Installation Guide for Snare Server v7

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance International Pty Ltd. This does not include those documents and software developed under the terms of the open source General Public Licence, which covers the Snare agents and some other software.

The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance International Pty Ltd. Other trademarks and trade names are marks' and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

Table of Contents

1. About this Guide 3

2. Hardware Configuration 4

3. Preparation 5

4. Snare Server Installation 6

5. Site specific items 16

1. About this Guide

This document details the steps required to install the components necessary to run the Snare Server as a standalone appliance on your hardware. The Snare Server relies on a number of Open Source tools, including the Linux Operating System, the Apache Web Server, and the PHP scripting language, amongst others - these are included with your installation media.

There are a number of configuration items, such as system passwords, that are specific to an installation. These are highlighted throughout this manual, and a section at the end of the document provides a space where you can record the site specific installation parameters. This document does not cover the installation and removal of specific Snare Agents; these are available as separate documents.

An appendix to this document also highlights several post-installation checks that will allow you to verify that the Snare Server has been installed correctly, and is operating optimally.

> **Important**
> This document does not cover the steps involved in migrating or upgrading an existing v4 / v5 / v6 Snare Server to Snare Server v7.
>
> Please review the Snare Server v7 Migration Guide for a side-by-side migration, and the Snare Server v7 Upgrade Guide for an over-the-top upgrade.

> **Other guides that may be useful to read**
> - Snare Server v7 Users Guide
> - Snare Server v7 Migration Guide
> - Snare Server v7 Upgrade Guide
> - Snare Agent Guides
> - Snare Server Troubleshooting Guide
> - Snare Toolset White Paper.

2. Hardware Configuration

2.1. Hardware Overview

The Snare Server is capable of running on a variety of hardware configurations, from laptops, right up to Linux partitions on mainframe systems. Hardware requirements are significantly dependent on the volume of audit received by the Snare Server, and the type and number of audit objectives defined.
However, in order for the Snare Server to be in a supported configuration, the following requirements MUST be followed. There should be no deviations from the specifications listed below.

ⓘ **Snare Server - Hardware Requirements**

- A 64-bit x86 compatible CPU (eg: Pentium Core I5, AMD64), preferably with two cores or more.
- 200Gb hard disk or larger. This should be recognized by an operating system as one single disk, and may be either IDE, SATA or SCSI. Hardware RAID may be used, as long as the RAID controller is capable of either emulating normal IDE/SATA/SCSI protocols, or has a supported driver available in Snare.
- An IDE, SATA or USB DVD writer supported by Snare. Most modern CD/DVD writers are ATAPI compatible, and will therefore work with the Snare Server. Some brands of USB Writers may be supported. Please consult the general compatibility notes below for more details.
- 2 Gb RAM, or more.
- A 100 megabit, or (preferably) a 1000 megabit (1 Gigabit) network card.
- Keyboard, mouse and monitor as appropriate.

⚠ **General compatibility notes**

In order to make compatibility research simpler, the Snare Server uses a Linux kernel from the Ubuntu 14.04 LTS 'Trusty' release. Hardware that is identified as compatible with the first release of Ubuntu 14.04 LTS 'Trusty' will also be accepted by the Snare Server.

2.2. Incompatible Hardware / Configurations

If commonly available hardware, or virtual machine implementations, are specifically identified as being incompatible with Snare Server version 7, the model numbers will be identified below.

ⓘ **Incompatible Hardware**

No hardware has yet been specifically identified as incompatible.

3. Preparation

Prior to installation, a check should be made of a number of configuration parameters required for the operation of the Snare Server. These configuration parameters are as follows:

⚠ **What You Need**

- An IP address for the Snare Server, and the Netmask of the local area network on which the Snare Server will be installed.
- A Hostname & fully qualified DNS Name for the Snare Server (your network team may wish to add this information into your organisational DNS server).
- The IP address of the default gateway for the local area network on which the Snare Server will be installed.
- The IP address of the organisational SMTP (Email server).
- The IP addresses of the organisational DNS server(s).
- The Snare Server download accessible from the Snare Secure Area at intersectalliance.com. Authorisation credentials and license are provided by your Snare Server support team.

In addition, you should make the following changes to the system BIOS in order to ensure that installation and operation proceed smoothly:

- Set the system to automatically boot when power is reapplied after a system power failure.
- Set the first CD/DVD drive to be bootable.

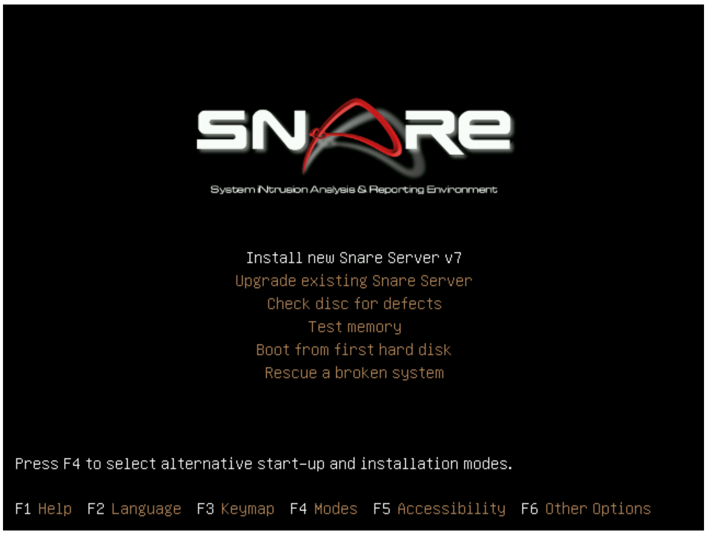
The steps required to accomplish the two operations above, vary depending on your system, and bios type.

4. Snare Server Installation

Snare is an appliance-like solution, that includes the operating system, and the Snare Server software, on the installation media. A heavily customised distribution of Linux is used for the baseline installation.

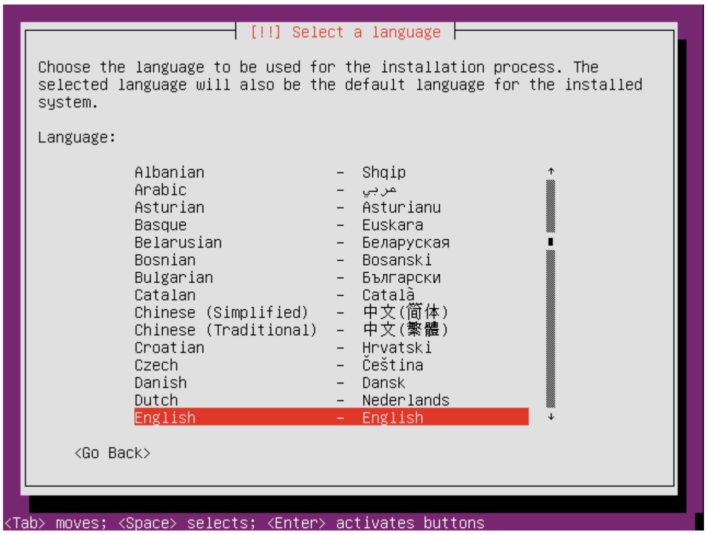
The system which will host the Snare Server must be configured to boot from the CD or DVD device. Please note that a monitor, mouse and keyboard should be connected to the server or workstation.

Once you boot from the Snare Server installation media, the installation will ask you a number of questions. The following images and instructions will guide you through the process of installation.

Snare Server Installation - Kickstart	
 System Intrusion Analysis & Reporting Environment Install new Snare Server v7 Upgrade existing Snare Server Check disc for defects Test memory Boot from first hard disk Rescue a broken system Press F4 to select alternative start-up and installation modes. F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options	Insert the Snare Server Installation media, and boot the computer. The Snare Server installation media will provide you with a guided install of the Linux operating system, and the Snare Server tools and utilities, presenting you with only those options that may vary from site to site, or from system to system, and specifically require your input. Hit ENTER on your keyboard.

Operating System Bootstrap	
	When you hit ENTER, the Snare Server will boot the Linux operating system. The screen will remain blank for some time, and then a new video mode will appear on your monitor. Please Wait

Language Selection

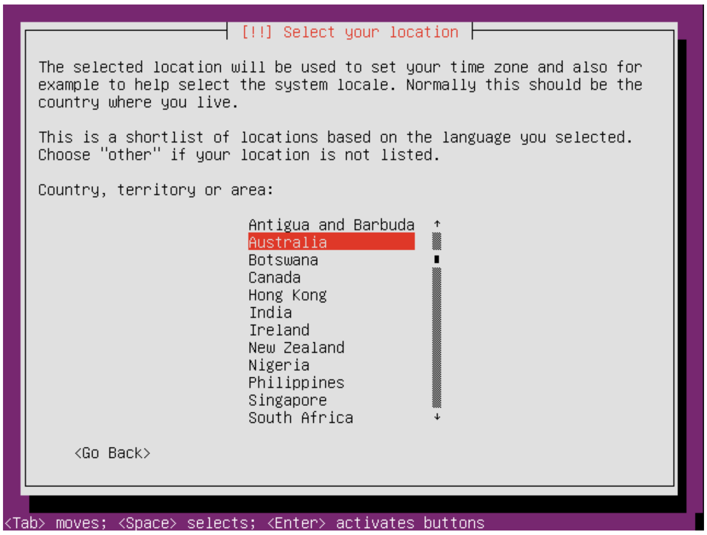


```
[!!] Select a language

Choose the language to be used for the installation process. The
selected language will also be the default language for the installed
system.

Language:

           Albanian               -  Shqip
           Arabic                 -  عربي
           Asturian               -  Asturianu
           Basque                 -  Euskara
           Belarusian             -  Беларуская
           Bosnian                -  Bosanski
           Bulgarian              -  Български
           Catalan                -  Català
           Chinese (Simplified)   -  中文(简体)
           Chinese (Traditional)  -  中文(繁體)
           Croatian               -  Hrvatski
           Czech                  -  Čeština
           Danish                 -  Dansk
           Dutch                  -  Nederlands
           English                -  English

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Although the Snare Server currently only supports the English language, some elements of the operating system installation process can be localised.

Select the language that is most appropriate for your current geographic location, and press ENTER.

Location Selection

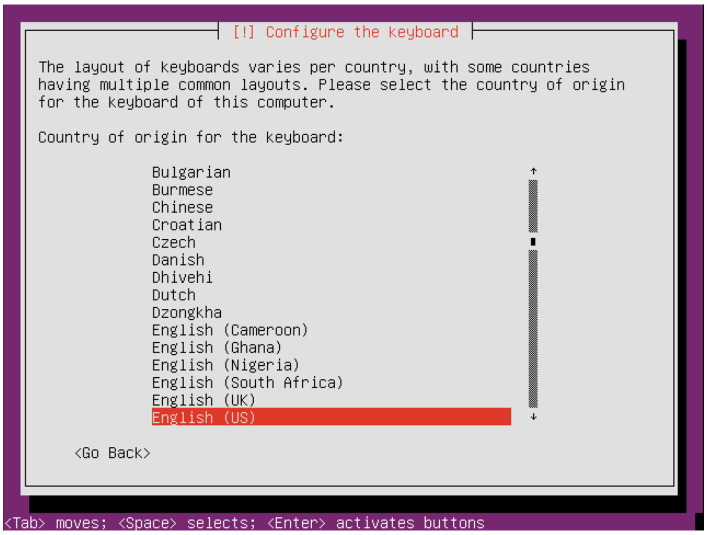


```
[!!] Select your location

The selected location will be used to set your time zone and also for
example to help select the system locale. Normally this should be the
country where you live.

This is a shortlist of locations based on the language you selected.
Choose "other" if your location is not listed.

Country, territory or area:

                        Antigua and Barbuda
                        Australia
                        Botswana
                        Canada
                        Hong Kong
                        India
                        Ireland
                        New Zealand
                        Nigeria
                        Philippines
                        Singapore
                        South Africa

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

The installer will attempt to provide a range of potential locations, based on your language selection.

Select your geographic location, and press ENTER.

Keyboard Layout

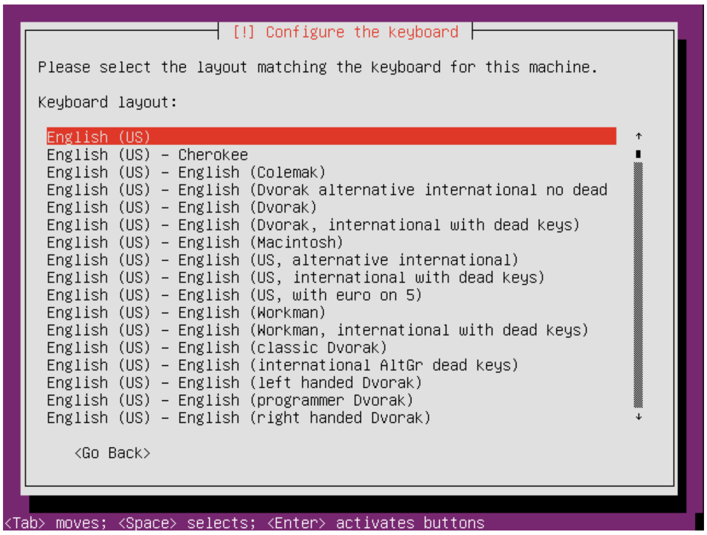


```
[!] Configure the keyboard

The layout of keyboards varies per country, with some countries
having multiple common layouts. Please select the country of origin
for the keyboard of this computer.

Country of origin for the keyboard:

             Bulgarian
             Burmese
             Chinese
             Croatian
             Czech
             Danish
             Dhivehi
             Dutch
             Dzongkha
             English (Cameroon)
             English (Ghana)
             English (Nigeria)
             English (South Africa)
             English (UK)
             English (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Local keyboard layouts are supported for the Snare Server.

Select an option appropriate for your type of keyboard, and press ENTER.

Keyboard Layout (2)

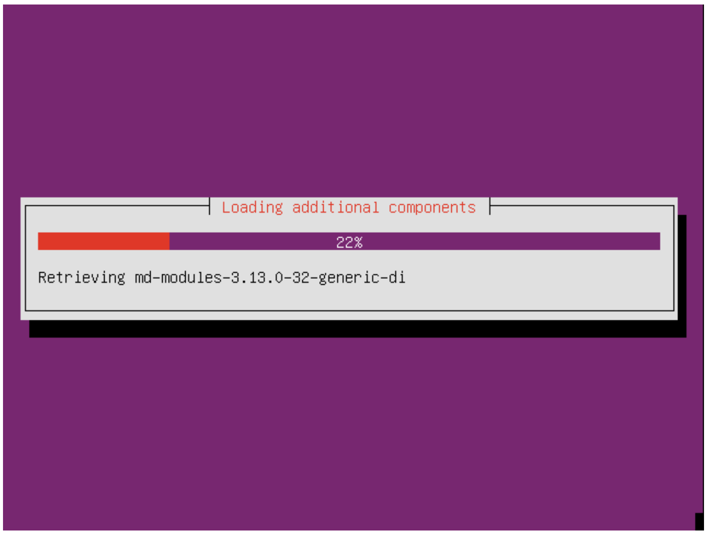


```
[!] Configure the keyboard

Please select the layout matching the keyboard for this machine.

Keyboard layout:

English (US)
English (US) - Cherokee
English (US) - English (Colemak)
English (US) - English (Dvorak alternative international no dead
English (US) - English (Dvorak)
English (US) - English (Dvorak, international with dead keys)
English (US) - English (Macintosh)
English (US) - English (US, alternative international)
English (US) - English (US, international with dead keys)
English (US) - English (US, with euro on 5)
English (US) - English (Workman)
English (US) - English (Workman, international with dead keys)
English (US) - English (classic Dvorak)
English (US) - English (international AltGr dead keys)
English (US) - English (left handed Dvorak)
English (US) - English (programmer Dvorak)
English (US) - English (right handed Dvorak)

   <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Some languages/locations provide more than one option for keyboard layouts (eg: Qwerty, Dvorak).

Select an option appropriate for your type of keyboard, and press ENTER.

Preparing for Installation

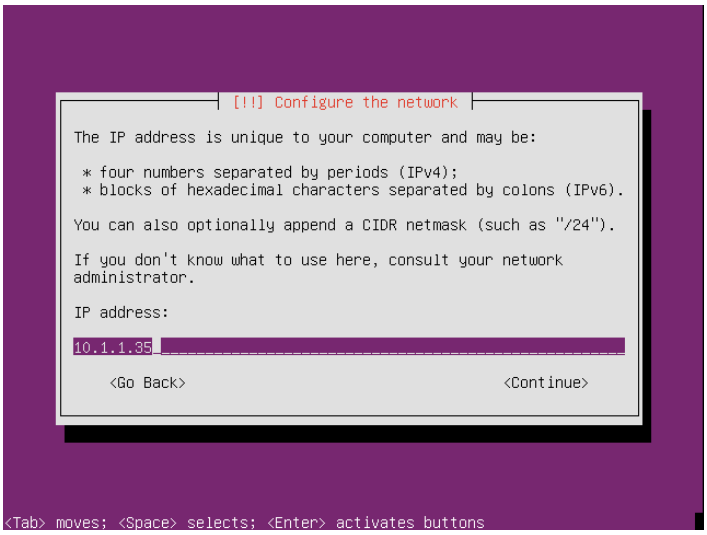


```
Loading additional components
                       22%
Retrieving md-modules-3.13.0-32-generic-di
```

The Snare Server will scan the local application database for installation targets, and load additional components.

Please wait.

IP Address Configuration

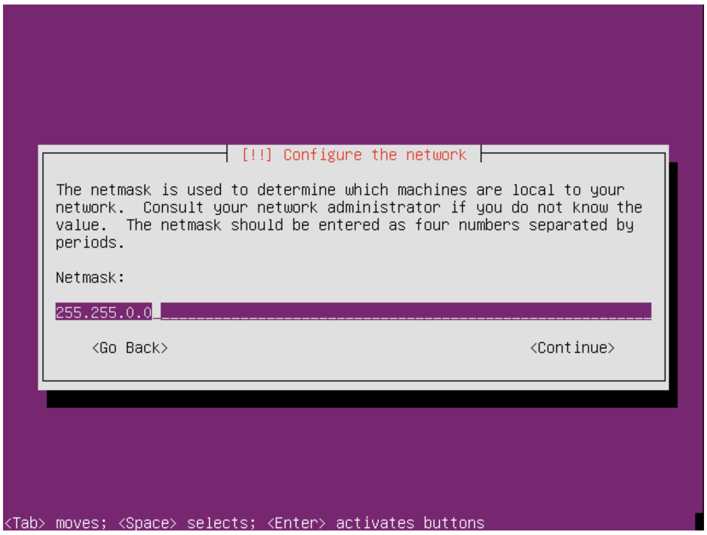


```
[!!] Configure the network

The IP address is unique to your computer and may be:

 * four numbers separated by periods (IPv4);
 * blocks of hexadecimal characters separated by colons (IPv6).

You can also optionally append a CIDR netmask (such as "/24").

If you don't know what to use here, consult your network
administrator.

IP address:

10.1.1.35_____________________________________________________

    <Go Back>                                       <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Your Snare Server will require an IP address in order to participate on the network. You may need to consult your network administration team for assistance with an appropriate allocation, so that address conflicts do not occur.

Type the IP Address of the Snare Server, and press ENTER.

Netmask

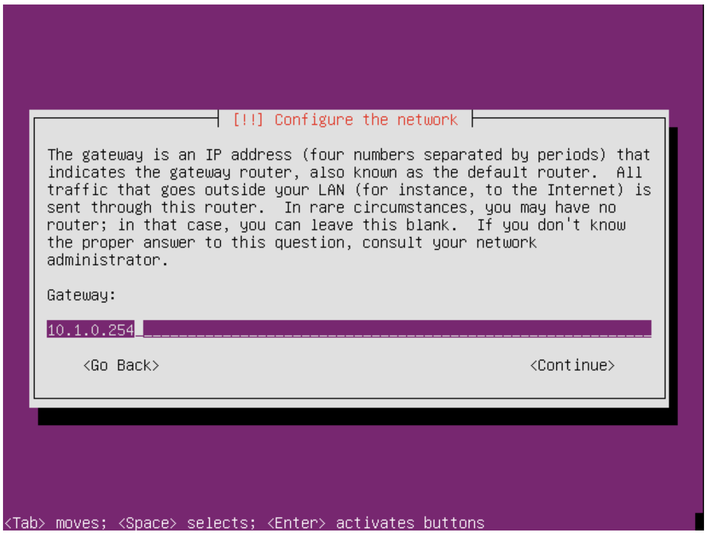


```
[!!] Configure the network

The netmask is used to determine which machines are local to your
network.  Consult your network administrator if you do not know the
value.  The netmask should be entered as four numbers separated by
periods.

Netmask:

255.255.0.0

    <Go Back>                                          <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Your Snare Server will need to know the netmask to use for the local network. You may need to consult with your network administration team for assistance with an appropriate value, but most networks on which a Snare Server will be installed will generally use either a 'Class C' (255.255.255.0), or 'Class B' (255.255.0.0) range.

Type the Netmask for the network on which the Snare Server will be active.

Default Gateway

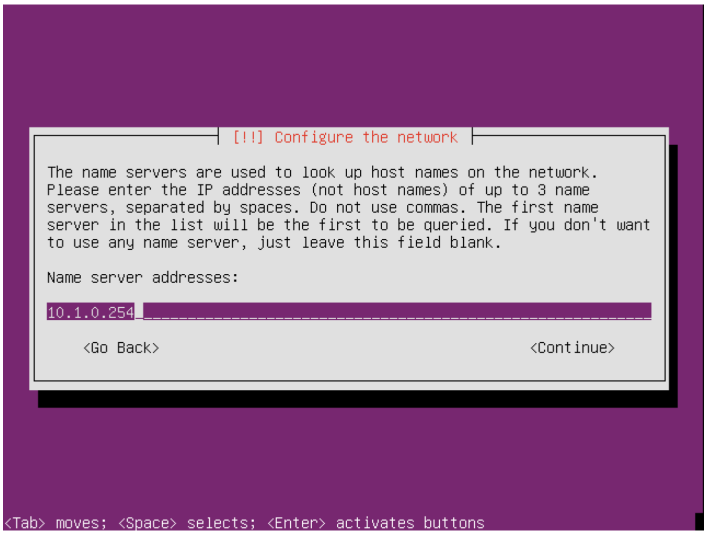


```
[!!] Configure the network

The gateway is an IP address (four numbers separated by periods) that
indicates the gateway router, also known as the default router.  All
traffic that goes outside your LAN (for instance, to the Internet) is
sent through this router.  In rare circumstances, you may have no
router; in that case, you can leave this blank.  If you don't know
the proper answer to this question, consult your network
administrator.

Gateway:

10.1.0.254

    <Go Back>                                          <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

In order to contact (and be contacted by) machines outside the local area network, your Snare Server will need to know the IP address of the default gateway on the local network. You may need to consult with your network administration team for an appropriate value.

Type the Default Gateway Address that the Snare Server should use to contact non-local network devices, and press ENTER.

Name Servers

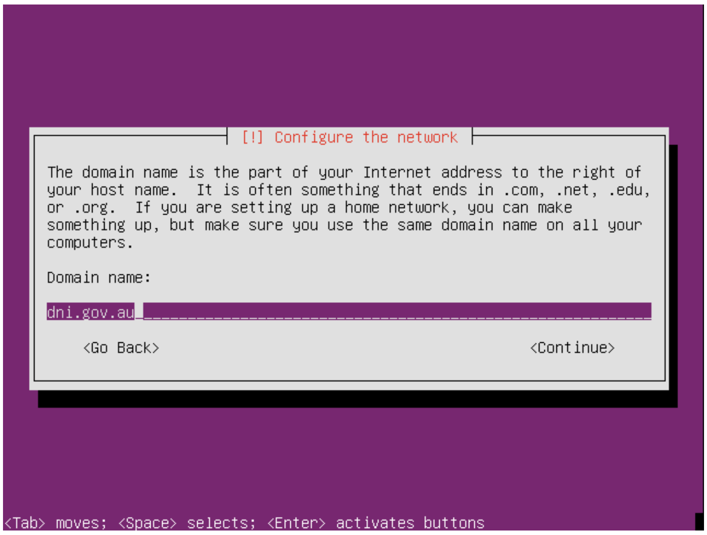


```
[!!] Configure the network

The name servers are used to look up host names on the network.
Please enter the IP addresses (not host names) of up to 3 name
servers, separated by spaces. Do not use commas. The first name
server in the list will be the first to be queried. If you don't want
to use any name server, just leave this field blank.

Name server addresses:

10.1.0.254

    <Go Back>                                          <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Enter the IP address of your Domain Name Server(s).

Space separated DNS Server IP addresses, then press ENTER

Domain Name

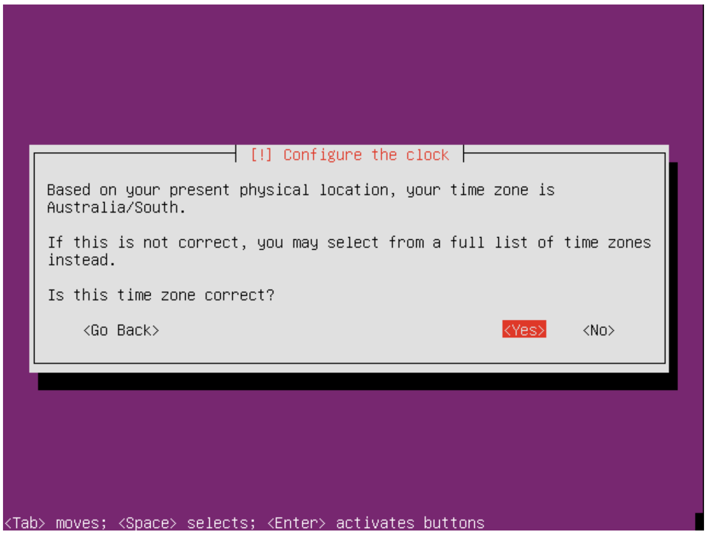


```
[!] Configure the network

The domain name is the part of your Internet address to the right of
your host name.  It is often something that ends in .com, .net, .edu,
or .org.  If you are setting up a home network, you can make
something up, but make sure you use the same domain name on all your
computers.

Domain name:

dni.gov.au

    <Go Back>                                              <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

The domain name is generally the alphabetic part of your company or organisational internet address; it may include '.gov' or '.com'. Do not include the hostname in this text entry box.

Type the domain name under which the Snare Server will exist, and press ENTER

Time Zone



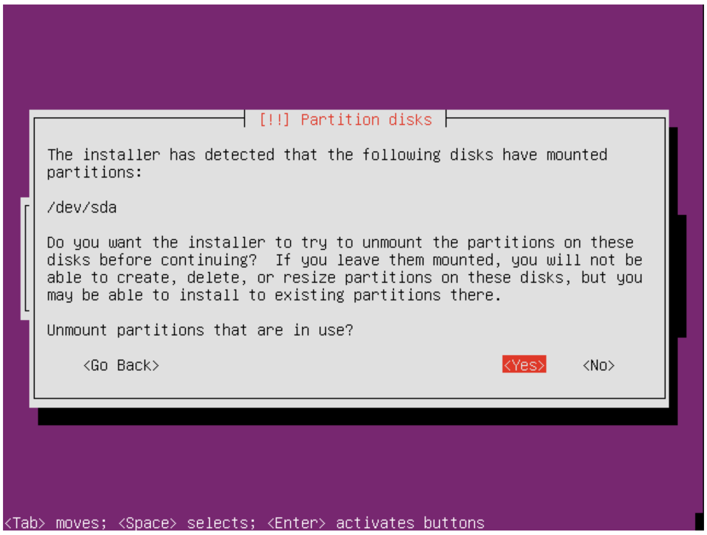
```
[!] Configure the clock

Based on your present physical location, your time zone is
Australia/South.

If this is not correct, you may select from a full list of time zones
instead.

Is this time zone correct?

    <Go Back>                                          <Yes>     <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

The Time Zone setting is important to ensure that your Snare Server retains appropriate time settings, particularly during events such as "Daylight Saving".

The installation process will attempt to detect your approximate physical location based on your earlier location and language settings.

Select your time zone. The list will be populated with values based on your earlier location and language selections.

Partitioning - mounted partitions



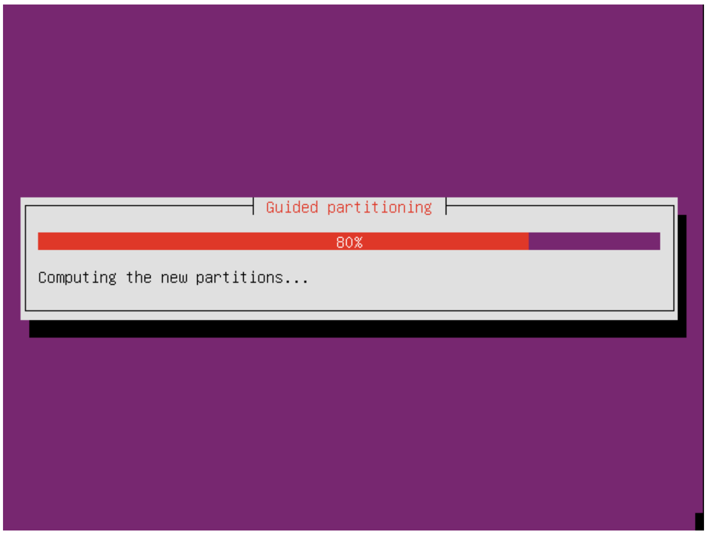
```
[!!] Partition disks

The installer has detected that the following disks have mounted
partitions:

/dev/sda

Do you want the installer to try to unmount the partitions on these
disks before continuing?  If you leave them mounted, you will not be
able to create, delete, or resize partitions on these disks, but you
may be able to install to existing partitions there.

Unmount partitions that are in use?

    <Go Back>                                          <Yes>     <No>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

If the server on which you intend to install Snare, already has disks formatted with a file system that Snare is able to recognise, the installer may attempt to mount the disks.

If it does so successfully, this dialog may appear, requesting that you unmount the partition.

Select 'Yes'.

Partitioning

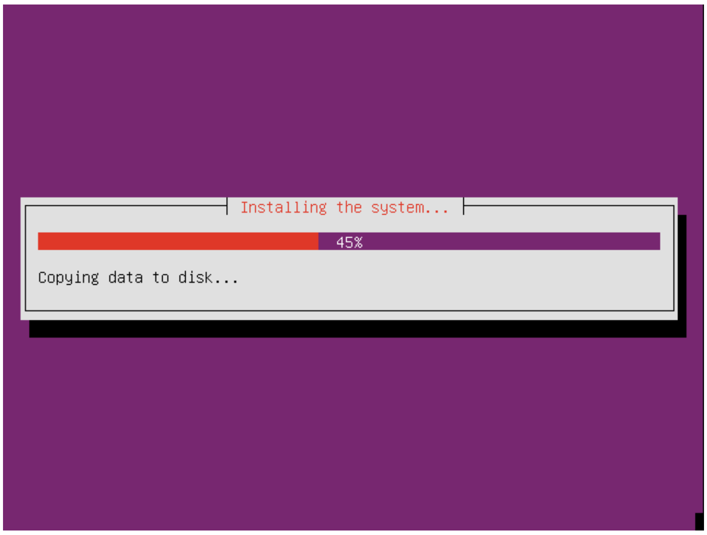


```
Guided partitioning
80%
Computing the new partitions...
```

The local disk will be automatically partitoned based on Snare's requirements.

Please Wait.

Installing the Base System

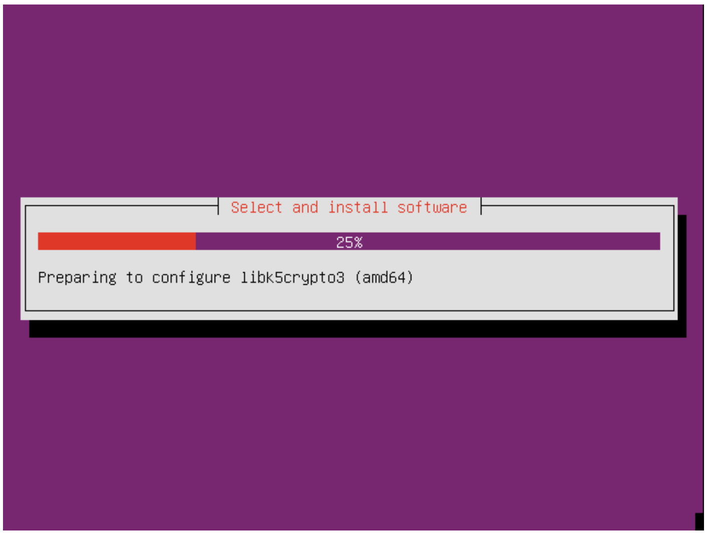


```
Installing the system...
45%
Copying data to disk...
```

The installation process will install the system packages required for the operation of the Snare Server.

Please Wait.

Selecting and Installing Software

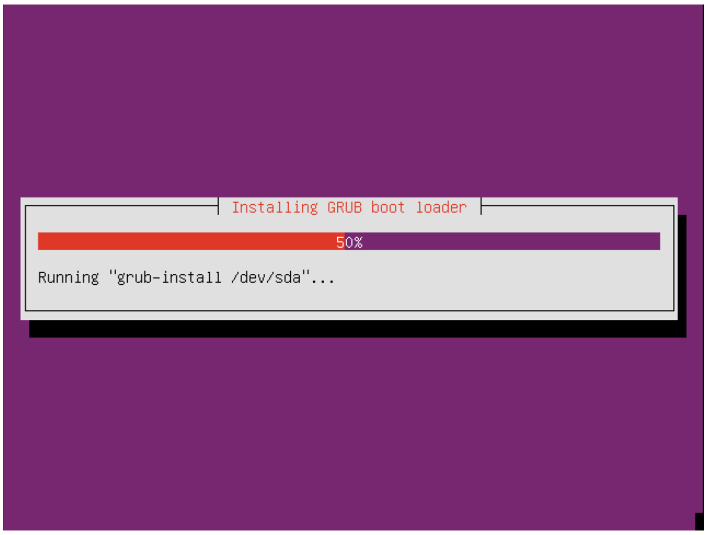


```
Select and install software
25%
Preparing to configure libk5crypto3 (amd64)
```

Additional packages required by Snare, over and above the operating-system level functions will also be installed.

Please Wait.

Installing Boot Loader



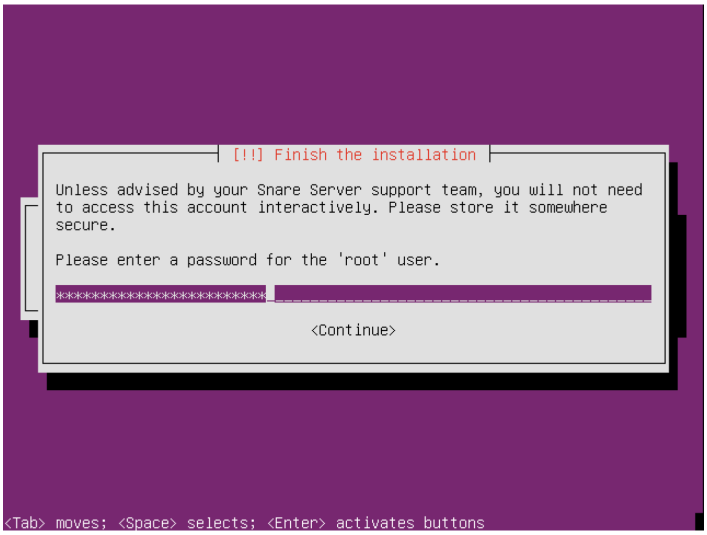
```
Installing GRUB boot loader
50%
Running "grub-install /dev/sda"...
```

The primary disk on the server will be set to boot the Snare Server operating system.

On some systems, the installer may confirm if it should install GRUB, or other similar system components. This should be answered with a "*Yes*", otherwise the Snare Server will not boot.

Please Wait.

Account Authentication



```
[!!] Finish the installation

Unless advised by your Snare Server support team, you will not need
to access this account interactively. Please store it somewhere
secure.

Please enter a password for the 'root' user.

*************************_

<Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

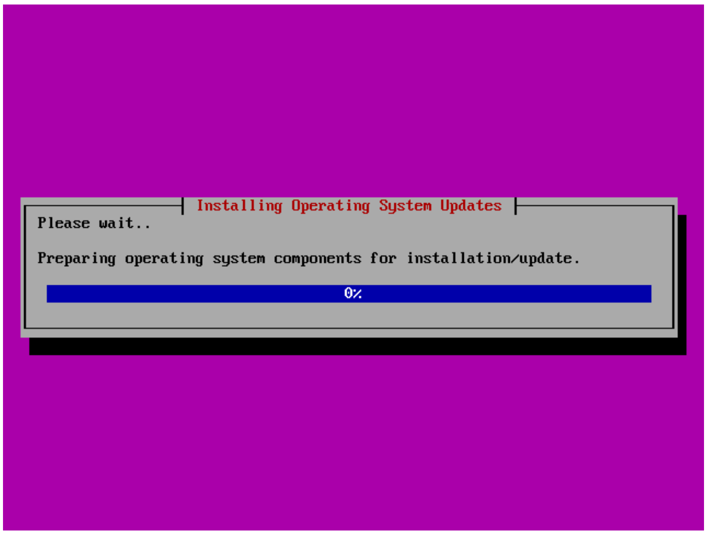
The installation subsystem will ask you to supply default passwords to several accounts, including:

- The Snare operating system 'root', and 'snare' user accounts, used for emergency hardware-level system administrative activities, as guided by your Snare Server support team.
- The Snare operating system 'snarexfer' account, which can be used by remote systems to transfer log data to the Snare Server via ftp or scp.

⚠ *Although the Snare Server implements several password complexity controls such as dictionary exclusions, minimal length, and so on; initial installation passwords are NOT subject to such controls.*

Enter appropriate passwords for each account.

System Reboot & Operating System Updates



```
Installing Operating System Updates
Please wait..

Preparing operating system components for installation/update.

0%
```

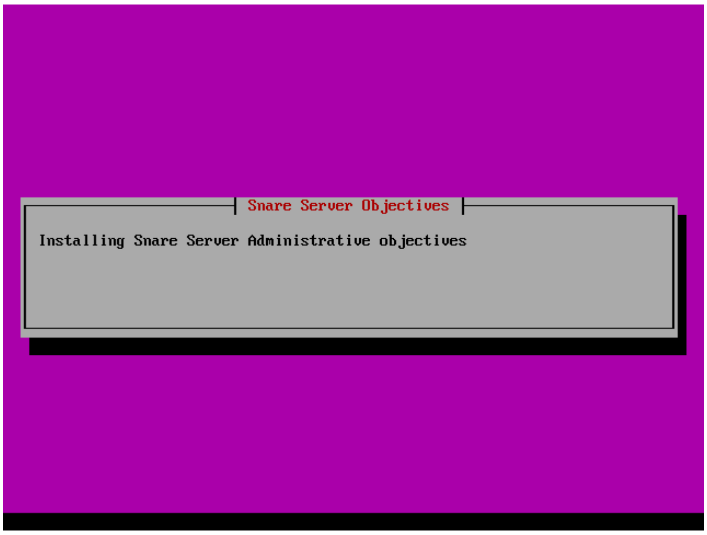
Once the installation process has completed, the Snare Server will automatically reboot.

At this point, specific components required for the operation of the event collection, analysis and reporting environment, will be installed; as will security updates to the baseline packages that come with the installation media.

This process should take approximately 8 minutes to complete, depending on the number of updates included. The most recent line from the raw output from the package update process, will be displayed within the dialog window.

Please wait.

Snare Server Bootstrap

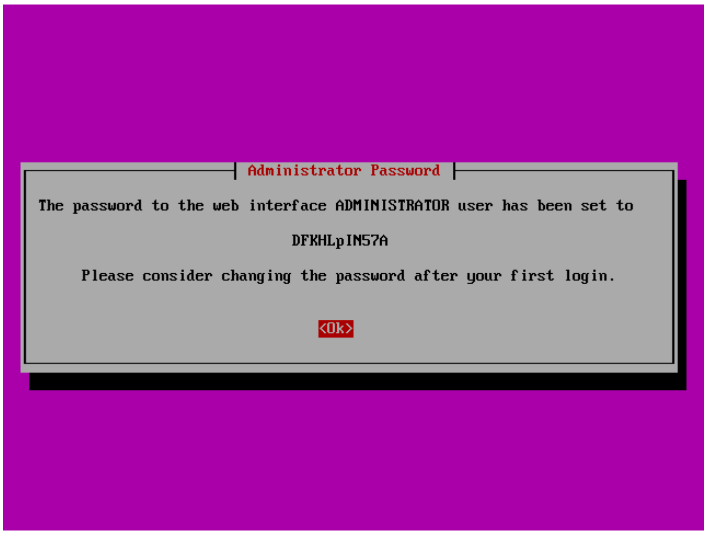


```
Snare Server Objectives
Installing Snare Server Administrative objectives
```

Several server-specific tasks will scroll through, including the installation and configuration of configuration databases, the installation of administrative objectives, and the initialisation of firewall rulesets.

Please wait.

Administrator Password



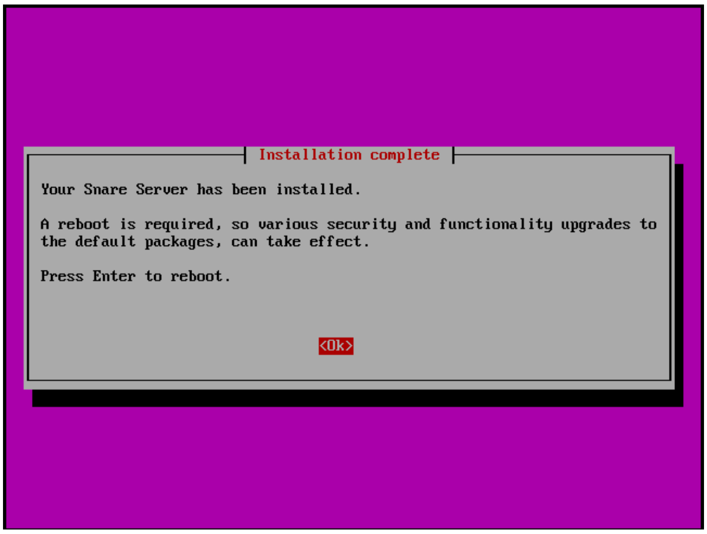
```
Administrator Password
The password to the web interface ADMINISTRATOR user has been set to

DFKHLpIN57A

Please consider changing the password after your first login.
```

An initial password for the "Administrator" account for the Snare Server web interface, will be generated, set, and displayed.

The password will be chosen from random alpha-numeric characters, be 10 characters in length, and will exclude look-alike characters such as O/0 and I/l.

Please note this password for future reference.

Restart to complete installation



```
Installation complete

Your Snare Server has been installed.

A reboot is required, so various security and functionality upgrades to
the default packages, can take effect.

Press Enter to reboot.

<Ok>
```

The Snare Server needs to reboot one last time at the completion of the installation process, to complete the upgrade process of system packages.

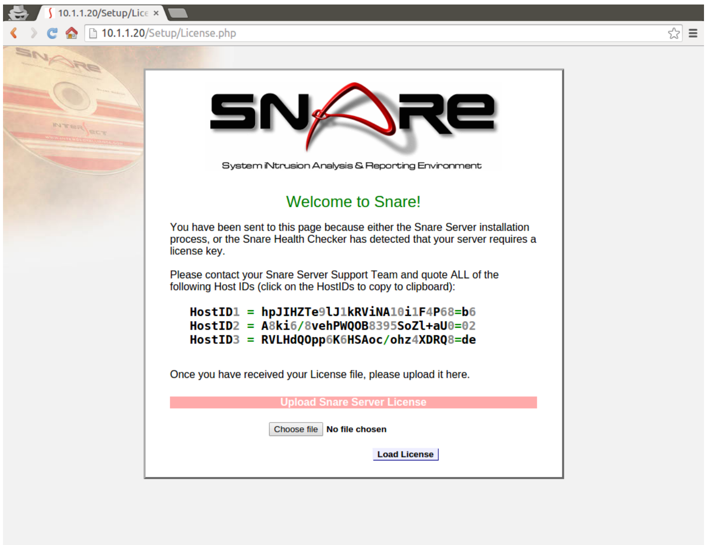
Press Enter to reboot.

Server Ready

The Snare server has now installed, and is ready to access via your web browser. Point your browser at the IP address or DNS name for your new server to continue.

You can also login to the console directly using the *snare* user and password set up during the installation process.

License Information


10.1.1.20/Setup/Lice
10.1.1.20/Setup/License.php
SNARE
System iNtrusion Analysis & Reporting Environment

Welcome to Snare!

You have been sent to this page because either the Snare Server installation process, or the Snare Health Checker has detected that your server requires a license key.

Please contact your Snare Server Support Team and quote ALL of the following Host IDs (click on the HostIDs to copy to clipboard):

```
HostID1 = hpJIHZTe9lJ1kRViNA10i1F4P68=b6
HostID2 = A8ki6/8vehPWQOB8395SoZl+aU0=02
HostID3 = RVLHdQOpp6K6HSAoc/ohz4XDRQ8=de
```

Once you have received your License file, please upload it here.

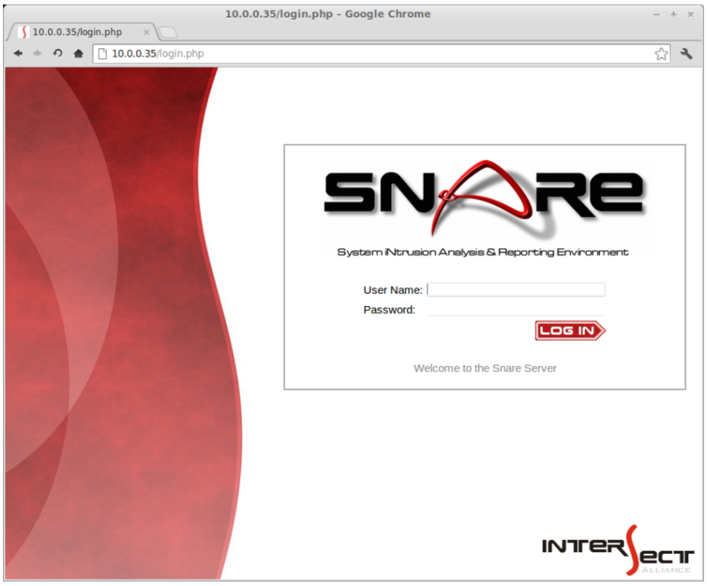
Upload Snare Server License

Please point your web browser at the Snare Server. A screen will appear, that identifies multiple HostID's - please contact your Snare Server support team, and supply these HostID's.

The Snare Server support team will provide you with a license to access the Snare Server.

Send the hostID's to the Snare Server support team.

Log in to the Snare Server

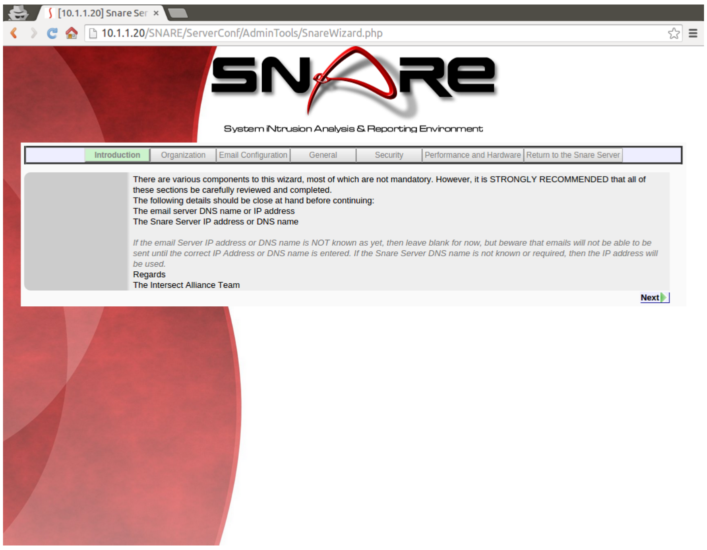


Welcome to the Snare Server

The Snare Server will present a login page. Enter the UserID "Administrator", and the password that was generated by the installation process.

Log into the Snare Server.

Configuration Wizard


[10.1.1.20] Snare Ser
10.1.1.20/SNARE/ServerConf/AdminTools/SnareWizard.php
SNARE
System iNtrusion Analysis & Reporting Environment
Introduction
Organization
Email Configuration
General
Security
Performance and Hardware
Return to the Snare Server
Next

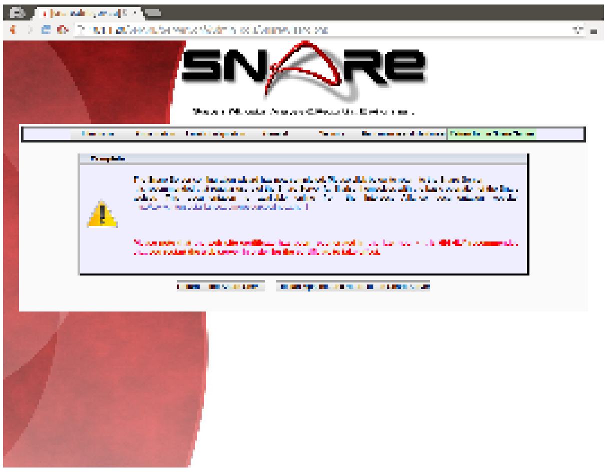
There are various components to this wizard, most of which are not mandatory. However, it is STRONGLY RECOMMENDED that all of these sections be carefully reviewed and completed.
The following details should be close at hand before continuing:
The email server DNS name or IP address
The Snare Server IP address or DNS name

If the email Server IP address or DNS name is NOT known as yet, then leave blank for now, but beware that emails will not be able to be sent until the correct IP Address or DNS name is entered. If the Snare Server DNS name is not known or required, then the IP address will be used.
Regards
The Intersect Alliance Team

When you first access the Snare Server, a configuration wizard will appear. Follow the prompts to configure your Snare Server. More details about the configuration can be found in the Snare Server Users Guide, and you can always come back to the Configuration Wizard at a later time as required.

Use the Next and Previous buttons to move between the sections.

Configuration Wizard - Done



Once the configuration wizard has finished - this page will return you to the Snare Server.

Press the "Return to the Snare Server" button.

5. Site specific items

Based on the above installation procedures, there are a number of site specific configuration items which will need to be set, and stored in a secure manner, such as a safe or approved, lockable cabinet. These configuration items are mainly passwords, so it is a good idea to choose a secure password, and to ensure that only the appropriate authorised staff have access to the passwords detailed below. The table below allows you to record key site specific configurations items at install-time.

Snare Server Installation Configuration items

Snare Server Installation undertaken by: …...

Date: …..

Signature:...

Agency Notes: …...

…..

…..

…..

Item	Configuration description	Site information
1	Snare Server "Root" password - Emergency maintenance	
2	Snare Server "snare" user password - Maintenance	
3	Snare Server "snarexfer" user password - log transfer	
4	Snare Server networking configuration	IP Address: Netmask: Default Gateway: DNS 1: DNS 2: DNS 3:
5	SMTP Server	IP Address: Hostname: