF needs to be configured in each domain's Public DNS zone. The SPF syntax is documented on the openspf website. You can use the easySFP or mailradar generation tools to create your SPF records.

Various online tools exist to test SPF records you can use your favorite search engine to locate one.

9.9.3 DKIM

DomainKeys Identified Mail (DKIM) is an email authentication system, it is also designed to detect and prevent against email spoofing.

DKIM allows the receiver to check that an email claimed to come from a specific domain was indeed authorized by the owner of that domain which is done using cryptographic authentication.

DKIM keys need to be generated for each domain for which you are relaying email through the Baruwa server on your Baruwa server, and the public key needs to be added to the domain's public DNS zone.

Various online tools exist to test DKIM records you can use your favorite search engine to locate one.

9.9.4 DMARC

Domain-based Message Authentication, Reporting & Conformance, is an email validation system designed to detect and prevent against email spoofing.

DMARC is built on top of two existing mechanisms, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

DMARC needs to be configured in each domain's public DNS zone. Various tools exist to help you generate DMARC records, use your favorite search engine to locate one.

Various online tools exist to test DKIM records you can use your favorite search engine to locate one.

CHAPTER

TEN

ADMINISTRATORS GUIDE

10.1 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.

10.1.1 Adding an Organization

Organizations can be added by either importing them using a YAML file, via the API or by adding them using the `Add Organization` form.

To add an Organization by import refer to *Importing Organizations*. To add an Organization via the API refer to the API documentation.

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

10.1.2 Updating an Organization

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

10.1.3 Deleting 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

10.1.4 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

10.1.5 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`

10.1.6 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`

10.1.7 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`

10.1.8 Importing Organizations

Full organizations with their admins and domains as well as other settings can be imported. To import organizations.

1. Click `Organizations`
2. Select organization > Click `Import Organizations`
3. Browse for the YAML file by clicking `Browse` next to the `YAML file` field
4. Click the `Import` Button

10.1.9 Exporting Organizations

You can export all the organizations on a system. To export organizations.

1. Click `Organizations`
2. Click `Export Organizations`
3. Click `Download the YAML file`
4. Save the file to your computer

10.1.10 Import domains in to an organization

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

1. Click `Organizations`
2. Select organization > Click `Import domains`
3. Browse for the YAML file by clicking `Browse` next to the `YAML file` field
4. Click the `Import` Button

10.1.11 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 YAML file`
5. Save the file to your computer

10.1.12 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

10.1.13 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. You can change the `Number of messages per 15 minutes` if the default is not high enough for you
8. Enter `Probable spam score` and `Definite spam score` values if you do not want to use the defaults
9. Select the What to do with probable spam and `What to do with definite spam` actions
10. Click `Add settings`

Update Outbound SMTP IP Address settings

1. Click `Organizations`
2. Click the organization name
3. Select the Relay Host in the list at the bottom and click the edit icon
4. Make the required changes
5. Click `Update settings`

Delete Outbound SMTP IP Address settings

1. Click `Organizations`
2. Click the organization name
3. Select the Relay Host in the list at the bottom and click the delete icon
4. Click `Delete 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. You can change the `Number of messages per 15 minutes` if the default is not high enough for you
10. Click `Add settings`

Update Outbound SMTP AUTH settings

1. Click `Organizations`
2. Click the organization name
3. Select the SMTP AUTH item in the list at the bottom and click the edit icon
4. Make the required changes
5. Click `Update settings`

Delete Outbound SMTP AUTH settings

1. Click `Organizations`
2. Click the organization name
3. Select the SMTP AUTH item in the list at the bottom and click the delete icon
4. Click `Delete settings`

10.1.14 Fallback servers

`Fallback servers` are used when no delivery server has been configured for a domain. They can be setup in cases where an organization has several domains whose mail is hosted on the same server so it would be repetitive to setup the same delivery server for each domain.

An Organization can have multiple `Fallback servers`.

Add a Fallback server

To add a Fallback server:

1. Click `Organizations`
2. Click the organization name
3. Click `Add Fallback 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

Update a Fallback server

1. Click `Organizations`
2. Click the organization name
3. Select the Fallback server in the list at the bottom and click the edit icon
4. Make the required changes
5. Click `Update server`

Delete a Fallback server

1. Click `Organizations`
2. Click the organization name
3. Select the Fallback server in the list at the bottom and click the delete icon
4. Click `Delete server`

10.1.15 Organization SmartHosts

`Organization SmartHosts` are used to route outbound email for domains in an organization that do not have a domain smarthost configured. This can be setup in cases where an organization has several domains whose outbound mail is routed via the same smarthost so it would be repetitive to setup the same smarthost for each domain.

An Organization can have multiple `Organization SmartHosts`.

Add a SmartHost

To add a SmartHost:

1. Click `Organizations`
2. Click the organization name
3. Click `Add SmartHost`
4. Enter server IP address or Hostname in the `Server address` field
5. Change the port in the `Port` field if your mail server does not use port 25
6. Enter a description of the SmartHost
7. Enter the `SMTP-AUTH username` and `SMTP-AUTH password` and `Retype Password` if using `SMTP-AUTH`.
8. Ensure the `Require TLS` checkbox is checked if using `SMTP-AUTH` or service uses TLS.
9. Ensure the `Enabled` checkbox is checked
10. Click the `Add SmartHost` button

Update a SmartHost

1. Click `Organizations`
2. Click the organization name
3. Select the SmartHost in the list at the bottom and click the edit icon
4. Make the required changes
5. Click `Update SmartHost`

Delete a SmartHost

1. Click `Organizations`
2. Click the organization name
3. Select the SmartHost in the list at the bottom and click the delete icon
4. Click `Delete SmartHost`

10.2 Managing Domains

Note: Domains can be managed via the API as well.

10.2.1 Adding a Domain

Domains can be added by either importing them using a YAML 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

10.2.2 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

10.2.3 Deleting a Domain

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

10.2.4 Exporting Domains

Domains can be exported to YAML, To export domains.

1. Click `Domains`
2. Click `Export Domains`
3. Click `Download the yaml file`
4. Save the YAML file to your computer

10.2.5 Domain Settings

Each domain has a range of additional settings that you can configure. These include *Delivery Servers*, *User Delivery Servers*, *SmartHosts*, *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 `Manage 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

User Delivery Servers

User Delivery servers are used to support split delivery of mail for users on a per user basis.

Multiple servers per domain are supported. The User Delivery servers are added to the domain to make them available for assignment to users within the domain.

Adding a User delivery server

1. Click `Domains`
2. Select the domain > Click the actions `Manage settings` icon
3. Click `Add User 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 User delivery server

1. Click `Domains`
2. Select the domain > Click the `Domain name`
3. Scroll to the bottom
4. Select the `User delivery server` > Click `Edit`

5. Make changes
6. Click the `Update server` button

Deleting a User delivery server

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

SmartHosts

SmartHosts are used to route outbound email via a SmartHost as opposed to routing it via the DNS based lookup of the MX record.

Multiple SmartHosts per domain are supported.

Adding a SmartHost

1. Click `Domains`
2. Select the domain > Click the actions `Manage settings` icon
3. Click `Add SmartHosts`
4. Enter server IP address or Hostname in the `Server address` field
5. Change the port in the `Port` field if your mail server does not use port 25
6. Enter a description of the SmartHost
7. Enter the `SMTP-AUTH username` and `SMTP-AUTH password` and `Retype Password` if using `SMTP-AUTH`.
8. Ensure the `Require TLS` checkbox is checked if using `SMTP-AUTH` or service uses TLS.
9. Ensure the `Enabled` checkbox is checked
10. Click the `Add SmartHost` button

Editing a SmartHost

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

Deleting a SmartHost

1. Click `Domains`
2. Select the domain > Click the `Domain name`
3. Scroll to the bottom under `SmartHosts`
4. Select the `SmartHost` > Click `Delete`
5. Click the `Delete SmartHost` button

Authentication Settings

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

Administrative accounts can not be configured to use external authentication.

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`
- `SAML2`

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

- `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 `Manage 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`, `SAML2` and `RADIUS` mechanisms require additional settings which can be added by *Adding AD/LDAP Authentication additional settings*, *Adding SAML2 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`	**Available**	**Not Available**
`%u`	**Available**	**Available**
`%d`	**Available**	**Available**
`%D`	**Available**	**Not Available**

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

Adding SAML2 Authentication additional settings

The SAML2 protocol requires the following additional settings.

- `IDP entityID` This is the SAML entityID
- `IDP Sign-in page URL` This is the SSO login end point
- `IDP Sign-out page URL` This is the SLO logout end point
- `IDP certificate` This is the IDP's certificate

To Add SAML2 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 SAML2 `Authentication server` > Click `Settings`
5. Enter the required settings
6. Click the `Save settings` button

The metadata for the domain's SP endpoint is available at the url:

`https://<baruwa-hostname>/a/metadata/<domain-name>`

You can configure your IDP to provide the following attributes which will be used to update the users local Baruwa profile.

- `urn:oid:0.9.2342.19200300.100.1.3`: Email aliases
- `urn:oid:2.5.4.4`: Surname
- `urn:oid:2.5.4.42`: Given Name

The NameID provided by the IDP should be the users email address.

The current Baruwa implementation supports the following bindings.

- `SP to IDP - HTTP Redirect Binding`
- `IDP to SP - HTTP Redirect Binding, HTTP POST Binding`

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 `Manage 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. Wikipidia

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 `Manage 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 `Manage 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 `Manage 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 `Manage 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 YAML file.

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

3. Click `Import accounts`
4. Browse for the YAML file by clicking `Browse` next to the `YAML file` field
5. Click the `Import` Button

Exporting Accounts

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

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

Rulesets

Note: Domain specific rule sets are not implemented yet.

10.2.6 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

10.2.7 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

10.3 Managing Accounts

Note: Accounts can be managed via the API as well.

10.3.1 Adding an Account

Accounts can be added by either importing them using a YAML 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

10.3.2 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

10.3.3 Deleting an Account

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

10.3.4 Exporting Accounts

Accounts can be exported to YAML, To export accounts.

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

10.3.5 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

10.3.6 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

10.3.7 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

10.3.8 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

10.3.9 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

10.3.10 Assign User Delivery Servers

Baruwa supports delivering of clean mail on a user specific basis. This means that email for some users in a domain can be delivered to a server different from the default delivery server.

To deliver a users mail to a specific server different from the default servers, you need to add `User Delivery Servers` to the users domain. The servers are then available for assignment to users.

To assign `User Delivery Servers` to a user:

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Assign User Delivery Servers`
4. Select the `User Delivery Servers`
5. Click the `Assign` button

10.3.11 Enable Two Factor Authentication

TOTP based Two Factor Authentication is supported. Any device or App that can generate TOTP tokens as well as scan QRcodes can be used. We recommend FreeOTP which is open source and developed by Redhat and available for Andriod and IOS.

To enable Two Factor Authentication for a user:

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Two Factor Authentication`
4. Click the `Show QR code` link
5. Scan the QRcode using your App
6. Check the `Enable Two Factor Authentication` checkbox
7. Click the `Update` button

10.3.12 Disable Two Factor Authentication

Disabling of Two Factor Authentication can only be performed by adminstrative users.

To disable Two Factor Authentication for a user:

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Two Factor Authentication`

4. Uncheck the `Enable Two Factor Authentication` checkbox
5. Click the `Update` button

10.3.13 Reset Two Factor Authentication

If the device used to generate TOTP tokens is lost or destroyed, the TOTP secret can be reset. This allows the user to enroll a new device. Resetting the TOTP secret can only be performed by adminstrative users.

To reset Two Factor Authentication for a user:

1. Click `Accounts`
2. Select the Account > Click the Username
3. Click `Two Factor Authentication`
4. Uncheck the `Reset OTP Secret` checkbox
5. Ensure the `Enable Two Factor Authentication` checkbox is unchecked
6. Click the `Update` button

10.3.14 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

10.3.15 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

10.4 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.

10.4.1 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.

10.4.2 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.

10.4.3 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.

10.5 Managing Settings

10.5.1 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

Note: Only add systems of `Standalone`, `Web and Mail System` and `Mail System` profile.

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. Enter the IP address `[only on clustered setups]`
5. Change the port if using different port `[only on clustered setups]`
6. Ensure the `Enabled` checkbox is checked
7. Click the `Add node` button

Update a Scanning Node

1. Click `Settings`
2. Select the Scanning Node in the list and click the edit icon
3. Make the required changes
4. Click the `Update node` button

Delete a Scanning Node

1. Click `Settings`
2. Select the Scanning Node in the list and click the delete icon
3. Click the `Delete 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

Adding an IP Address

Baruwa supports the use of Random IP addresses from an address pool as well as the assignment of dedicated IP addresses to domains, delivery servers and fallback servers. The IP addresses need to be added to the server entry in the management interface.

To add an address to a server.

1. Click `Settings`
2. Select the scanning node > Click the hostname
3. Click `Add IP Address`
4. Enter the `IP Address` in the `IP Address` field
5. Enter an Optional description
6. Ensure the `Enabled` checkbox is checked
7. Check the `External` checkbox if this address is used to deliver internet mail
8. Click the `Add IP Address` button

Updating an IP Address

To update an existing IP address.

1. Click `Settings`
2. Select the scanning node > Click the hostname
3. Select the IP address in the list and Click the `Edit IP Address` icon
4. Make the required changes
5. Click the `Update IP Address` button

Deleting an IP Address

To delete an existing IP address.

1. Click `Settings`
2. Select the scanning node > Click the hostname
3. Select the IP address in the list and Click the `Delete IP Address` icon
4. Click the `Delete IP Address` button

10.5.2 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

10.5.3 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
- TLS Enforcement List

Empty Reply Checks Exemptions List

The `Empty Reply Checks Exemptions` list is used to exempt an IP/Network address or range from Empty Reply Checks, Empty Reply checks block email messages that have an empty `Repy-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 `^\Nregexp\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/Network Addresses or range 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/Network Addresses or range 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. This list is used both inbound and outbound.

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/Network addresses or range 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/Network addresses or range 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

TLS Enforcement List

The `TLS Enforcement List` is for IP addresses and Hostnames that you require `TLS` for. `TLS` will be required for all connections, none `TLS` connections will fail.

Adding to the TLS Enforcement List

To add an entry to the list, you:

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

Updating a TLS Enforcement List entry

To edit an entry in the `TLS Enforcement` list, you:

1. Mouse over or Click `Settings`
2. Click `MTA Settings`
3. Click `TLS Enforcement 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 TLS Enforcement List

To delete an entry in the `TLS Enforcement` list, you:

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

10.5.4 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

From the list under Local Scores

1. Find the Rule in the list
2. Click the Delete icon under the Actions column
3. Click the `Delete Local Score` Button

10.6 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

10.6.1 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.

10.6.2 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`)

10.6.3 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 our the above actions can be found in the user guide's *Processing queued messages* section.

10.6.4 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.

10.7 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*

10.7.1 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                       send-top-spammer-list       update-delta-index
celerybeat                  create-admin-user           post                        ␣
↪send-pdf-reports             send-whitelist-data         update-mta-lookup
celeryd                     exe                         prune-database              ␣
↪send-pdf-reports-ng          serve                       update-queue-stats
celeryev                    help                        prune-quarantine            ␣
↪send-quarantine-reports      setup-app                   update-rulesets
change-user-password        make-config                 request                     ␣
↪send-quarantine-reports-ng   shell                       update-sa-rules
```

10.7.2 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

10.7.3 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
- `-n ORG_NAME, --organization-name=ORG_NAME` Process only this organization's accounts
- `-d DOMAIN_NAME, --domain-name=DOMAIN_NAME` Process only this domain's accounts
- `-u USER_NAME, --username=USER_NAME` Process only this username's report
- `-f, --force` Force sending of reports even if hour is not in user or domain set timezone

10.7.4 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

10.7.5 Spamassassin rule description updates

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

Updates the Spamassassin rule descriptions in the database.

10.7.6 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

10.7.7 Mail queue Stats updates

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

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

10.7.8 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.

10.7.9 Create an administrator account

```
paster create-admin-user -u USERNAME -p PASSWORD -e EMAIL -t TIMEZONE /etc/baruwa/
↪production.ini
```

Create an administrator account

10.7.10 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.

10.7.11 Generate list of top spammers

```
paster send-top-spammer-list -e EMAIL [-m -s SPAMSCORE -p REPORT_PERIOD -d] [/etc/
↪baruwa/production.ini]
```

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]

10.7.12 Generate list of clean senders

```
paster send-whitelist-data -e EMAIL [-m -s SPAMSCORE -p REPORT_PERIOD -d] [/etc/
↪baruwa/production.ini]
```

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]

10.7.13 Create Scanner rulesets

```
paster update-rulesets [/etc/baruwa/production.ini]
```

This will create or update the necessary Scanner rulesets.

10.7.14 Create MTA lookup files

```
paster update-mta-lookup [/etc/baruwa/production.ini]
```

This will create or update the MTA CDB lookup files.

10.7.15 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

10.8 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.

10.8.1 /etc/cron.d/baruwa

This contains several commands which are run at different intervals.

Interval	Command	Description
3 Minutes	paster update-queue-stats /etc/baruwa/production.ini	Updates the mail queue statistics
@ 00H00	paster update-sa-rules /etc/baruwa/production.ini	Updates the Spam rules descriptions for the web interface
Hourly	paster send-quarantine-reports /etc/baruwa/production.ini	Sends out the quarantine reports in the users timezone
@ 01H00	paster prune-database /etc/baruwa/production.ini	Archives old records to the archive table and prunes old records from the archive table
@ 02H00	paster prune-quarantine /etc/baruwa/production.ini	Deletes old quarantined messages from disk
@ 10 mins every hour on the 1st	paster send-pdf-reports /etc/baruwa/production.ini	Sends out the PDF reports in the users timezone
@ 20 mins every hour every day	paster send-pdf-reports -t domain -p daily -d 1 /etc/baruwa/production.ini	Sends out the daily PDF reports in users timezone
@ 30 mins every hour on Monday	paster send-pdf-reports -t domain -p weekly -d 7 /etc/baruwa/production.ini	Sends out the weekly PDF reports in users

10.8.2 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`

10.9 Baruwa Backups

10.9.1 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.

10.9.2 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`.

Note: The default configuration stores filesystem backups for `10` days, if your server does not have sufficient space you need to change the `keep` option to a lower value in `/etc/backup.d/20-server-fs.rdiff`

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

10.9.3 Frequency

The backups are created once a day.

10.9.4 Disabling Backups

Backups can be disabled by unchecking the `Enable Backups` checkbox on the `Management Other Settings` screen of the *baruwa-setup* utility.

10.10 Monitoring

10.10.1 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.

10.10.2 SNMP

With BaruwaOS >= `6.7.4` it is possible to monitor Baruwa Enterprise Edition systems using the SNMP protocol. To enable SNMP monitoring check the `Enable SNMP Agent` checkbox on the `Management Other Settings` screen of the *baruwa-setup* utility.

Authentication

BaruwaOS only exposes an `SNMPv3` interface. The username is `baruwa`, the password is autogenerated when the system is setup.

To obtain the password run the following command, (you need to provide the passphrase):

```
baruwa-setup -e snmp_password
```

Monitoring points

The monitoring points available are the same as the ones exposed via NRPE. The OIDs to walk are `UCD-SNMP-MIB::dskTable`, `UCD-SNMP-MIB::prTable` and `UCD-SNMP-MIB::extTable`

Firewall

The firewall port 161 inbound is open to all, you need to restrict this by allowing access only from your monitoring IP addresses.

10.11 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 is will display the logs specific to the system profile.

To use the `baruwa-logs` command simply run:

```
baruwa-logs
```

10.11.1 Nginx

- /var/log/nginx/[hostname].log

10.11.2 Uwsgi

- /var/log/uwsgi/uwsgi-baruwa.log

10.11.3 Baruwa

- /var/log/baruwa/celeryd.log
- /var/log/baruwa/what-who.log

10.11.4 MailScanner

- /var/log/maillog

10.11.5 Exim

- /var/log/exim/main.log
- /var/log/exim/reject.log

10.11.6 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

10.11.7 ClamAV

- /var/log/clamav/clamd.log
- /var/log/clamav/freshclam.log
- /var/log/clamav-unofficial-sigs/clamav-unofficial-sigs.log

10.11.8 Manticore

- /var/log/manticore/query.log
- /var/log/manticore/searchd.log

10.11.9 Pgbouncer

- /var/log/pgbouncer/pgbouncer.log

10.11.10 PostgreSQL

- /var/lib/pgsql/10/data/log/postgresql-[day].log

10.11.11 BackupNinja

- /var/log/backupninja.log

10.11.12 Syncthing

- /var/log/syncthing/syncthing.log

10.12 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

10.13 YAML Import File format

10.13.1 Organizations import

A sample of the YAML Organizations import format is provided below.

```
organizations:
- admins:
  - account_type: 2
    active: true
    addresses: []
```

```
    created_on: 2016-04-26 11:33:30.251905
    email: !!python/unicode 'tony@home.topdog-software.com'
    firstname: !!python/unicode ''
    high_score: 0.0
    last_login: 2016-04-26 11:33:30.251905
    lastname: !!python/unicode ''
    lists: []
    local: true
    low_score: 0.0
    password1: !!python/unicode ''
    password2: !!python/unicode ''
    send_report: true
    signatures: []
    spam_checks: true
    timezone: !!python/unicode 'Africa/Johannesburg'
    username: !!python/unicode 'topdog'
  domains:
  - aliases:
    - name: !!python/unicode 'mojo.com'
      status: true
    - name: !!python/unicode 'mojo2.com'
      status: true
    authservers:
    - address: !!python/unicode '192.168.1.150'
      enabled: true
      ldapsettings: []
      port: 993
      protocol: 2
      radiussettings: []
      split_address: true
      user_map_template: !!python/unicode ''
    - address: !!python/unicode '192.168.1.150'
      enabled: true
      ldapsettings:
      - basedn: !!python/unicode 'cn=users,dc=topdog-software,dc=com'
        binddn: !!python/unicode 'uid=andrew,cn=users,dc=topdog-software,dc=com'
        bindpw: !!python/unicode ''
        emailattribute: !!python/unicode 'mail'
        emailsearch_scope: !!python/unicode 'subtree'
        emailsearchfilter: !!python/unicode 'mail=%u@topdog-software,dc=com'
        nameattribute: !!python/unicode 'uid'
        search_scope: !!python/unicode 'subtree'
        searchfilter: !!python/unicode ''
        usesearch: false
        usetls: true
      port: 389
      protocol: 5
      radiussettings: []
      split_address: true
      user_map_template: !!python/unicode ''
    delivery_mode: 1
    dkimkeys: []
    high_score: 0.0
    highspam_actions: 2
    language: !!python/unicode 'en'
    ldap_callout: true
    low_score: 0.0
    message_size: !!python/unicode '0'
```

```
    name: !!python/unicode 'home.topdog-software.com'
    report_every: 3
    servers:
    - address: !!python/unicode 'build2.home.topdog-software.com'
      enabled: true
      port: 25
      protocol: 1
    signatures: []
    site_url: !!python/unicode 'https://standalone.home.topdog-software.com'
    smtp_callout: true
    spam_actions: 2
    spam_checks: true
    status: true
    timezone: !!python/unicode 'Africa/Johannesburg'
    users:
    - account_type: 3
      active: true
      addresses:
      - address: !!python/unicode 'angel+*@home.topdog-software.com'
        enabled: true
        username: !!python/unicode 'angel@home.topdog-software.com'
      created_on: 2016-04-26 11:33:28.927721
      email: !!python/unicode 'angel@home.topdog-software.com'
      firstname: null
      high_score: 0.0
      last_login: 2016-04-26 11:33:28.927721
      lastname: null
      lists: []
      local: false
      low_score: 0.0
      password1: !!python/unicode ''
      password2: !!python/unicode ''
      send_report: true
      signatures: []
      spam_checks: true
      timezone: !!python/unicode 'Africa/Johannesburg'
      username: !!python/unicode 'angel@home.topdog-software.com'
    virus_actions: 2
    virus_checks: true
    virus_checks_at_smtp: true
  name: !!python/unicode 'Asante'
  relaysettings:
  - address: !!python/unicode '192.168.3.0/24'
    description: !!python/unicode 'hosted network'
    enabled: true
    high_score: 0.0
    highspam_actions: 2
    low_score: 0.0
    password1: !!python/unicode ''
    password2: !!python/unicode ''
    ratelimit: 250
    spam_actions: 2
    username: !!python/unicode ''
- admins: []
  domains:
  - aliases: []
    authservers:
    - address: !!python/unicode 'mail.tdss.co.za'
```

```
    enabled: true
    ldapsettings: []
    port: 110
    protocol: 1
    radiussettings: []
    split_address: true
    user_map_template: !!python/unicode ''
  delivery_mode: 1
  dkimkeys:
  - enabled: false
    pri_key: !!python/unicode '-----BEGIN RSA PRIVATE KEY-----
      MIIEpQIBAAKCAQEA4yQ2oy+5XoDdO2zQtaY0m7wTVAh2GsYwOo9yrUksMLfj33bH
      Uri6JI3Z8kPaFIeP/H+a0diFWWgtfKVzhl50vqYVXtAA9GdykbhjOlzU697Tqg6Z
      7/StEsJ5r5GRxwxCeEydfgmVzG+dbYangpHy2QkBQwSqOvFX3a3VZyUpUNTq+n7V
      jo/PZ2hWxL/tPiV82g0rqj4VPB95vBicENIA6g9+pEOZLnG2QcdP6hWED/Dd5nQr
      GDKKjAdX0SyXDrfgcfSoVOCIO4jWxdv2Nq/Q49DsV30PTB4hmLN4VyAdZNJJB5m0
      Y91IcJ66F2ftYClVoPCObF2KPNEeOufoQ7DAfwIDAQABAoIBAQDdbSAWVR/QEK+a
      jqmnay894kq1UMpRr4K0k8KnSv3ZQGrUHWaSLaLIn8AnfB3MhZrH+11h1EGqtvQg
      3umPw+TrNdz/YKaNm4sEo0uYSYcHqWGOFk3arhtKfmtBzBbghAMIYyflBlMRyH0f
      mHUTxFOJYE3ql1GbxEpzwFKZCpEMSa26Ho602kkEHe22rdfLkDOHtS9AERcwllGt
      GTHrETlUoV1WL2fOnoxx7T+qL5LfFVXZGipllSzpf1L0RK5uo7bsmOvOUF7x6yxY
      z8pM8hNlHW0MKyKei3oG0fWNg/FxXKxk7ursQOtbucjeSaVu76WfEf5vLWbncfql
      7kzrAGWBAoGBAPdh3aIrhBM+zm6lcHsFTw+Pc7vYIG5jZcId03r7j3itBdWYacne
      suj2dpS5gFY5gkOn4OVkzIA0LMasE2Jd1POfGOeiLp6KZxwHp4f8cuLlBmNDPl6n
      q2+F3hf5dPGMDVHo4yvWvpe74D2d6jM8bBFWuQxpNH5mXR1yF1kx09QdAoGBAOsN
      13fov3M0j/ZFy6M669gSFOOWGv57MhxjkFY3CNBG7qlFwdcDTFE8Ncw2vZTfDebM
      9+oV4GurukTF3HsSph/bEL1mOXT/oO9c9ksbaiCddy5SZqMDBWoAk95Iy0uwc0ud
      CGe+wmb9jhAoH2c1SSQswkGz/5r7FvfG62kT/UxLAoGBAIiMtbkBSisRXQNIQLk3
      KffN2DVUzDoClbW7nvNgjkYvQ2wucB5k1d6vxK69YjC2F8hej04wAI23vwt/Ckge
      wSAkrquVIySSAu4+72OpnoTNpGQARxoadQ/fFcOoB7wY8XVIFrUpGRVKODHqy86y
      SHidpRFLtRUcTcOmKWsrjOClAoGAH4BAYyqHFdpyfK/H5b1MxC1QLVv9jCNYiONz
      AYronHkVHQxjOPyRKsXl89NWPvBRvZ+0jeOWqvddxD+8F6ZdKyHBsZBUnPBxUgLk
      YxZud6aCxWt3o9sQy67+IikhTah9GyIVcUnoZcMPWez2oG9MuRNiiUmlNND3uAcp
      n3B1XtcCgYEA8gzfmLw4Zv6DWcJeXYlx6J65ns9BnPeIC3+tGbtksavV4zuge/f+
      GMcfUtt+zOtvDwqQd2AgpweaHCZX2goD7+3AvzMn8gQn113jHTSFlbCUhvfmwCBO
      WxrSXE4RHaMTDlce6e6J1h8j8esdjPDdaK6wuv6s+AnibEaY8xZCiRA=
      -----END RSA PRIVATE KEY-----
      '
    pub_key: !!python/unicode '-----BEGIN PUBLIC KEY-----
      MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4yQ2oy+5XoDdO2zQtaY0
      m7wTVAh2GsYwOo9yrUksMLfj33bHUri6JI3Z8kPaFIeP/H+a0diFWWgtfKVzhl50
      vqYVXtAA9GdykbhjOlzU697Tqg6Z7/StEsJ5r5GRxwxCeEydfgmVzG+dbYangpHy
      2QkBQwSqOvFX3a3VZyUpUNTq+n7Vjo/PZ2hWxL/tPiV82g0rqj4VPB95vBicENIA
      6g9+pEOZLnG2QcdP6hWED/Dd5nQrGDKKjAdX0SyXDrfgcfSoVOCIO4jWxdv2Nq/Q
      49DsV30PTB4hmLN4VyAdZNJJB5m0Y91IcJ66F2ftYClVoPCObF2KPNEeOufoQ7DA
      fwIDAQAB
      -----END PUBLIC KEY-----
      '
  high_score: 0.0
  highspam_actions: 2
  language: !!python/unicode 'en'
  ldap_callout: true
  low_score: 0.0
  message_size: !!python/unicode '0'
  name: !!python/unicode 'baruwa.com'
  report_every: 3
  servers:
  - address: !!python/unicode '192.168.1.150'
```

```
      enabled: true
      port: 25
      protocol: 1
    signatures: []
    site_url: !!python/unicode 'https://standalone.home.topdog-software.com'
    smtp_callout: true
    spam_actions: 2
    spam_checks: true
    status: true
    timezone: !!python/unicode 'Africa/Abidjan'
    users: []
    virus_actions: 2
    virus_checks: true
    virus_checks_at_smtp: true
  name: !!python/unicode 'Baruwa'
  relaysettings: []
```

10.13.2 Domains import

A sample of the YAML Domains import format is provided below.

```
domains:
- aliases:
  - name: !!python/unicode 'mojo.com'
    status: true
  - name: !!python/unicode 'mojo2.com'
    status: true
  authservers:
  - address: !!python/unicode '192.168.1.150'
    enabled: true
    ldapsettings: []
    port: 993
    protocol: 2
    radiussettings: []
    split_address: true
    user_map_template: !!python/unicode ''
  - address: !!python/unicode '192.168.1.150'
    enabled: true
    ldapsettings:
    - basedn: !!python/unicode 'cn=users,dc=topdog-software,dc=com'
      binddn: !!python/unicode 'uid=andrew,cn=users,dc=topdog-software,dc=com'
      bindpw: !!python/unicode ''
      emailattribute: !!python/unicode 'mail'
      emailsearch_scope: !!python/unicode 'subtree'
      emailsearchfilter: !!python/unicode 'mail=%u@topdog-software,dc=com'
      nameattribute: !!python/unicode 'uid'
      search_scope: !!python/unicode 'subtree'
      searchfilter: !!python/unicode ''
      usesearch: false
      usetls: true
    port: 389
    protocol: 5
    radiussettings: []
    split_address: true
    user_map_template: !!python/unicode ''
  delivery_mode: 1
```

```
  dkimkeys: []
  high_score: 0.0
  highspam_actions: 2
  language: !!python/unicode 'en'
  ldap_callout: false
  low_score: 0.0
  message_size: !!python/unicode '0'
  name: !!python/unicode 'home.topdog-software.com'
  report_every: 3
  servers:
  - address: !!python/unicode 'build2.home.topdog-software.com'
    enabled: true
    port: 25
    protocol: 1
  signatures: []
  site_url: !!python/unicode 'https://standalone.home.topdog-software.com'
  smtp_callout: true
  spam_actions: 2
  spam_checks: true
  status: true
  timezone: !!python/unicode 'Africa/Johannesburg'
  users:
  - account_type: 3
    active: true
    addresses:
    - address: !!python/unicode 'angel+*@home.topdog-software.com'
      enabled: true
      username: !!python/unicode 'angel@home.topdog-software.com'
    created_on: 2016-04-29 16:49:33.315026
    email: !!python/unicode 'angel@home.topdog-software.com'
    firstname: null
    high_score: 0.0
    last_login: 2016-04-29 17:18:45.828066
    lastname: null
    lists: []
    local: false
    low_score: 0.0
    password1: !!python/unicode ''
    password2: !!python/unicode ''
    send_report: true
    signatures: []
    spam_checks: true
    timezone: !!python/unicode 'Africa/Johannesburg'
    username: !!python/unicode 'angel@home.topdog-software.com'
  virus_actions: 2
  virus_checks: true
  virus_checks_at_smtp: true
- aliases: []
  authservers:
  - address: !!python/unicode 'mail.tdss.co.za'
    enabled: true
    ldapsettings: []
    port: 110
    protocol: 1
    radiussettings: []
    split_address: true
    user_map_template: !!python/unicode ''
  delivery_mode: 1
```

```
  dkimkeys: []
  high_score: 0.0
  highspam_actions: 2
  language: !!python/unicode 'en'
  ldap_callout: false
  low_score: 0.0
  message_size: !!python/unicode '0'
  name: !!python/unicode 'baruwa.com'
  report_every: 3
  servers:
  - address: !!python/unicode '192.168.1.150'
    enabled: true
    port: 25
    protocol: 1
  signatures: []
  site_url: !!python/unicode 'https://standalone.home.topdog-software.com'
  smtp_callout: true
  spam_actions: 2
  spam_checks: true
  status: true
  timezone: !!python/unicode 'Africa/Abidjan'
  users: []
  virus_actions: 2
  virus_checks: false
  virus_checks_at_smtp: true
```

10.13.3 Accounts import

A sample of the YAML Accounts import format is provided below.

```
accounts:
- account_type: 1
  active: true
  addresses: []
  created_on: 2016-04-29 15:09:02.621265
  email: !!python/unicode 'andrew@home.topdog-software.com'
  firstname: null
  high_score: 0.0
  last_login: 2016-04-29 19:19:18.352069
  lastname: null
  lists: []
  local: true
  low_score: 0.0
  password1: !!python/unicode ''
  password2: !!python/unicode ''
  send_report: true
  signatures: []
  spam_checks: true
  timezone: !!python/unicode 'Africa/Johannesburg'
  username: !!python/unicode 'andrew'
- account_type: 3
  active: true
  addresses:
  - address: !!python/unicode 'angel+*@home.topdog-software.com'
    enabled: true
    username: !!python/unicode 'angel@home.topdog-software.com'
```

```
  created_on: 2016-04-29 16:49:33.315026
  email: !!python/unicode 'angel@home.topdog-software.com'
  firstname: null
  high_score: 0.0
  last_login: 2016-04-29 17:18:45.828066
  lastname: null
  lists: []
  local: false
  low_score: 0.0
  password1: !!python/unicode ''
  password2: !!python/unicode ''
  send_report: true
  signatures: []
  spam_checks: true
  timezone: !!python/unicode 'Africa/Johannesburg'
  username: !!python/unicode 'angel@home.topdog-software.com'
- account_type: 2
  active: true
  addresses: []
  created_on: 2016-04-29 16:49:37.133774
  email: !!python/unicode 'tony@home.topdog-software.com'
  firstname: !!python/unicode ''
  high_score: 0.0
  last_login: 2016-04-29 17:17:37.023041
  lastname: !!python/unicode ''
  lists: []
  local: true
  low_score: 0.0
  password1: !!python/unicode ''
  password2: !!python/unicode ''
  send_report: true
  signatures: []
  spam_checks: true
  timezone: !!python/unicode 'Africa/Johannesburg'
  username: !!python/unicode 'topdog'
```

10.14 Man Pages

10.14.1 baruwa-setup

Baruwa Enterprise Edition management tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-setup [options]

DESCRIPTION

`baruwa-setup` is a utility program used to manage Baruwa Enterprise Edition servers. It simplifies the management of systems by collecting configuration information, performing configuration changes, storing configuration information, performing system updates and other system management tasks.

On the first ran a passphrase is set, this passphrase is used to encrypt the system configuration data that is collected. Ensure you set a strong passphrase and do not loose this passphrase as it is not possible to recover this passphrase.

All system updates and upgrades should be done using the baruwa-setup command. Do `NOT` use the `yum` command to perform upgrades as that will leave your system in an unconfigured inconsistent state.

OPTIONS

-b ENGINE, --config-engine=ENGINE Sets the configuration engine to use, only SaltStack supported at the moment

-p PUPPET_FILE, --puppet-manifest=PUPPET_FILE Sets the Puppet Manifest file to load settings from for migration

-s, --skip-questions Skip questions, Only install updates and configure the system

-c, --configure Skip questions and updates, Only configure system

-e, --export-manifest Export the configuration settings to a SaltStack SLS settings

-r, --reset-passphrase Reset the baruwa-setup passphrase

-g, --regenerate-passwords Regenerate the autogenerated system credentials

-v, --version Prints the version number and exits.

-h, --help Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-import`
- `man 8 puppet2salt`

10.14.2 paster

Baruwa Enterprise Edition house keeping tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

paster [paster_options] COMMAND [command_options]

DESCRIPTION

Custom paster commands provided to enable scripting of house keeping tasks such as quarantine cleanup, Database maintenance, configuration updates etc.

OPTIONS

-v, --version	Prints the version number and exits.
-h, --help	Prints a usage message and exits.

Commands

`camqadm` CAMQP Admin

`celerybeat` Start the celery beat server

`celeryd` Start the celery worker

`celeryev` Celery event command.

`change-user-password` Change a user's password

`check-user-password` Check a user's password

`create-admin-user` Create an administrator account

`dump-mta-lookup-file` Display the contents MTA cdb lookup files

`prune-database` archives, then deletes old records, and trims archive

`prune-quarantine` cleans the quarantine directory

`send-pdf-reports` Send summary PDF reports

`send-quarantine-reports` Send quarantine reports

`send-top-spammer-list` Generates a list of top spammers and emails it

`send-whitelist-data` Generates a list of top ham senders for whitelisting

`update-delta-index` Update the Delta and RT indexes[messages, archive]

`update-mta-lookup` Generates cdb lookup files for the MTA

`update-queue-stats` Read the items in the queue and populate DB

`update-rulesets` Generates file based Scanner rulesets

`update-sa-rules` Update the Spamassassin rule descriptions

SEE ALSO

- `man 8 baruwa-setup`
- `man 8 updatedelta.pl`

10.14.3 baruwa-backup2db.pl

Restores logs from the backup databases

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-backup2db.pl [options]

DESCRIPTION

baruwa-backup2db.pl restores logs from the backup databases into the main Baruwa database

OPTIONS

--cleanup, -c	Cleanup old records from the backup DB.
--version, -V	Show this program's version number and exit.
--delete, -d	Delete problem records from the backup DB.
--help, -h	Show this help message and exit.

SEE ALSO

```
man 8 paster
```

10.14.4 baruwa-dmarcexpire

DMARC history data expiration tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-dmarcexpire [options]

DESCRIPTION

baruwa-dmarcexpire expires old records from the database that is part of the Baruwa DMARC aggregate reporting feature.

OPTIONS

--alltables	Expire records in all tables rather than only the large ones.
--config=config	Indicates the config file to read settings from defaults to /etc/baruwa/dmarc-reports.ini
--expire=days	Indicates the number of days of data to keep. The default is 30
--verbose	Requests verbose output.
--version	Prints version number and exits.
--help, -h	Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-dmarcimport`
- `man 8 baruwa-dmarcreports`

10.14.5 baruwa-dmarcimport

DMARC aggregate report data import tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-dmarcimport [options]

DESCRIPTION

baruwa-dmarcimport reads per-message data recorded Baruwa and stores it, for later use by `baruwa-dmarcreports(8)` to generate aggregate reports.

OPTIONS

--config=config	Indicates the config file to read settings from defaults to /etc/baruwa/dmarc-reports.ini
--verbose	Requests verbose output.
--version	Prints version number and exits.
--help, -h	Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-dmarcexpire`
- `man 8 baruwa-dmarcreports`

10.14.6 baruwa-dmarcreports

DMARC aggregate report generation tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-dmarcreports [options]

DESCRIPTION

baruwa-dmarcreports generates periodic DMARC aggregate reports.

OPTIONS

--config=config	Indicates the config file to read settings from defaults to /etc/baruwa/dmarc-reports.ini
--day	Generate reports on day boundaries. Overrides the value of –interval
--domain=name	Generates a report (if one is due) for the named domain, rather than checking all of them
--interval=secs	Generates reports only for hosts that have not had a report generated in at least the last 86400 seconds
--keepfiles	Keep xml files (in local directory)
-n	Synonym for –test

--nodomain=name	Skips generating a report for the named domain. Can be specified multiple times to skip multiple reporting domains.
--noupdate	Suppresses marking the time of the transmission of the report in the database.
--test	Don't send reports
--utc	Instructs the database to change to the UTC timezone.
--verbose	Increase the amount of verbosity written to standard output.
--version	Prints version number and exits.
--help, -h	Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-dmarcexpire`
- `man 8 baruwa-dmarcimport`

10.14.7 updatedelta.pl

Update search index delta indexes

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

updatedelta.pl [index] [realtime]

DESCRIPTION

updatedelta.pl updates Baruwa search index delta indexes

OPTIONS

-i, --index	Specifies the index name
-r, --realtime	Indicates this is a realtime index
-c, --config	Specifies the configuration file to use defaults to /etc/baruwa/updatedelta.ini
-h, --help	Prints a usage message and exits.

SEE ALSO

`man 8 paster`

10.14.8 baruwa-import

Baruwa Enterprise Edition settings recovery tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

baruwa-import [options]

DESCRIPTION

`baruwa-import` is a utility program used to reads configuration settings from system files and generates output in the `baruwa-setup` SaltStack SLS format.

It can be used to recover some settings in cases where the `baruwa-setup` passphrase has been lost.

OPTIONS

-v, --version	Prints the version number and exits.
-h, --help	Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-setup`
- `man 8 puppet2salt`

10.14.9 puppet2salt

Baruwa Enterprise Edition settings conversion tool

Author Andrew Colin Kissa andrew@topdog.za.net

Date 2016-05-17

Version 2.1.3

Manual section 8

Manual group System Administration Utilities

SYNOPSIS

puppet2salt [options]

DESCRIPTION

`puppet2salt` is a utility program used to convert a Baruwa puppet manifest settings file to the Baruwa salt settings file format.

OPTIONS

-p PUPPET_FILE, --puppet-manifest=PUPPET_FILE	Sets the location of the Puppet Manifest file to convert
-v, --version	Prints the version number and exits.
-h, --help	Prints a usage message and exits.

SEE ALSO

- `man 8 baruwa-setup`
- `man 8 baruwa-import`

10.15 Frequently Asked Questions

10.15.1 General Faqs

Answers to many common general questions.

Do i need a Back End subscription ?

If you intend on running a single server using the *Standalone System* you do not need a Back End Subscription.

Back End Subscriptions are only required for Back End servers which are used in a clustered setup.

What is a Front End server ?

A front end server is one that is installed using any of the following profiles

- *Standalone System*
- *Web and Mail System*
- *Mail System*
- *Web Interface System*

What is a Back End server ?

A back end server is one that is installed using any of the following profiles

- *Backend System*
- *Search Index System*
- *Database System*
- *Message Queue System*
- *Cache System*

Do i need a PAID subscription for back end servers ?

Answer: `Yes`

From BaruwaOS version 6.7.4 subscriptions for back end systems are now paid subscriptions, Free subscriptions are no longer available.

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.

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.

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.

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.

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.

Do you support other payment methods apart from PayPal ?

Answer: `Yes`

We support the PayFast subscription system for users you do not have PayPal. PayFast payments are processed in South African Rands `ZAR`.

South African business users should use the PayFast subscription system to make payments in South African Rands `ZAR`.

Why do you require a PayPal/PayFast account for the 30 day Trial ?

The requirement of a PayPal/PayFast account is simply to prevent abuse as users just keep resigning for trials to keep their install working without purchasing a subscription.

The subscription system is automated and linked to the PayPal/PayFast IPN system so we are unable to provide out of band trials requests.

How many trial subscriptions can i request ?

We will only issue a maximum of 2 Frontend and 4 backend subscriptions.

Who qualifies for trial subscriptions ?

Only new users without existing licenses qualify for trial subscriptions.

Users with existing or previous licenses should purchase full subscriptions.

I would like to resale Baruwa Enterprise Edition subscriptions

Please contact us to request access to our reseller program.

Do you have an online demo system ?

No, you can setup a demo system on one of the supported cloud providers if you would like to experience the features. Check *Cloud Installation* for details.

Does the solution support DANE, DMARC, SPF, DKIM, etc ?

Most email related features and protocols are supported, please check the full *Feature List*

10.15.2 Technical Faqs

Answers to many common technical questions.

How do i request a new feature ?

Answer: `Use the issue tracker`

Open a feature request on the issue tracker

How do i report a non security bug ?

Answer: `Use the issue tracker`

Open a bug report on the issue tracker

How do i report a security bug ?

Answer: `Email security@baruwa.com`

If you think you've found a security vulnerability with Baruwa, please send a message to security@baruwa.com. Do NOT post a bug report to our issue tracking system or disclose the issue on our mailing lists.

How do i tailor Baruwa Enterprise Edition to my specific needs ?

Refer to the *Customization* section.

Can i manage Baruwa Enterprise Edition servers without using baruwa-setup ?

Answer: `Yes`

Yes you can, you can choose to do the configuration manually or using a configuration management too. SaltStack can be used easily as we provide salt states which are used by baruwa-setup in the background. You could also convert this states to a different configuration management tool.

How do i rebrand Baruwa Enterprise Edition servers ?

Refer to the *Themes* section, note that if you would like to remove the powered by notices you need to purchase a branding license.

What happens if i remove/hide/obscure the copyright notices without a license ?

That is a violation of the terms and we will revoke your subscription without a refund of any sums paid.

Why can i download rpm or deb packages to install on my system ?

We no longer provide packages, the solution is now packaged as a custom OS.

What are the settings i should use to configure LDAP/AD ?

The short answer is if you are asking, you probably should not be using LDAP/AD as you could inadvertently open yourself up to security holes.

The long answer is all LDAP directories are not setup in the same way, so there is no one size fits all configuration we can provide.

It is advisable you create an account with very limited privileges in the directory to use for the LDAP operations and bind as that account.

The following are common configurations that you could attempt.

Setting	Description	Active Directory	OpenLDAP
Base DN	The location within the directory to start searching	dc=domain,dc=com	dc=domain,dc=com
Username Attribute	The directory attribute in which the username is stored	samAccountName, userPrincipalName	uid
Email attribute	The directory attribute in which the email address is stored	mail	mail
Bind DN	The DN to bind as to perform operations	cn=Administrator,cn=users,dc=domain,dc=com, Administrator@domain.com	cn=root,dc=domain,dc=com
Bind password	The password for the Bind DN		
Use TLS	Use the STARTTLS option		
Search for userDN	Search for the userDN to bind to	Yes in most cases	No in most cases
Email Search Filter	The filter used to locate email addresses in an entry	(|(proxyAddresses=SMTP:%u@%d) (proxyAddress=smtp:%u@%d)(mail=%u@%d))	mail=%u@%d

Which MTA does Baruwa Enterprise use ?

Answer: `Exim`

Baruwa Enterprise uses a customized version of the Exim MTA

SMTP AUTH on port 25 no longer works, why ?

SMTP AUTH is no longer offered on port 25 starting with BaruwaOS 6.7.4. The reason for this is documented in the release notes at *SMTP Authentication*

How do i add a default delivery server ?

In Baruwa default delivery servers are called Fallback servers and they can be added to an Organization. Any domain in the Organization which does not have a delivery server configured will use the Fallback servers configured for that organization.

Refer to *Fallback servers* for more info.

How do i uninstall Baruwa Enterprise Edition ?

Baruwa Enterprise Edition is an operating system not an application, to remove it from your computer system you need to reformat the hard drive and install a different operating system.

How do i remove Baruwa ?

Refer to *How do i uninstall Baruwa Enterprise Edition ?*

My messages match ClamAV signature Heuristics.OLE2.ContainsMacros, how do i allow them through ?

The message contains an attachment that contains macros and you have configured the system to block documents with macros. You need to turn of the `Block Macros` option in `baruwa-setup`.

Baruwa is rejecting messages at SMTP time but i would like the messages available in the interface

To prevent messages from being rejected at SMTP time, you need to turn off the `Enable SMTP Time Rejection` option in `baruwa-setup`.

I want all messages logged regardless of status, what do i do ?

You need to turn off the `Enable SMTP Time Rejection` option in `baruwa-setup`.

How do i enable remote technical support access ?

We use SSH Keys to access your system, need to install our ssh key below to the `authorized_keys` file of the account you want us to access. We require access to accounts with `root` privileges either as `root` directly or via an account with `sudo` access to `root`.

You can restrict access on your firewall to our remote support system: `support.baruwa.com` (`84.200.48.209`)

SSH KEY

```
# == start key
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC86+4YcvrDXdBFkrxtQnNGNXJ8ccqcbecs//qw8B/
↪ltwLvLL0VXeS0m1dimlzw4gXz4U4q+ZxFBzMPJgje5JnFFa75PaYDTwJ/ZQeE/
↪j85uEVJB4WFXFbqMbFUBYFP13y3HLVQ/eaX+OdPnRlyJU03pwgPo9kSnaO4x7aJyM9WiFLSQW/
↪WB6n7nJtHqLXAqYrpjLL3ivR9icr04Zmql6+wU3fWRAWr4Mu4UcKh5ko4SsZk+DzbhSUnQ8IuCzOU39j3tx2Xbvm0rRCYZjje0
↪fbN87CFdC1UWyxExVSgiKJJu8Fmmp95QJGRfb+dmBGLcfsakaBvPtE2IE50uiMpb/
↪iziTYr9hhJuXtnn8lJFlNGlxDurjvKj6BZ/wbmupYe4mkMt/JJFzgD9ZLsM1/ph66a8u1U0pz1cd/
↪tZUsMrjQ5E5cKd4VPX+9DMgZugzXU0HA0CrsAm4eU7ukNbhA3u1MR12NYO4v+ytS/
↪VtWWMBninlHABlE5A34E0FSUU9lNdSAG9k7diiX096m4WOPtahTec9QML7AZ7CXVA0FlRSEbMREiUFKEPpb5YP0owAkAsdmFKCr
↪pcdi4GjgudLxN8QRiqKUQ== enterprise-support@support.baruwa.com
# == end key
```

10.16 Release Notes

10.16.1 BaruwaOS 6.10

New Features

Upstream Release

This release tracks the upstream base OS's update 6.10. The release notes for the upstream OS can be found at on the upstreams website

Depreciations

None

Known Issues

None

10.16.2 BaruwaOS 6.9.1

New Features

PostgreSQL upgrade

The PostgreSQL database has been updated to 10.1 which is the latest version, improves performance and has lots of features not available in the previous versions.

`baruwa-setup` will automatically migrate your database from 8.4.20 to 10.1, although this process has been tested you may run into issues. Make sure you schedule changes with your change management process and create a large upgrade window. If possible ensure you make the changes during the time window in which technical support is guaranteed to be available.

Backend Clustering

For many users clustering of backend systems to eliminate single points of failure has been one of the most requested features. It is now possible to cluster backend systems thus eliminating the single point of failure in a Baruwa cluster.

Fail over between the active master to slaves is automated for database systems user intervention is not required.

Read and write operations are automatically split, read operations are sent to the slave servers while write operations are sent to the master.

To maintain a quoram and prevent split brain issues cluster components must be deployed in odd numbers. This is specifically important for systems in the backend segment. Do not deploy a backend cluster segment that has even number of components.

Memcached does not support clustering so it is now an optional component. If you are currently using Memcached but would like transparent cluster fail over support you need to disable Memcached and use the built in uwsgi caching system.

With backend segment clustering enabled, the cluster is now resilient to backend failures. The web interfaces can now remain operational in event of a backend failure.

It is also possible now to perform upgrades on backend systems without affecting the end users.

For efficient operation your backend components should be located at different locations such that an outage does not take down all the systems at the same time. If the systems are at the same location and an outage takes down all the systems then recovery of such a cluster is a more involved process.

For more info refer to *Clustering*

TLS encryption

TLS encryption for backend services is now mandatory, the *Backend Traffic Encryption* options have been depreciated. All services with external interfaces within the cluster now run over TLS.

To support this the builtin CA has been enhanced and automated. New cluster members now request certificates from the bootstrap server during the setup process.

Certificates are issued from intermediate CA's for various components. To support the verification process the root CA certificate needs to be copied to the non bootstrap servers in the cluster prior to configuration.

For more info refer to *Root CA Key*

Search Improvements

Instant search results have been extended to cover all the search functions in the web interface, in previous versions instant search only covered the messages search function. For all other search functions the indexing was delayed. So if you added a domain for example you would not be able to search for it immediatly. If is now possible to obtain the results immediatly after adding the domain.

The search indexing operation has further been optimised to use less RAM and CPU. In previous versions search indexing used up lots of system resources and crushed often. This release addresses many of those issues.

User Delivery Servers

We have added support for `User Delivery Servers`, using this feature it is now possible to deliver mail for different users in a domain to different servers.

`User Delivery Servers` are added to a domain, and can then be assigned to user accounts in that domain.

Multiple `User Delivery Servers` can be added to a domain as well as assigned to a user.

For more info refer to *User Delivery Servers*

SmartHosts

We have added support for `SmartHosts`, using this feature it is now possible to route outbound mail for a domain or an organization via an upstream smarthost.

This feature is useful for customers who want to send out mail via an external server that performs branding for example or archiving.

At the moment `IP Address` and `SMTP AUTH` based routing is supported. For `SMTP AUTH` the `CRAM-MD5` and `PLAIN` mechanisms are supported over TLS.

For more info refer to *SmartHosts* and *Organization SmartHosts*.

SAML2 external authentication support

Support has been added for the SAML2 external authentication method. Domains can now be configured to use SAML2 external authentication.

Due to the way in which this protocol works, it is not possible to login from the main login page. A special url has been created which you will need to provide your users with the url takes the following format:

`https://baruwa.example.com/a/login/domain`

So if your baruwa url is `baruwa.example.com` and the SAML2 enabled domain is `example.net` then the url to use will be:

`https://baruwa.example.com/a/login/example.net`

The metadata for any domains you configure for SAML2 external authentication will be available at:

`https://baruwa.example.com/a/metadata/domain`

As is with the above `example.net` domain the metadata url will be:

`https://baruwa.example.com/a/metadata/example.net`

This is a technology preview so please test before putting into full scale production.

TOTP Two Factor OTP authentication support

TOTP based Two Factor Authentication is supported. Any device or App that can generate TOTP tokens as well as scan QRcodes can be used. We recommend FreeOTP which is open source and developed by Redhat and available for Andriod and IOS.

Avast Anti Virus Engine support

The Avast Anti Virus Engine is now supported and can be configured as an SMTP Time or POST SMTP Time Anti Virus Engine. Avast AV requires a subscription, which you can purchase from us.

Support for blank email addresses in lists manager

It is now possible to enter a blank from address in the lists manager, this allows users to manage list entries for senders that set a blank <> address such as auto responders, bounce messages, etc.

Support for disabling search

Indexed search is resource intensive, in some setups it is not worth the expense deploying extra resources to manage search. It is now possible to disable indexed search. Users can then use filters to find the messages they need.

An option has been added to `baruwa-setup` to allow for enabling and disabling of the search functionality.

Modular external authentication

External authentication is now modular meaning that you can install only the external authentication methods that you require and use. For example if you do not use LDAP you can disable that module.

On upgrade all external authentication modules will be disabled make sure that you enable the ones that you use in `baruwa-setup`.

Scanner RAM disk support

The mail scanning component now supports the use of a RAM disk. This can be used on systems where disk access is slow and causing a bottleneck. This option requires 1GB of dedicated RAM to operate correctly.

To enable use of the RAM disk, enable that in `baruwa-setup`.

Optimization of MTA configuration

The MTA dynamic configuration system has been optimized by consolidating the settings in to fewer files. This improves system performance by keeping less files open at any time.

Simplified Configuration

The number of configuration screens in clustered systems has been reduced. Most of the configuration options have been moved to the backend systems. For most options you only need to set them once on the bootstrap server. The other members of the cluster then pull these cluster wide configurations from the bootstrap server.

This is improves on the previous configuration where you needed to re-enter the same settings on several servers.

Due to the above changes, when upgrading you need to check the settings on your frontend systems and add those settings to your bootstrap server before running the updates on the frontend systems.

Improved Archive filtering

Filtering of archive contents has been improved. More archive types are now supported including 7zip based archives.

Depreciations

External Authentication

External authentication is now modular, all modules are disabled by default on upgrade. You need to explicitly enable the modules that you want to use.

Encrypt all backend traffic

The `Encrypt all backend traffic` option has been depreciated as backend encryption is now mandatory.

Memcached

Memcached is now an optional component. It was previously a mandatory component on `mail` profile systems, this is no longer the case.

Known Issues

Template changes

If you are using a custom template and do not update your templates you will ran into issues, ensure that you update your templates on upgrade.

Simplified Configuration

Make sure that you copy the configuration settings from existing frontend systems to your bootstrap server prior to updating the frontend systems.

You can get the settings from your frontend system by running the `baruwa-setup -e` command

MTA configuration overide for SMTP Time scanning changes

The MTA configuration overide for SMTP Time scanning have changed, please read the documentation and update your custom overides.

Firewall rules overwrite

On some system profiles especially the clustered ones, the firewal rules will be overwritten. If you have custom rules you need to readd them after the upgrade

The CA file /etc/pki/BaruwaCA/certs/BaruwaCA.pem is missing

You need to copy that file over from your bootstap server.

Disk space

Please ensure you have sufficient free space on your system before starting with the upgrade. On database and backend systems you need to have 3 times the size of /var/lib/pgsql available.

WebApp Error: <class 'socket.gaierror'>: [Errno -2] Name or service

This means that localhost4 is not configured as an entry for 127.0.0.1 in /etc/hosts. You need to modify that and add an entry for localhost4

no quorum: only 1 vote(s) for Legion baruwacluster, 2 needed to elect a Lord

Refer to the solution for *digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c* below.

digital envelope routines:EVP_DecryptFinal_ex:bad decrypt:evp_enc.c

If you have the above error in your logs then it means the autogenerated session key on the backend in a cluster contains unwanted characters.

A manual fix to the database is required. Follow the following steps on the backend server or database server.

1. Generate a 35 character random string as follows:

```
mkpasswd -l 35 -s 0
```

2. Connect to your baruwa-setup database:

```
sqlcipher /var/lib/baruwa-setup/baruwasetup.db
```

3. Enter the following commands at the `sqlite>` prompt. Replace `_pp_` with your actual passphrase, `_rand_string_` with string from step 1:

```
PRAGMA KEY="_pp_";
UPDATE baruwasetup SET session_secret="_rand_string_";
.quit
```

4. Run the baruwa-setup command on your backend server and repeat on your nodes.

10.16.3 BaruwaOS 6.9

New Features

Upstream Release

This release tracks the upstream base OS's update 6.9. The release notes for the upstream OS can be found at on the upstreams website

Support for disabling SMTP TIME rejections

Some users prefer to accept all messages regardless of the Virus infection status and Spam characteristics and quarantine the messages to allow them to be accessed via the web interface.

We have added the `Enable SMTP Time Rejection` option to `baruwa-setup` to allow enabling and disabling rejection of messages at SMTP Time.

The recommended approach is to reject most messages at SMTP Time.

Support for disabling the DANE protocol

An option has been added to `baruwa-setup` to allow for the enabling and disabling the builtin DANE protocol support.

Improved Local Scores management

The management of spam rule local scores has been improved, it is now possible to set spam rule local scores to 0.0. It is also now possible to delete local scores.

Improved Sophos Integration

The more efficient `SAVDI` and `SOPHIE` integration option is now available for After SMTP time Anti-Virus scanning using `Sophos Antivirus for Linux`.

To enable POST SMTP Time Scanning, select the `Sophos SAVID` under virus checks in the MailScanner settings section of the interface.

Improved F-Prot Integration

It is now possible to perform SMTP time Anti-Virus scanning using `F-Prot`.

This option is documented at *F-PROT*

We implemented this using the `FSCAND` protocol and submitted the patch to the upstream. Our contribution was accepted and will be part of Exim 4.90. We have back ported the patch to Exim 4.89 for use in BaruwaOS.

Improved NTP Syncronization

This release has integrated the Chrony daemon to manage the network time sync function on the system. This replaces the cron driven ntpdate system we had in place. Chrony has several advantages over the traditional ntpd system shipped by default on most systems.

Improved Anti-Virus Signature updates

This release implements updates of custom ClamAV Anti-Virus signatures using the built in freshclam system using `DatabaseCustomURL` options that point to our mirror network.

Due to the above changes the `clamav-unofficial-sigs` package is thus depreciated and removed.

Improved Queue Monitoring support

With the introduction of the queuefile transport there are potentially 3 queues in Baruwa.

- `MTA queue`
- `Inbound queue`
- `Outbound queue`

It is now possible to view the status of all the queues in the web interface. The `MTA queue` and `Inbound queue` are combined in the inbound queue view in the web interface.

It is also possible to monitor all the above queues both via NRPE and via SNMP.

The monitoring points configured for NRPE are the following.

- `MTA queue` - exim_queue
- `Inbound queue` - exim_scan_queue
- `Outbound queue` - exim_outbound_queue

To enable monitoring of the MTA queues including the queuefile transport queue we built a brand new nrpe plugin called `check_exim_queue` and packaged as `nagios-plugins-check-exim-queue`.

Under SNMP the queues are available as

- `MTA queue` - inboundq
- `Inbound queue` - scanq
- `Outbound queue` - outboundq

Improved Rate Limiting

In the previous versions it was not possible to rate limit hosts within CIDR networks, this version fixes that issue. Rate limiting will work correctly for relay hosts that are within a CIDR network configured for outbound relay.

Improved Brute Force Protection

MTA brute force SMTP password cracking protection has been furthe enhanced in this version to catch various tricks used by cracking software.

A new `baruwa-unblock.sh` command has been implemented for use in unblocking hosts and users that have been blocked by brute force protection and MTA reputation management.

The email generated when a sender has been blocked now includes instructions on how to use the `baruwa-unblock.sh` command to unblock the sender.

Depreciations

ntpdate removed

With the implementation of Chrony the `ntpdate` package has been depreciated and removed.

clamav-unofficial-sigs removed

Custom ClamAV signature updates are now handled by the built in freshclam system, the `clamav-unofficial-sigs` package is thus depreciated and removed.

Known Issues

ERROR with rpm_check_debug vs depsolve:', 'bind-libs = 32:9.8.2-0.47.rc1.el6_8.4 is needed by (installed) bind-32:9.8.2-0.47.rc1.el6_8.4.x86_64'

If you get the above error when running *baruwa-setup* then run the following commands before running *baruwa-setup* again:

```
yum erase bind -y
sed -i -e 's/nameserver 127.0.0.1/nameserver 8.8.8.8/' /etc/resolv.conf
```

Mail log entries containing 'utf8 support required but not offered for forwarding'

If some messages are not being delivered an the logs contain the above error run the following commands:

```
echo "smtputf8_advertise_hosts =" >> /etc/exim/custom-vars.post
service mailscanner restart
```

10.16.4 BaruwaOS 6.8.1

New Features

Queuefile Transport support

BaruwaOS now uses the queuefile transport to queue messages for scanning.

IDNA support

BaruwaOS now supports IDNA. Internationalized domain names can now be configured on the system and translation is automatically handled. Most functions in the web interface that use domain names and host names now have IDNA support.

This feature is still a technology preview so may be rough around the edges.

MTA improvements

The MTA has added support for the following as technology previews.

- CHUNKING ESMTP
- PRDR
- SMTPUTF8
- DANE

DANE protocol support

BaruwaOS now supports the DANE protocol both in client and server mode. This feature is still a technology preview so may be rough around the edges.

To better support `DNSSEC` on BaruwaOS, the `Bind` DNS caching server has been replaced with the `Unbound` caching server. Forward zones configured for the `Bind` server will automatically be migrated by the `baruwa-setup` command.

Improved outbound relaying

This version improves upon the outbound relaying functionality within BaruwaOS.

The following issues have been fixed.

- SPF checking on outbound messages fails
- DNSBL checks run on outbound connections authenticated via SMTP-AUTH
- IPv6 Addresses not working when configured as relay clients.

Starting with this version, servers relaying through Baruwa will no longer trigger SPF failures.

Starting with this version, users connecting via SMTP-AUTH will not have their IP addresses checked on DNSBL's, this will allow for users from SOHO with dynamic network addresses to relay mail via Baruwa servers.

IPv6 relay clients will now be able to relay via Baruwa servers.

Improved IPv6 support

Note: **NOTE:** Accepting of external mail via IPv6 addresses is discouraged as our data feeds do not yet adequetly track IPv6 spam sources.

The handling of IPv6 addresses has been further enhanced in this version.

It is now possible to add IPv6 addresses to the Approved and Banned sender lists.

It is also possible to configure IPv6 addresses as relay clients.

It is now possible to proxy IPv6 connections to Baruwa servers.

Various bugs related to handling of IPv6 addresses were fixed in this update.

Blocking of Macros

`baruwa-setup` now has an option to enable the blocking of messages that contain macros. Messages containing documents with macros will be blocked by the ClamAV engine. The signature that will be matched is `Heuristics.OLE2.ContainsMacros`.

Improved Sophos Integration

The more efficient `SAVDI` and `SOPHIE` integration option is now available for SMTP time Anti-Virus scanning using `Sophos Antivirus for Linux`. This option is documented at *Sophos SAVID*

Depreciations

Bind

The `Bind` DNS caching server has been replaced by the `Unbound` DNS caching server.

This means the way forward zones are configured has changed. Forward zones now need to be configured based on the `Unbound` format.

Existing zones added to the previous `Bind` server will be automatically migrated to `Unbound` format by the `baruwa-setup` tool.

New zones can be added to `/etc/unbound/conf.d/local.conf`. Please refer to the `Unbound` documentation for in depth information.

SMTP Sender Callback verification

The use of SMTP callbacks to verify the existense of email accounts when the senders reverse DNS record does not exist has now been depreciated.

Scanner Spam Lists

The use of Scanner `Spam Lists (Settings > MailScanner Settings > Spam Checks > Spam List)` is depreciated. Please do not enable those entries. If you have them enabled, please deselect them.

This option will be removed in the next release.

Scanner Spam Domain Lists

The use of Scanner `Spam Domain Lists (Settings > MailScanner Settings > Spam Checks > Spam Domain List)` is depreciated. Please do not enable those entries. If you have them enabled, please deselect them.

This option will be removed in the next release.

Known Issues

Queue Changes

Due to the switch to the queuefile transport mail received before or during the upgrade may not be processed. In order to ensure that no mail is left unprocessed or lost, messages need to be copied from the old queue into the new queue.

This is a manual process and can be done using the process below:

```
service mailscanner stop
mv -vf /var/spool/exim.in/input/* /var/spool/exim.in/baruwa/input/
service mailscanner start
```

The messages should now be processed correctly.

OLE2BlockMacros: Pattern not found

If you encounter that error then ran:

```
mv /etc/clamd.conf.rpmnew /etc/clamd.conf
```

If that does not resolve the issue, then find the line `OLE2BlockMacros` in `/etc/clamd.conf` and comment it out.

Out of memory Errors

The upgrade process may crush on virtual systems with less than 6GB of RAM. Please ensure that you have >= 6GB of RAM prior to upgrading your system.

10.16.5 BaruwaOS 6.8

New Features

Upstream Release

This release tracks the upstream base OS's update 6.8. The release notes for the upstream OS can be found at on the upstreams website

ACME TLS Certificates

Baruwa now supports the ACME client protocol. This allows for requesting of certificates from ACME compartible Certificate Authorities such as CertBot formerly known as Lets Encrypt a free and open CA which issues browser recognized certificates.

Baruwa will now request Certbot certificates for the HTTPS and SMTP TLS services if you do not have a CA issued certificate. Certbot certificates are supported by a wide range of browsers so you should no longer have the warnings generated when using the Baruwa CA auto generated certificates.

The system checks to ensure that it will be possible to validate the requests by checking that the hostnames resolve to a Public IP address that is assigned to the system. If the check fails then Certbot certificates will not be requested and the local CA certificates will be issued.

In some cases, the public IP address is not assigned to the system and traffic is port forwarded to the Baruwa system. In those cases the automatic detection will fail. As a work around you need to create a check file on the system this tells *baruwa-setup* to bypass the checks and request the certificates anyway.

To create the check file run the following command:

```
touch /etc/baruwa/acme.enable
```

To disable the use of Certbot certificates you can create a disable check file:

```
touch /etc/baruwa/acme.disable
```

For the validation process to succeed, it should be possible for external systems to connect to your system on port 80. The Certbot validation system makes a connection to the hostname(s) specified in the certificate request to verify that you control the hostname before issuing the certificates.

The CertBot CA does not support issuing certificates to IP addresses so the certificates that are issued will not contain your IP addresses as alternative names as is the case with Baruwa CA issued certificates.

CertBot CA issued certificates are valid for only 90 days at a time, On a Baruwa system a scheduled process runs to check and update the certificate before it expires. The scheduled process runs every 3 days and will renew the certificate if is <= 5 days from expiry.

DMARC Reporting

Baruwa now supports DMARC reporting, both forensic and aggregate reports are supported.

Forensic reports are sent out immediatly when the mail is processed, Aggregate reports are sent out once a day.

DMARC reporting can be enabled using *baruwa-setup*

Fallback servers

It is now possible to configure delivery servers for an Organization, these delivery servers are called Fallback servers.

If a domain in the Organization does not have delivery servers configured the Fallback servers for the Organization will be used instead.

This can be used in cases where an Organization has several domains which are hosted on the same mail server.

For more info refer to *Fallback servers*

MTA Random IP Address Pools

Baruwa now supports the use of a random IP address from a pool of IP addresses. To use a random IP address from a pool of IP addresses, you need to:

- Configure the IP addresses as virtual or physical interfaces on the Baruwa server(s).
- Add the IP addresses in the web interface under the Server to which the address is assigned via *Adding an IP Address*

Baruwa will automatically use one random IP address from the assigned addresses each time it makes an outbound SMTP connection.

The above is useful to be able to remove and add IP addresses to the system when an address has been blacklisted for example.

To assign specific IP addresses to specific customer domains you can use the *Dedicated IP Addresses* feature.

Dedicated IP Addresses

Baruwa now supports the setting of dedicated IP addresses for:

- Domains
- Delivery servers
- Fallback servers

So it is now possible to assign dedicated IP addresses to a domain, delivery server and fallback server.

The effect of the above assignments is as follows:

- All email from the domain name will be sent from the assigned IP address
- All email to a delivery server will be sent from the assigned IP address
- All email to a fallback server will be sent using the assigned IP address

The above comes in handy when you want to seperate traffic flows in a multi customer hosted enviroment such that one customers reputation does not affect other customers reputation.

To use this feature:

- Configure the IP addresses as virtual or physical interfaces on the Baruwa server(s).
- Add the IP addresses in the web interface under the Server to which the address is assigned via *Adding an IP Address*
- Assign the IP address to either the domain, delivery server or fallback server.

Null routing

It is now possible to discard all mail sent to a domain without delivering it to the delivery servers.

An option has been added to allow users to discard all mail addressed to the domain.

Enforcing TLS

It is now possible to enforce the use of TLS connections for hosts and domains.

Domains hosted on the Baruwa server can now be configured to only deliver mail to the delivery servers using TLS connections by setting the `Require TLS` on the delivery or fallback servers.

SMTP clients sending Outbound mail via the Baruwa server are already required to use TLS for SMTP AUTH connections, now it is also possible to enforce the use of TLS for none SMTP AUTH connections using the `Require TLS` on the relay settings.

For inbound messages it is also possible to enforce TLS using the *TLS Enforcement List*

Content Protection Info

The reasons why a message was blocked by the Content Protection System are now displayed on the message detail page.

After SMTP Anti Virus Rejection Info

The rejection messages from the After SMTP Anti Virus checks are now displayed on the message detail page.

API

The API has been extended to support Fallback servers and Null routing.

Man Pages

BaruwaOS now includes *Man Pages* for all the Baruwa Enterprise Edition commands.

Depreciations

None

Known Issues

ERROR with rpm_check_debug vs depsolve:', 'libselinux = 2.0.94-5.8.el6 is needed by (installed) libselinux-ruby-2.0.94-5.8.el6.x86_64'

If you get the above error when running *baruwa-setup* then run the following commands before running *baruwa-setup* again:

```
yum install baruwa-setup -y
yum erase libselinux-ruby -y
```

Salt Engine reported error(s) Processing state cmd.run[mailscanner-create-cdb] failed => Command "paster update-mta-lookup /etc/baruwa/production.ini"

If you get the above error when running *baruwa-setup* then run the following command before running *baruwa-setup* again:

```
paster setup-app /etc/baruwa/production.ini
```

Salt Engine reported error(s) Processing state augeas.change[mailscanner-config-dmarc-reports.ini] failed => Error: Unable to save to file

If you get the above error when running *baruwa-setup* then logout of the current session and log back in before running *baruwa-setup* again

Salt Engine reported error(s) Processing state baruwa_certs.present[acme-request-certificate] failed => Failed to issue certificate

The above error means baruwa-setup was unable to issue the Lets encrypt certificate for your server. Please review the *ACME TLS Certificates* section if you want to use Lets encrypt certificates. If you do not want to use Lets encrypt certificate, run the following command before running *baruwa-setup* again:

```
touch /etc/baruwa/acme.disable
```

Salt Engine reported error(s)

If you get the above error when running *baruwa-setup* run *baruwa-setup* again

10.16.6 BaruwaOS 6.7.4

New Features

Backend Systems subscriptions

Beginning with BaruwaOS `6.7.4` backend systems will require a `PAID` subscription. Existing systems installed prior to `6.7.4` being released are exempt from this requirement.

Simplified Configuration

The configuration on `Standalone` profiles has been simplified, there are fewer screens and most of the credentials are now generated automatically.

This will reduce the human factor errors and improve security as strong credentials are now generated automatically.

The *baruwa-setup* utility now includes an option to refresh the system credentials that are automatically generated. To regenerate credentials run *baruwa-setup* with the `-g` option.

Built in Cache

A new built in caching mechanism has been added that allows for replacement of the current memcached solution.

The built in cache is the default cache on new `Standalone` installations and can also be used on the `Web and Mail System` and the `Web Interface System` profiles.

In a clustered setup port 11211 needs to be allowed inbound to the system, this port is used by the nodes in a cluster to replicate cache data.

The memcached cache can still be used, the `Enable Memcache` option on the `Management Other Settings` screen of the *baruwa-setup* utility can be used to enable or disable memcached.

This option is important for enviroments where memcached errors are frequent.

Cluster Master

A loose cluster master system has been introduced, nodes in a cluster can now elect a leader node.

The leader node is the node that performs tasks that must only be carried out by one system with in the cluster at a time like sending of reports or cleaning up the quarantine.

The cluster traffic used to elect the leader node is sent on port 3542, this port needs to be allowed on firewalls between the nodes in both directions.

The cluster leader elections only take place on `Web and Mail System` nodes.

The other systems use a distributed locking system to ensure that tasks are executed by only one server in a cluster.

YAML Imports

The data import system has been overhauled. The previous system was unable to import all the data required to setup fully functional systems.

The new system uses the YAML format to import organizations, relay settings, domain administrators, domains, domain aliases, delivery servers, authentication servers and user accounts.

It is also possible to import just domains or accounts into an existing organization or domain respectively.

The old system that used CSV files has been removed.

YAML Exports

The data export system has been overhauled. The previous system was unable to export all the setup data.

The new system exports data in the YAML format and includes almost all the configuration data on the system.

Organizations can be exported and will include all the data within the organization which includes relay settings, domain administrators, domains, domain aliases, delivery servers, authentication servers, lists, signatures, dkim settings and user accounts.

It is also possible to export domains and accounts with the data contained in those containers.

Passwords are not part of the data export. The password entries will be blank in any export.

The old system that exported data to CSV files has been removed.

Cron System

On `Standalone` and `Web and Mail System` profiles, scheduled tasks are now run using the uWSGI system not the traditional cron system.

This integrates with the *Cluster Master* system to ensure that tasks are run by only one node in a cluster.

Baruwa Service

On `Standalone` and `Web and Mail System` profiles backend tasks are now run using the uWSGI system, the standalone Baruwa service is no longer required or installed.

On `Mail System` profiles which do not run the uWSGI system a baruwa-service package is installed this provides the standalone Baruwa service.

Backend Traffic Encryption

It is now possible to encrypt all traffic between backend and front end nodes and between the backend nodes themselves.

The `Encrypt all backend traffic` option works by installing a TLS tunneling service which will encrypt connections from the source and decrypt them at the destination for the specific application streams.

The `Encrypt all backend traffic` option can also be used on LAN to thwart capturing of data by sniffing of packets on a LAN.

Authentication

The authentication of certificates takes place using certificate pinning, this means you have to copy the servers certificate to the client.

On the server side the certificate file contains both the private key and the certificate do NOT copy the whole file to the client only copy the certificate, to extract the certificate run the following command on the server.:

```
openssl x509 -in /etc/pki/baruwa/certs/$(hostname).pem
```

On the client side the certificates need to be stored in `/etc/pki/baruwa/certs/_IPADDRESS_.pem` where `_IPADDRESS_` is the IP address of the server configured in the *baruwa-setup* utility

The `Encrypt all backend traffic` option must be configured on all systems in the cluster both front end and backend for the cluster to function correctly.

SMTP TLS Ciphers

Previously only strong ciphers were allowed on all SMTP connections, to allow for increased interoperability with other systems this has been changed to normal ciphers on port `25`.

Please refer to *SMTP Authentication* for the impact of this change.

Additional Anti Virus Engines

This release supports more additional Anti Virus Engines in addition to the built in ClamAV engine. The supported engines are documented in the *Additional Anti Virus Engines* section.

SNMP Monitoring

SNMP monitoring is now supported. It is documented in the *SNMP* section.

HTTP Proxy Protocol Support

The HTTP service now supports the Proxy Protocol, meaning Baruwa web services can now be placed behind load balancers that support the Proxy Protocol such as HAProxy and Amazon ELB. The proxy protocol makes the actual client IP address visible to the Baruwa service instead of having all requests appear like they came from the load balancer.

The SMTP service already supports the Proxy Protocol.

HTTP Log to Syslog

The HTTP service now supports the option to log to syslog. Using syslog the logs can be aggregated and processed.

The SMTP service already supports logging to syslog.

API

Added support for get domain by name

Network Ports

The following additional ports are now used.

PORT	PROTOCOL	DIRECTION	DESCRIPTION
11211	UDP	BETWEEN NODES	CACHE SYNC TRAFFIC
3542	UDP	BETWEEN NODES	CLUSTER TRAFFIC
161	UDP	INBOUND	SNMP

Depreciations

SMTP Authentication

SMTP Authentication on port `25` is no longer supported due to the *SMTP TLS Ciphers* change. SMTP AUTH is now only offered on ports `465` and `587` which still require strong ciphers.

Relay settings configurations that use port `25` will need to be updated.

Puppet

The Puppet configuration management system has been removed from BaruwaOS. The only supported configuration engine is now Salt.

It is still possible to import puppet manifests as part of the upgrade.

Memcached

On `Standalone` profiles memcached has been depreciated, the *Built in Cache* system is now the default.

DKIM

Messages that fail DKIM checks will no longer be blocked at SMTP time.

Imports

Importing of domains and accounts from CSV files is no longer supported. The CSV system has been replaced by the *YAML Imports* system.

Exports

Exporting of domains and accounts to CSV files is no longer supported. The CSV system has been replaced by the *YAML Exports* system.

Known Issues

ERROR: Pidfile (/var/run/baruwa/celeryd/celeryd.pid) already exists.

If you see the above error in you logs run the following command:

```
kill `cat /var/run/baruwa/celeryd/celeryd.pid`
rm -vf /var/run/baruwa/celeryd/celeryd.pid
```

Service clamd is already enabled, and is dead

If you get the above error when running *baruwa-setup* then run the following command before running *baruwa-setup* again:

```
freshclam
```

failed to open DB file /var/spool/exim.in/db/retry: Permission denied (euid=93 egid=93)

If you see the above error in you logs run the following command:

```
chown exim.exim /var/spool/exim.in/db/retry
```

10.17 Upgrading

10.17.1 2.1.8

- Enhancement

- Bug fix

Backward compatibility

None

New dependencies

None

Template changes

None

Upgrading

Review the release notes for *BaruwaOS 6.10* and changelog for versions *2.1.8*, the upgrade notes for *2.1.8* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

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.

Backup your baruwa-setup database

Backup your baruwa-setup database by running the following command:

```
cp -a /var/lib/baruwa-setup/baruwasetup.db /var/lib/baruwa-setup/baruwasetup.db.orig
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.2 2.1.7

- Enhancement
- Bug fix

Backward compatibility

Template changes introduce a compatibility issue.

New dependencies

None

Template changes

- baruwa/templates/accounts/account.html
- baruwa/templates/accounts/assignuserdestinations.html
- baruwa/templates/accounts/searchresults.html
- baruwa/templates/domains/adddestination.html
- baruwa/templates/domains/addsmarthost.html
- baruwa/templates/domains/deletedestination.html
- baruwa/templates/domains/deletesmarthost.html
- baruwa/templates/domains/detail.html
- baruwa/templates/domains/editdestination.html
- baruwa/templates/domains/editsmarthost.html
- baruwa/templates/domains/testdestination.html
- baruwa/templates/organizations/addsmarthost.html
- baruwa/templates/organizations/deletesmarthost.html
- baruwa/templates/organizations/detail.html
- baruwa/templates/organizations/editsmarthost.html
- baruwa/templates/settings/domain_settings.html

Upgrading

Review the release notes for *BaruwaOS 6.9.1* and changelog for versions *2.1.7* and *2.1.6*, the upgrade notes for *2.1.6* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

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.

Backup your baruwa-setup database

Backup your baruwa-setup database by running the following command:

```
cp -a /var/lib/baruwa-setup/baruwasetup.db /var/lib/baruwa-setup/baruwasetup.db.orig
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.3 2.1.6

- Enhancement
- Bug fix

Backward compatibility

Template changes introduce a compatibility issue.

New dependencies

None

Template changes

- accounts/account.html
- accounts/index.html
- accounts/login.html
- domains/detail.html

- domains/index.html
- general/error.html
- lists/index.html
- mailscanner/senders.include
- messages/archive.html
- messages/index.html
- messages/listing.html
- messages/quarantine.html
- organizations/index.html
- saml/metadata.xml
- saml2/errors.html
- saml2/init.html
- saml2/loggedout.html
- saml2/metadata/idp.xml
- saml2/metadata/sp.xml
- status/audit.html
- twofactor/2fa.html

Upgrading

Review the release notes for BaruwaOS *BaruwaOS 6.9.1* and changelog for version *2.1.6* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

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.

Backup your baruwa-setup database

Backup your baruwa-setup database by running the following command:

```
cp -a /var/lib/baruwa-setup/baruwasetup.db /var/lib/baruwa-setup/baruwasetup.db.orig
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.4 2.1.5

- Enhancement
- Bug fix

Backward compatibility

None

New dependencies

None

Template changes

- mailscanner/virus.checks.rules
- domains/detail.html
- settings/localscores.html
- settings/localscores_delete.html
- settings/localscores_searchresults.html

Upgrading

Review the release notes for BaruwaOS *BaruwaOS 6.9* and changelog for version *2.1.5* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum install baruwa-setup -y
```

Backup your baruwa-setup database

Backup your baruwa-setup database by running the following command:

```
cp -a /var/lib/baruwa-setup/baruwasetup.db /var/lib/baruwa-setup/baruwasetup.db.orig
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.5 2.1.4

- Enhancement
- Bug fix

Backward compatibility

New dependencies

None

Template changes

The following template files have been changed.

- mailscanner/senders.include
- settings/policy_rules.html
- domains/detail.html

Upgrading

Review the release notes for BaruwaOS *BaruwaOS 6.8.1* and changelog for version *2.1.4* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

Memory Requirements

The minimum memory requirements have changed, if your system is virtual and has less that 6GB of RAM you need to upgrade that to >= 6GB of RAM prior to upgrading. Please note the upgrade process could crash if you to not follow the above recommendation.

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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum install baruwa-setup -y
```

Backup your baruwa-setup database

Backup your baruwa-setup database by running the following command:

```
cp -a /var/lib/baruwa-setup/baruwasetup.db /var/lib/baruwa-setup/baruwasetup.db.orig
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

Migrate messages to new queue

To copy messages from the old queue into the new queue run the following:

```
service mailscanner stop
mv -vf /var/spool/exim.in/input/* /var/spool/exim.in/baruwa/input/
service mailscanner start
```

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.

10.17.6 2.1.3

- Enhancement
- Bug fix

Backward compatibility

New dependencies

None

Template changes

The following template files have been changed.

- forms/base.html
- domains/detail.html
- info/smtp-codes.html
- messages/detail.html
- messages/functions.html
- settings/index.html
- settings/addserver.html
- settings/editserver.html
- settings/deleteserver.html
- settings/showserver.html
- settings/addipaddress.html
- settings/editipaddress.html
- settings/deleteipaddress.html
- organizations/add.html
- organizations/detail.html
- organizations/adddestination.html
- organizations/editdestination.html
- organizations/deletedestination.html

Upgrading

Review the release notes for BaruwaOS *BaruwaOS 6.8* and changelog for version *2.1.3* and read the updated documentation before you proceed with the upgrade.

If you are on versions < 2.0.7, you need to purchase hands on support for a manual upgrade contact support to do so.

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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum install baruwa-setup -y
```

Remove the libselinux-ruby rpm

You need to uninstall the libselinux-ruby rpm:

```
yum erase libselinux-ruby -y
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.7 2.1.2

- Enhancement
- Bug fix

Backward compatibility

New dependencies

None

Template changes

The following template files have been changed.

- static/500.html
- accounts/exportstatus.html
- accounts/importstatus.html
- domains/exportstatus.html
- organizations/exportstatus.html
- organizations/importorgs.html
- organizations/importorgsstatus.html
- organizations/index.html
- organizations/exportstatus.html
- organizations/importorgs.html
- organizations/importorgsstatus.html

Upgrading

Review the release notes for BaruwaOS *BaruwaOS 6.7.4* and changelog for version *2.1.2* 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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum upgrade baruwa-setup -y
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.8 2.1.1

- Enhancement
- Bug fix

Backward compatibility

New dependencies

None

New configuration options

- `baruwa.system_type` - Sets the system type

Template changes

Upgrading

Review the changelog for version *2.1.1* 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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum upgrade baruwa-setup -y
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.9 2.1.0

- Enhancement
- Bug fix

Backward compatibility

New dependencies

- pysyncthing
- python-spamc

New configuration options

- `baruwa.ipaddress` - Sets the hosts ip address.
- `baruwa.sync.apikey` - Sets the sync API key, only used in clusters which shared quarantine

Template changes

The following template files have been changed.

- status/serverstatus.html
- settings/addserver.html
- settings/editserver.html

- settings/localscores.html
- settings/localscores_searchresults.html

Upgrading

Review the changelog for version *2.1.0* 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.

Upgrade the baruwa-setup tool

To ensure you have the latest baruwa-setup tool run the following command:

```
yum upgrade baruwa-setup -y
```

Run setup utility

To perform the upgrade you run the baruwa-setup command as follows:

```
baruwa-setup
```

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.

10.17.10 2.0.10

- Enhancement
- Bug fix

Backward compatibility

New dependencies

- python-ipaddr
- python-maxminddb

- libmaxminddb

New configuration options

None

Template changes

None

Upgrading

Review the changelog for version *2.0.10* 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
```

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.

10.17.11 2.0.9

- Enhancement
- Bug fix

Backward compatibility

New dependencies

None

New configuration options

None

Template changes

The following template files have been changed.

- base.html
- accounts/login.html
- info/smtp-codes.html
- general/error.html
- messages/quarantine.html

Upgrading

Review the changelog for version *2.0.9* 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
```

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.

10.17.12 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.

10.17.13 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

Passwords file

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.

baruwa-setup fails with sa-compile error

If you get the following error when running `baruwa-setup`:

```
Salt Engine reported error(s),
Processing state:
Cmd.run(spamassassin-initial-sa-compile)
failed => command "sa-compile" run
```

Run the following command:

```
mv -vf /etc/MailScanner/spam.assassin.prefs.conf.rpmnew /etc/MailScanner/spam.
↪assassin.prefs.conf
```

Then run `baruwa-setup` again:

```
baruwa-setup -p /usr/local/src/$(hostname).pp
```

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 >= 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.

10.17.14 Old Versions

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
```

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).pp.orig
/etc/puppet/bin/update-puppet-config.pl -oldconfig /etc/puppet/manifests/toasters/
↪baruwa/$(hostname).pp.orig \
-newconfig /etc/puppet/manifests/toasters/baruwa/init.pp > /etc/puppet/manifests/
↪toasters/baruwa/$(hostname).pp
puppet -v /etc/puppet/manifests/toasters/baruwa/$(hostname).pp
service mailscanner restart
service uwsgi restart
service baruwa restart
```

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
```

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
```

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.

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.

10.18 Changelogs

10.18.1 2.1.8

- FEATURE: Implemented get domain alias by name in API
- FEATURE: Implemented support for indexing of IDNA addresses
- FIX: Accessing spam quarantine generates error
- FIX: Deleting a user generates an error
- FIX: Allow deleting list items of domains that have been removed
- FIX: Display correct error in quarantine reports cmd
- FIX: Exception sending cmdline quarantine rpts

- FIX: Internal close invalidates the full session
- FIX: celery task update_queue_stats fails
- FIX: Catch integerity error in dbclean
- FIX: Exception in domain aliases API
- FIX: local variable pheader referenced before assignment
- FIX: Close open redirect in /accounts/loggedout
- FIX: Add locking to sa rules updates
- FIX: Conversion exception in lists module
- FIX: Generate user reports before admin reports
- FIX: Deletion of org smarthosts failed
- FIX: Unbound session error when deleting an alias
- FIX: Key error when accessing login.action path
- FIX: InvalidCodepoint when displaying IDNA encoded user parts

10.18.2 2.1.7

- FEATURE: Added support clustering backend systems
- FEATURE: Added support for User Delivery Servers
- FEATURE: Added support for SmartHosts
- FEATURE: Added support for system wide instant search
- FEATURE: Added Database based distributed locking
- FEATURE: Added Scanner RAM disk support
- FEATURE: Added TLS support for all cluster servers
- FEATURE: Improvements to MTA cdb files
- FEATURE: PostgreSQL updated to version 10.1
- FIX: Remove old kernels
- FIX: Optimization of dbclean
- FIX: Optimization of DB queries
- FIX: Catch keyerror on missing LDAP mail attrib
- FIX: Improvements to search indexing system resource usage
- FIX: Generation of subject block list fails if unicode chars used

10.18.3 2.1.6

- FEATURE: Allow disabling of the search index
- FEATURE: Modular external authentication
- FEATURE: SAML2 external authentication Support
- FEATURE: TOTP OATH Two Factor One time Password support

- FEATURE: Improve quarantine reporting
- FEATURE: Improvements to dedicated IP support
- FEATURE: Added support for the Avast Anti Virus Engine
- FEATURE: Added support for blank email addresses in lists manager
- FIX: Added index on messageid of messagestatus
- FIX: Run paster prune-quarantine on all nodes
- FIX: log baruwa-check.sh errors instead of stderr
- FIX: Exception on updating delivery server via API
- FIX: Disable freshclam warnings
- FIX: Catch exception in test destination
- FIX: Make the baruwa-check-bs.sh command more roburst
- FIX: Remove Heuristics.OLE2.ContainsMacros from defaults
- FIX: Gracefully catch invalid email addresses
- FIX: Exception generated when using regex filters
- FIX: Prevent creation of users with forbidden chars

10.18.4 2.1.5

- FEATURE: Added support for after SMTP virus scanning using the Sophos SAVID daemon and the sophie protocol.
- FEATURE: Allow setting of local scores to 0.0
- FEATURE: Support for disabling the DANE protocol
- FEATURE: Support for disabling SMTP TIME rejections
- FEATURE: Added baruwa-check-bs command to monitor BSQL
- FEATURE: Add baruwa-unblock.sh command to unblock abusive senders
- FIX: Sort search results
- FIX: Recover from crushed database prune issue
- FIX: InvalidCodepoint error on mangled usernames
- FIX: Searching for email addresses under lists fails
- FIX: Deleting list entries created by domain admins fails
- FIX: IndexError exception in baruwa.lib.db on domains list
- FIX: Ensure baruwa-custom.cf.local contains only IP addresses
- FIX: Alias Addresses being incorrectly removed
- FIX: Support RAW UTF8 names in the CDB databases
- FIX: Testing destination server fails with exception
- FIX: Indexer crashes when merging indexes
- FIX: Template exception when paging policies

- FIX: Incorrect moderniser js asset link
- FIX: Improve context help messages
- FIX: Make string handling more roburst
- FIX: From address not displayed in IE
- FIX: Use windowed queries in dbclean
- FIX: Strip newline from rules loaded from file
- FIX: Prune old records from indexer_killlist table
- FIX: Ensure disabling Virus Checks for a domain works
- FIX: Add signature creation to paster update-rulesets
- FIX: Add creation of rulesets to paster update-rulesets
- FIX: Mask encoding errors in baruwa-backup2db.pl and BaruwaSQL
- FIX: Add flushing to ensure subsequent queries pickup the changes
- FIX: Improvements to queue checks, support the pre-queuefile queue
- FIX: Ensure ruleset changes are written to db before file generation

10.18.5 2.1.4

- Perform connection check from the actual mail-node, fixes issue #104
- Implemented windowed delete queries for messages and archive
- Added delete flag to baruwa-backup2db.pl, fixes issue #110
- Added Heuristics.OLE2.ContainsMacros to default list of spam-virii
- Use named queue to process queuefile messages
- UI improvements for selecting items in lists
- Improved IPv6 support for lists, MTA settings and relays, fixes issue #108
- Added functionality to prune old audit logs
- Improved updatedelta indexing script
- Depreciate spam lists and spam domain lists
- Display the email rule description not the log description in content protection
- FIX: Integrety error when deleting users with API settings
- FIX: Use lower case comparisons for email addresses
- FIX: Ensure node hostnames are lowercase
- FIX: Log user out if they delete their own account
- FIX: Redirect user to the home page on update or deletion of account
- FIX: Update attributes on LDAP/AD accounts, fixes issue #105
- FIX: Crashes when merging delta indexes
- FIX: Optimise updating of SA rules
- FIX: Compact IPv6 addresses in the configurations

- FIX: Queue stats not updated when msglog missing
- FIX: Decode hostname for queue items SQL insert
- FIX: Exception when deleting a fallback server
- FIX: Reason for queuing was showing undetermined
- FIX: SA warnings in prune-quarantine paster command
- FIX: ambiguous format strings in the lists module
- FIX: Rear exception in the settings module
- FIX: Immediatly clean up spam in baruwa-backup2db.pl when msg is flagged as spam
- FIX: non unicode warnings in multiple modules
- FIX: Deletion of account fails if reset token exists
- FIX: Missing cronjobs in the web profile
- FIX: SAWarning on ruleset text filters
- FIX: Ensure cache config is purgable
- FIX: API deletes do not work, fixes issue #109
- FIX: Use of uninitialized value $answer errors in baruwa-dmarcreports
- FIX: Texts different when editing domain fixes issue #97
- FIX: Support IPv6 Addresses in quarantine sync, fixes issue #89
- FIX: TypeError exception comparing datetimes
- FIX: Allow export of large audit logs
- FIX: CSV data export regression
- FIX: Sqlalchemy depreciation errors
- FIX: Invalid netblock error when ipv6 address is checked against ipv6 range, fixes issue #102
- FIX: dmarc-expire fails to expire due to database constraint
- FIX: Regression in importing domains due to dedicated ip addresses
- FIX: Silence baruwa-dmarcreports warnings
- FIX: Incorrect cronjob installed
- FIX: Regression in sending quarantine reports
- FIX: Rare exception in updating rulesets
- Implemented IDNA support
- FIX: Use correct events API
- FIX: Typos and defaults in the settings form

10.18.6 2.1.3

- Implemented Null routing, Fixes #78
- Implemented Fallback routing
- Implemented Random IP Address Pool support

- Implemented Dedicated IP Address support
- Added support for generating and sending DMARC reports, Fixes #77
- Added Content policy blocked information, Fixes #76
- Added option to specify hosts requiring TLS/SSL, Fixes #79
- Added man pages for commands
- Refactored to allow for mounting scanner spool directory to a RAMdisk
- Updated translations
- Updated Documentation
- FIX: SPF exemptions not working
- FIX: Cache full issue when using uWSGI cache
- FIX: Prevent changing of admin username
- FIX: Improvements to the scanner init script
- FIX: PDF reports and email messages not translated
- FIX: Updating existing domains via the API generates an error
- FIX: Remove AWL table cleanup from dbclean
- FIX: Prevent users entering invalid data into the lists manager
- FIX: Use Unix socket for indexer connection when encrypt all backend traffic is set

10.18.7 2.1.2

- Improved templating performance
- Updated DNSBLs on the info page
- Added SNMP monitoring support
- Added support for the Sophos AV
- Added support for disabling backups
- Added support for the new syncthing address format
- Reimplemented the import and export system to use YAML
- Added support for TLS encryption of all backend traffic
- Added support for get domain by name to API, Fixes #72
- Added support for additional scanner POST SMTP scanning
- Added support for builtin high speed cache as a replacement for Memcached
- Updated Documentation
- FIX: Hostname custom themes not working
- FIX: Could not delete Relay Setting. Form returned "Password is WAY too short" error
- FIX: Generate AV settings when changed in interface
- FIX: CDB files not being updated. This occured when an organization was deleted along with all its domains.
- FIX: Rare key exception in relayed via template

- FIX: Incorrect link in local scores search results
- FIX: Exception generated when duplicate mta settings are added
- FIX: Exception generated when logged user changes username
- FIX: Branding issue in info page
- FIX: Correctly route the update serial task
- FIX: get_lang function exceptions caused by browsers that do not send cookies

10.18.8 2.1.1

- Added system_type config option
- Made sync functionality optional
- Updated init script to work with salt
- Support shared flag on web system types
- Relocated the baruwa service pid directory
- Renamed delivery methods to avoid confusion
- Ensure init script sets correct log file perms
- Updated Documentation
- Remove Banned Senders from appearing in Quarantine Report, Fixes #67
- FIX: Fixed local scores edit link
- FIX: Wrong link to edit SA score rule
- FIX: Catch exception in policy methods task
- FIX: Fixed message operations in distributed clusters
- FIX: DKIM not being added for alias domains Fixes: #66
- FIX: HTML editor not loading when editing a domain signature
- FIX: Wrong text in helpbox in the webinterface fixes issue #64
- FIX: Deleting organization leaves orphan Relaysettings, fixes issue #65

10.18.9 2.1.0

- Implemented builtin cluster quarantine syncronization. A detailed description is available at *Shared quarantine*
- Implemented search functionality for local scores
- Reimplemented the Spam learning system to make it faster and use less Memory.
- Reimplemented authentication system to use server side sessions as opposed to client side encrypted cookies
- FIX: Improved the IP address and IP range validations
- FIX: Improved the status generation functionality, replacing calls to unix utilities with built in code.

10.18.10 2.0.10

- Implemented support for CIDRs and network ranges in exemption lists closes #61
- Improved IP address validation in WEB and MTA
- Improved Geo lookups by switching to the faster Maxmind DB
- Updated documentation
- FIX: Catch encoding error in cdb file generator
- FIX: Catch indexerror in queuestats command
- FIX: Catch invalid IP range in lists
- FIX: Allow addition of email addresses in domain aliases domains
- FIX: Update routedata on domain aliases updates
- FIX: Some templates not rendering correctly on non branded servers

10.18.11 2.0.9

- Implemented local scanner settings cache to allow the scanner to continue scanning mail while the backend or database server is not available
- Added dynamically generated trusted_networks spamassassin configuration built from the relays added under organizations. This will ensure relayed messages are not checked on DNSBL's. Improving outbound functionality.
- Made improvements to yum plugin to run only when managed packages are changed
- Implemented filesystem based data loss prevention
- Spec and module updated to ensure proper permissions on restoredb directory
- Added functionality to prevent duplicates being restored from backup db
- Implemented user friendly error logging for perl modules
- Added timeout lock release function
- Modified baruwa-backup2db.pl run as root user
- Use timeout locks release instead of sleep
- Made local settings updates cluster aware
- Improved default policy extraction
- Added the version and copyright to templates
- Improved authentication backend roburstness
- Disabled the ability for domain admins to add lists to all
- FIX: Quarantine reports not sent on clustered setup due to missing logo
- FIX: Syntax error in quarantine reports cmd
- FIX: Catch indexerror exception in bulk operations
- FIX: Regression in the lists module display
- FIX: Authentication settings typos

- FIX: Rendering of release page without javascript
- FIX: Regression causing message processing to fail
- FIX: Removed duplication of preferences in sa-lint
- FIX: SQLalchemny non unicode param warning
- FIX: Only send one block notification on blocking an abusive client
- FIX: Error generated when delta index is run prior to full indexing.
- FIX: paster prune-database was not honouring config options
- FIX: Typo in upgrade documentation

10.18.12 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 PgSQL 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

10.18.13 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 addrs
- FIX: Incorrect rules being generated.

10.18.14 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

10.18.15 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

10.18.16 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

10.18.17 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.

10.18.18 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.

10.18.19 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

CHAPTER

ELEVEN

USER GUIDE

11.1 Signing In and Signing Out

11.1.1 Signing In

To signin 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.

11.1.2 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.

11.2 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.

11.2.1 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.

11.2.2 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

11.3 Personalizing Your Account

You can personalize various settings of your account using the account page.

11.3.1 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

11.3.2 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 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

11.3.3 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 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

11.3.4 Enable or Disable Spam Checks

You can choose to enable or disable Spam checks on messages destined to your account.

1. Go to the 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

11.3.5 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 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

11.3.6 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 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

11.4 Messages

11.4.1 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.

11.4.2 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.

11.4.3 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.

11.4.4 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.

11.4.5 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.

11.4.6 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

11.4.7 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

11.4.8 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

11.4.9 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.

11.5 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.

11.5.1 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

11.5.2 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

11.6 Reports

The reports view allows you to run a set of predefined reports. The following reports are available.

11.6.1 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.

11.6.2 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`

11.6.3 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`

11.7 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

11.7.1 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`

11.8 Baruwa Search Tips and Tricks

Baruwa supports many of the search tricks you use in popular web search engines.

11.8.1 Search with an exact phrase

To search for an exact phrase enclose the phrase in quotes `"Blocked message"`

11.8.2 Search for one or other

Use the pipe character `|` to separate the phrases `"Barrack Obama" | "Mike Tyson"`

11.8.3 Search using a wildcard

Use the star character * For example `boy*` will match `boy`, `boyfriend`

11.8.4 Search using the negate operator

`shaken !stirred` or `shaken -stirred` will match phrases with shaken but not `shaken stirred`

11.8.5 Search using grouping

`(red | green | blue) car` will match `red car`, `green car` or `blue car`

11.8.6 Search Specific fields

Note: It is also possible to limit your search to specific fields, the field operators will be provided later.

CHAPTER

TWELVE

SUPPORT

12.1 Bundled support

All Baruwa Enterprise Edition subscriptions include bundled email only support.

Email only support is available `8x5 UTC+2` 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. Baruwa Enterprise Edition support staff and developers subscribe to and actively monitor this list.

12.2 Paid support

Paid 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.

Paid support is provided under annual support agreements, we do not provide adhoc paid support.

To request a quotation, please email `enterprise (AT) baruwa.com`.

12.3 Support Package Matrix

	Standard	Gold	Platinum	Platinum Plus
Support Hours	8x5	8x5	24x5	24x7
Response time	36 Hours	24 Hours	12 Hours	6 Hours
Email Support	Yes	Yes	Yes	Yes
Chat Support	No	No	Yes	Yes
Phone Support	No	No	No	Yes
Remote Monitoring	No	Yes	Yes	Yes
Paid Support	No	Yes	Yes	Yes
Payment period	N/A	Annual	Annual	Annual

12.3.1 Terms explained

- 8x5 - 08H00 - 17H00 UTC+2 Monday - Friday
- 24x5 - 24Hours UTC+2 Monday - Friday

- 24x7 - 24Hours UTC+2 Monday - Sunday

CHAPTER

THIRTEEN

PREVIOUS DOCUMENTATION

The documentation for previous versions is available using at the following locations

- 2.1.7
- 2.1.6
- 2.1.5
- 2.1.4
- 2.1.3
- 2.1.2
- 2.1.1
- 2.1.0
- 2.0.10
- 2.0.9
- 2.0.8
- 2.0.7
- 2.0.6
- 2.0.5
- 2.0.4