AVAYA

SCS 4.0

Disaster Recovery Planning

Task Based Guide

Copyright © 2010 Avaya Inc.
All Rights Reserved.

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/ LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER.
UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:http://www.avaya.com/support

Copyright © 2010 ITEL, All Rights Reserved

The copyright in the material belongs to ITEL and no part of the material may be reproduced in any form without the prior written permission of a duly authorised representative of ITEL.

Table of Contents

Disaster Recovery Planning 6

How to Use this Guide 7

A Note on High Availability (HA) Configuration 8

Process and Procedure 9

The Programming Record 9
Scheduling Regular Backups 9
Scheduled Backups 10
Manual Backups 12
- Manual Backups to Local Storage 12
- Manual Backups – To FTP 15

User Profile Exports 17
- Importing from a CSV File 19

Recovering the SCS System 21

System Restore 22

Restoring from the Server Archive 22
Restoring by File Upload 23

System Rebuild (without High Availability) 26

Creating an SCS Installation Build 26
- Downloading the SCS ISO File 26
- Burning the ISO File to DVD 26
- Creating a Bootable USB Image 28

Configuring LAN and SIP Settings 33
- Activation and Restore 44
- Restoring from FTP 45
- Restoring by File Upload 46

System Rebuild (with High Availability) 48

Scenario 1: Rebuilding the Master Server (no backup) 49

Creating an SCS Installation Build 51
- Downloading the SCS ISO File 51
- Burning the ISO File to DVD 51
- Creating a Bootable USB Image 53

Configuring the SCS Master Server 58
Licensing the System 68
Creating the Secondary Server Profile 69
Synchronising the Servers 71

Scenario 2: Rebuilding the Master Server with a Backup Archive 76

Creating an SCS Installation Build 77
Downloading the SCS ISO File 77
Burning the ISO File to DVD 77
Creating a Bootable USB Image 79
Licensing the System 95
Restoring Backup Archives 95
Restoring by File Upload 96
Sending Server Profiles 98

Scenario 3: Rolling System Configuration Back with a Backup Archive 100

Restoring Backup Archives 100
Restoring from the Local Archive or FTP 100
Restoring by File Upload from a Secondary Location 101
Sending the Secondary Server Profile 102

Scenario 4: Rebuild the Secondary Server 105

Gathering Secondary Server Profile Information 106
Creating an SCS Installation Build 107
Downloading the SCS ISO File 107
Burning the ISO File to DVD 107
Creating a Bootable USB Image 109
Configuring the Secondary Server 114
Sending the Secondary Server Profile 124

Avaya Documentation Links 126

Disaster Recovery Planning

Note: This guide details disaster recovery strategies for the SCS running on the **Dell** platform, for other platforms please see documentation provided with the system.

The Software Communication System (SCS) provides a critical service to your business enterprise telecommunications. If the worst should ever happen and your SCS system fails, you will need a fast and reliable method for restoring systems and services with minimum fuss. The ‘Break Glass in Emergency’ approach is inefficient and more often than not causes much stress and wasted time. Prevention is definitely better than cure. It is a fact known to all IT professionals that sometimes systems fail (be it through hardware failure or human error) but if the right preventative measures and processes are in place, system failure does not have to be elevated to disaster. It is for this reason that we recommend you read this guide early on and implement some of the procedures discussed within.

The purpose of this brief guide is twofold: 1) to highlight a few simple measures that can be put in to place to help guard against prolonged down time and data loss in the event that your SCS should fail for some reason; 2) to guide you through the process of recovering your system and your services.

Not all topics discussed in this guide will be relevant to all administrators; different configurations create different scenarios, for example, not all sites will employ a High Availability configuration. The intention is to provide clear and easy guidance on the quickest and easiest methods for recovering your SCS system. The only section that will be relevant to all SCS administrators is the ‘Process and Procedure’ section, because it offers insight into some techniques that might be employed to lessen the chances of major inconvenience, should issues arise with your SCS.

How to Use this Guide

This guide has been split into two parts. The first part deals with processes and procedures for protecting your SCS system from account data and configuration loss, and looks in some detail at facilities such as Export and Backup. It is recommended that you study this section in order to find out how best to guard against prolonged down time should the worst happen.

The second section, ‘Recovering the SCS System’ deals with specific recovery techniques. Because of the scenario-based nature of this section, it is not expected that you will read it from start to finish. Rather the intention is that you will be able to select from the table of contents, found at the front of the guide, which scenario best suits your particular circumstances. Scenarios range from single server installations with complete backup archives to HA setups with no archive. Each individual scenario segment is a complete step-by-step guide to getting your system up and running again, covering all aspects of the task from creating an installation DVD or USB thumb drive to restoring archives, so there is no need to flick backwards and forwards through the guide to find particular processes.

A Note on High Availability (HA) Configuration

The SCS server can be configured with High Availability (HA) fault tolerance to ensure service continuity in the event of server failure by setting up **two** servers:

- **Master** The master server provides the day-to-day operational platform for the SCS. (Some operational load is shared with the distributed system during normal circumstances).

- **Distributed system** The distributed system server (also known as the Redundant Server) provides temporary continuation of call service in the event that the master server fails. (The distributed system shares some operational load with the master during normal circumstances).

Setting up a High Availability configuration **does not** automatically guarantee the continuation of **all** services in the event of master server failure; some services, such as voicemail and conferencing, will be unavailable while the master server is offline. The redundant server should therefore not be treated as a permanent replacement for the primary master server, should the master fail.

Following is a list of services that are **unavailable** in the absence of the master server:

- **Media services** – voicemail, auto attendant, Call Park, call centre ACD

- **Configuration services**

- **Administrator and User portals**

- **Instant Messaging**

Even without these services, calls can still be made and received to and from internal and external numbers; crucially, this includes emergency numbers.

Although there are advantages to be gained from configuring a High Availability system, administrators should not lose sight of the fact that clear processes and solid planning will limit the time that master server operation is interrupted.

Process and Procedure

IT processes and procedures often determine how quickly vital systems are brought back online after hardware or human error. The following section details some measures that, if put in place, will help lessen the time it takes to recover the system and therefore speed up service continuity.

The Programming Record

The Programming Record is a series of forms that have been created to allow you to store critical configuration information about the key components that make up your SCS system – for example, the SCS server, dial plans, media gateways, etc. As soon as initial installation and setup have been completed, or whenever configuration changes are made to the system, system administrators can store the new details in this easy-to-use form. The Programming Record can then be used as a reference for restoring system settings later. **The Programming Record is not intended for use as a an import medium.**

Once filled in, ensure that both a hardcopy and an electronic copy of the Programming Record are kept in a safe location and updated whenever changes are made to the SCS's configuration.

Scheduling Regular Backups

The backup archive is perhaps your most important asset in a disaster recovery situation. **The importance of taking regular backups cannot be overstated.** The SCS backup utility is capable of archiving configuration and voicemail data and can be scheduled to run at regular intervals. Backup data is stored on the server by default, but it can also be downloaded and stored on a workstation or laptop – it is recommended that all backup archives be saved to a secondary location, in case of server failure.

The Backup utility can be configured to email configuration backups to the system administrator whenever they are taken. Voicemail backups cannot be emailed because of the size of most voice files, but they can be downloaded manually by the administrator. Alternatively, an FTP option can be employed to automatically move all backups to a secondary location.

The following pages detail how to create backup archives manually and automatically.

Note: Ensure that backup files are transferred to a secondary location, either by manually saving them to a suitable destination folder or by requesting email notification/attachments (voicemail files must always be transferred manually due to size limitations on most mail servers).

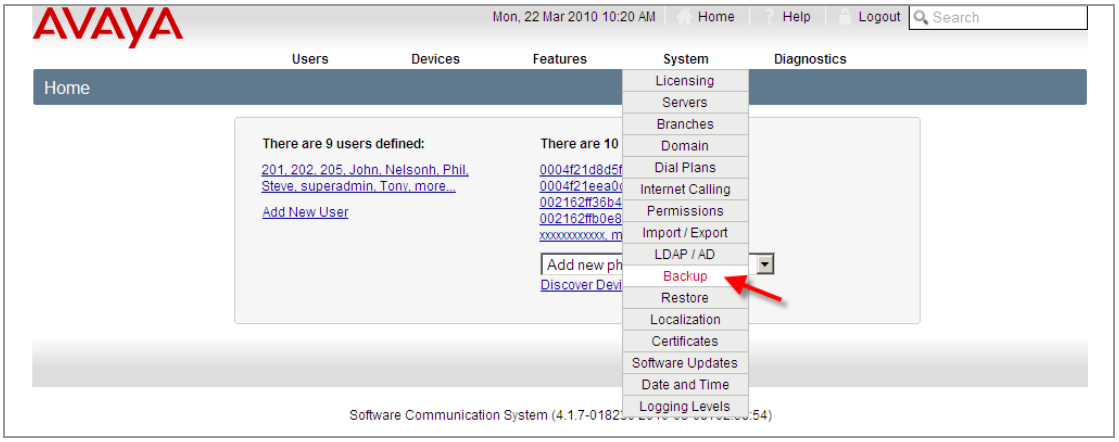
Scheduled Backups

Regularly scheduled backups offer the greatest chance of data recovery in the event of system failure. As is the case with manual backups, the SCS will create a backup archive locally and, if configured to do so, forward a copy of all backup configuration files to an email address – voicemail backup files must be copied manually, since they cannot be emailed due to size constraints.

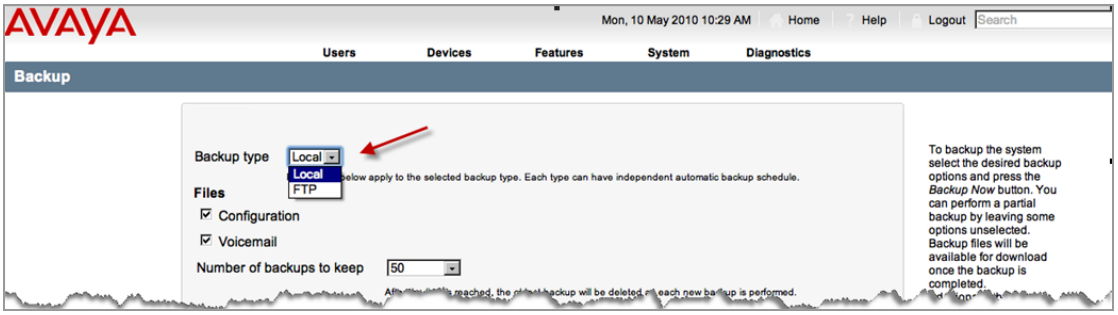
The Backup utility can also be configured to automatically pass archives directly to an FTP site – users should note that if the FTP option is employed, archives will not be stored in the SCS internal storage.

To create a backup schedule:

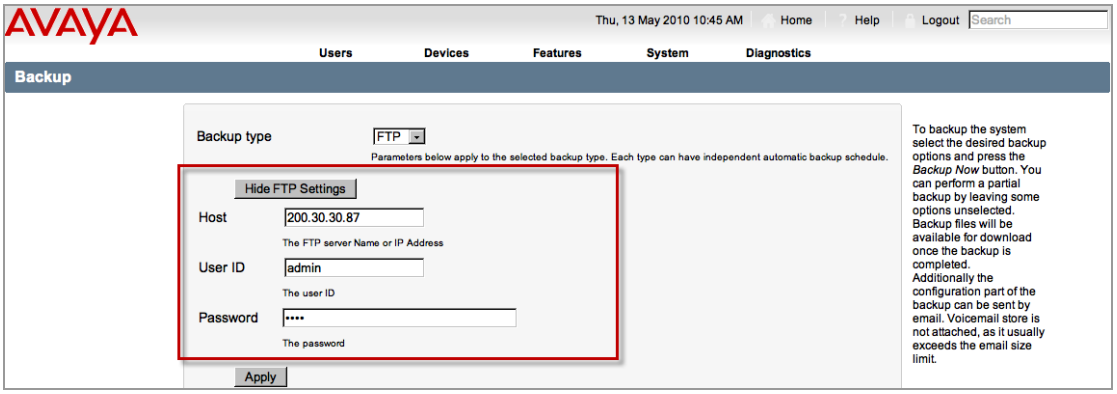
1. Open the **System** menu and select **Backup**.



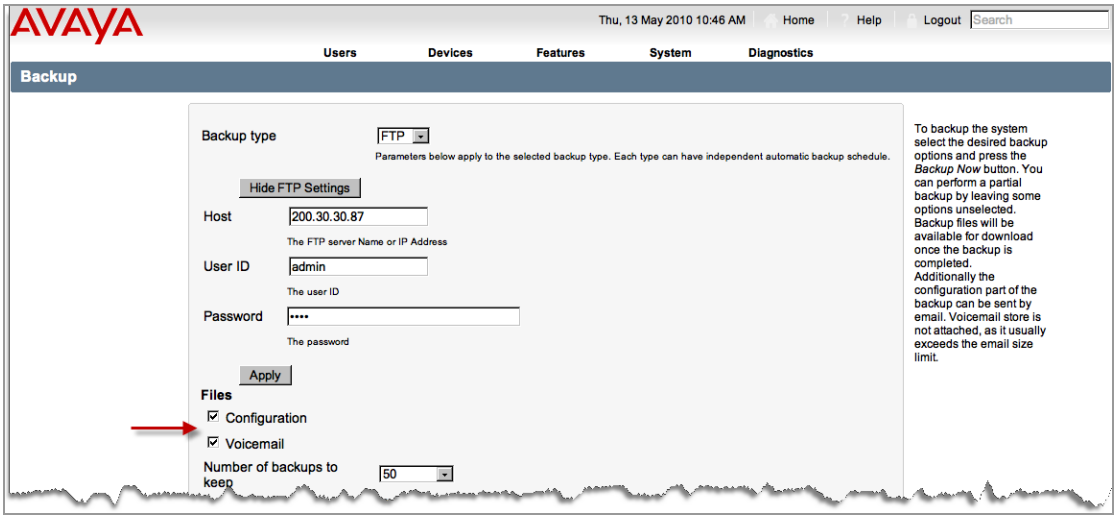
2. Choose between **Local** and **FTP** storage.



3. If you select FTP you may need to set FTP settings – click on **Show FTP Settings** to set the address, username and password of the FTP server if necessary.



4. Using the check-boxes, choose which SCS components you would like to back up. Choose from configuration files and/or voicemail files. Configuration archives will contain SCS configuration data, while voicemail archives will contain just messages.



5. Open the drop-down menu and select how many backups you would like the SCS to store on the server. If **Unlimited** is selected, the SCS will store an indeterminate number of backup files; selecting a limited number will result in the oldest records being overwritten once the limit has been reached.

   If you elected to save to an FTP location you do not need to configure this option because backup archives will already go to a secondary location.

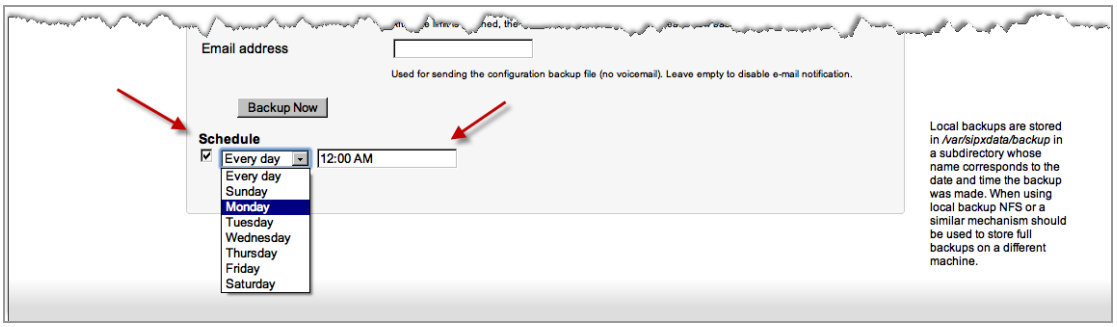
Note: The SCS server will not store an indefinite number of archive files if **Unlimited** is selected; eventually archive storage capacity will be reached, in which case, the oldest records will be overwritten with new records.

6. Enter an email address to which backup notifications and copies of configuration archives can be sent. Voicemail archives cannot be emailed due to the size of audio files.

As with the previous field, if you selected the FTP backup option at the top of the screen, you will not need to fill this field since the backup files will automatically transfer to a secondary location.

7. Tick the **Schedule** check-box.

8. Open the drop-down menu and select the day of the week on which you would like backups to take place.



9. Enter the time of day at which you would like backups to take place (enter the time in 12-hour format).

10. Click **OK**.

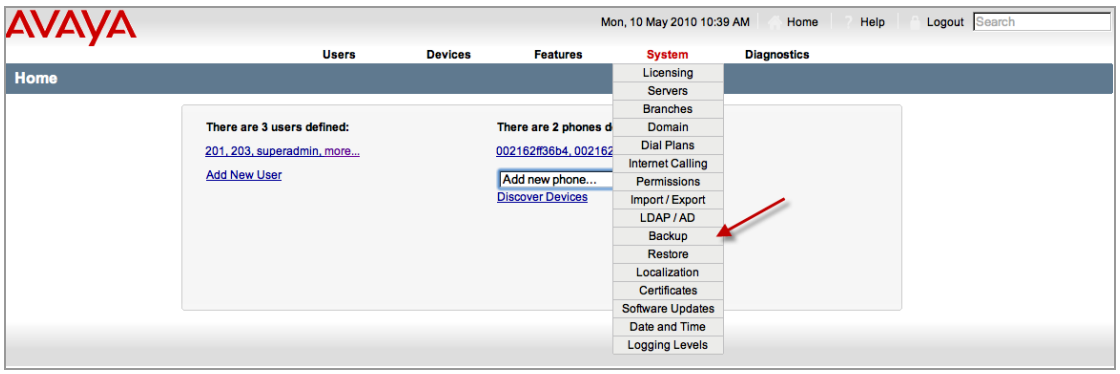
The schedule is set. The next backup will take place at the appointed time.

Manual Backups

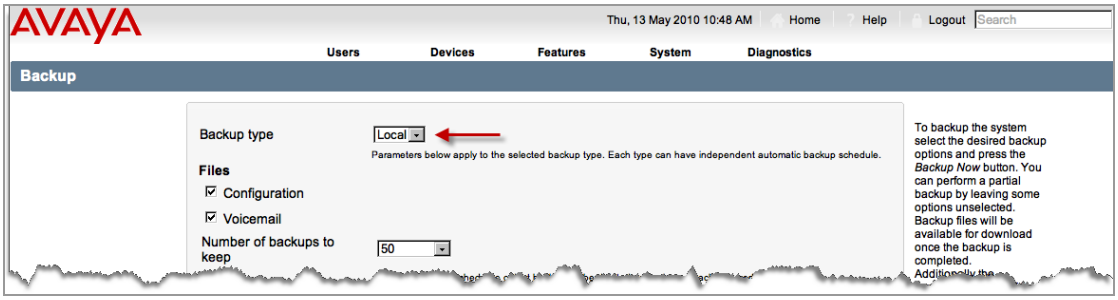
Manual Backups to Local Storage

Backups can be stored internally on your SCS server or locally on the administrator's workstation (or other workstation/laptop). It is recommended that backup archives are kept in a secondary location to guard against data loss in the unlikely event that the master server fails.

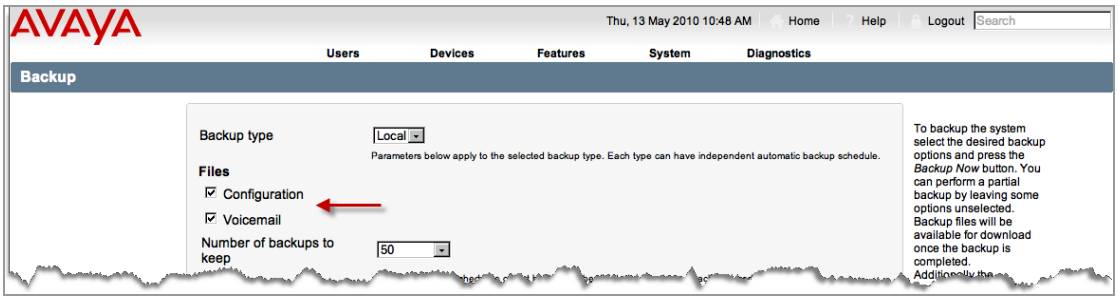
1. Open the **System** menu and select **Backup**.



1. Ensure that the drop-down menu at the top of the screen is set to **Local**.

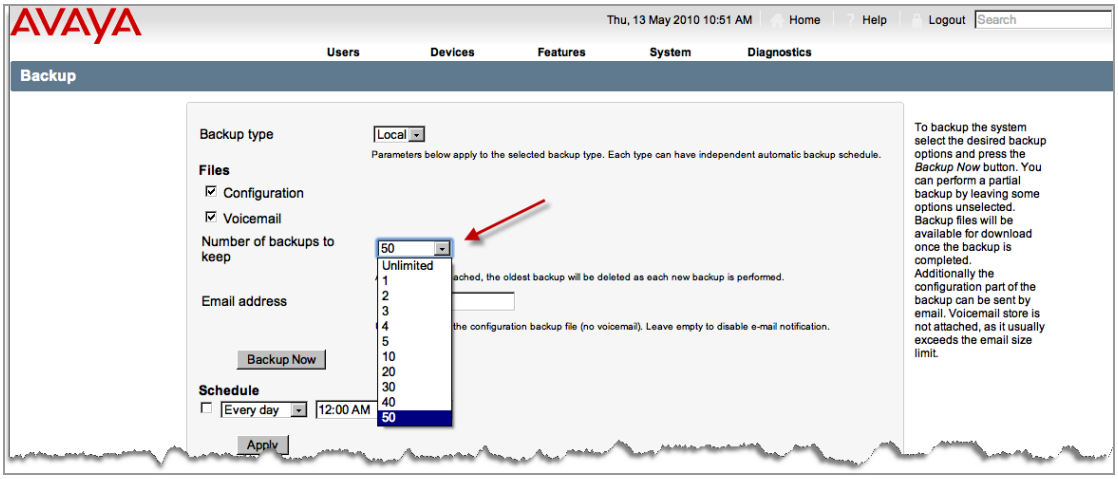


2. Using the check-boxes, choose which SCS components you would like to backup. Choose from configuration files and/or voicemail files. Configuration archives will contain SCS configuration data, while voicemail archives will contain just messages.

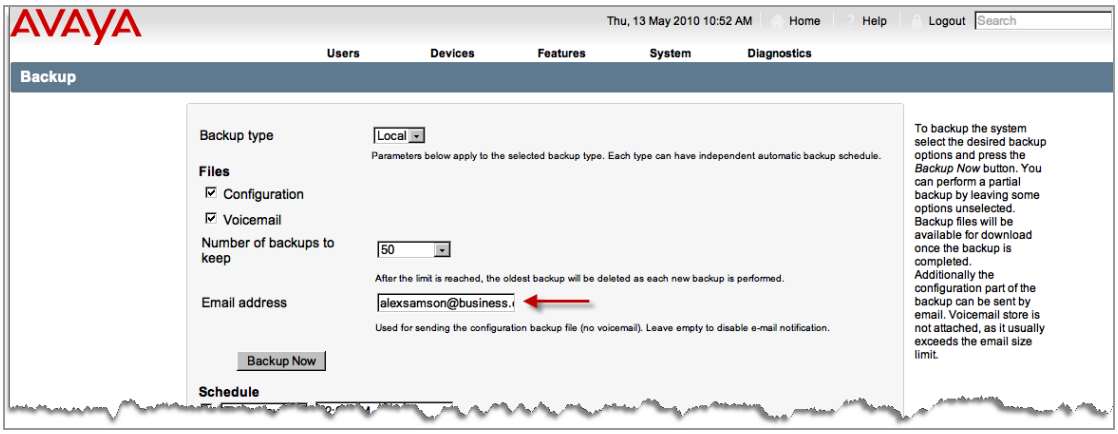


3. Open the drop-down menu and select how many backups you would like the SCS to store on the server. If **Unlimited** is selected, the SCS will store an indeterminate number of backup files; selecting a limited number will result in the oldest records being overwritten by new records once the limit has been reached.

Note: The SCS server will not store an indefinite number of archive files if **Unlimited** is selected; eventually archive storage capacity will be reached, in which case, the oldest records will be overwritten with new records.

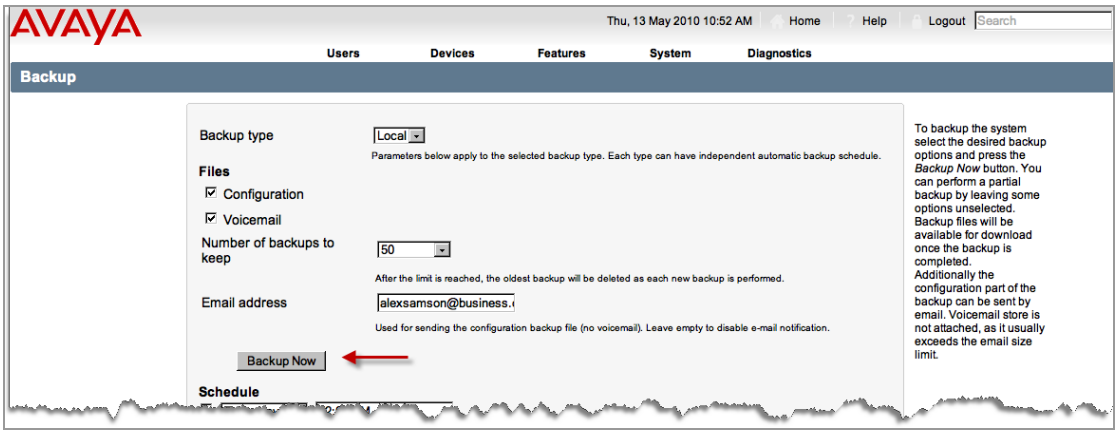


4. Enter an email address in the text box to enable email notification of backups. The SCS will attach and send a copy of each backup file. Leave this box empty to disable email notifications.



Note: Email notifications will **not** include voicemail backup files, due to the large size of voicemail files. To ensure voicemail backups are saved to a secondary location, click on the relevant file link and save the archive manually when backup is complete – see step 7.

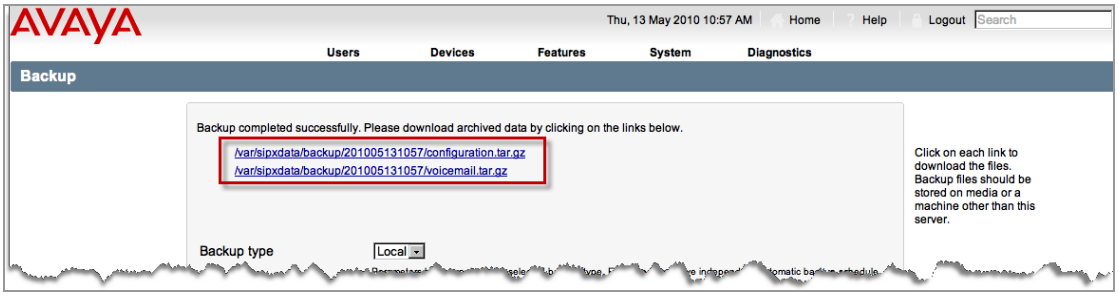
5. Click the **Backup Now** button.



6. Archive files are created in the following default directory on the SCS server: **/var/sipxdata/backup/yyyymmddtttt/backuptype.tar.gz** where *yyyymmddtttt* is the year, month, day and time of the backup and *backuptype* is the type of backup, e.g., configuration files or voicemail files.

7. a) If you did not enter an email address at step 4, click on each file link to save the files to your local workstation's drive and then continue to step 8.

   b) If you did enter an email address, configuration backups will be sent automatically to the designated email address. However, voicemail backups **will not** be forwarded to email. Click on the voicemail link to download a copy of the file to your preferred destination.



8. When the save dialogue appears, click the **Save** button – by default Mozilla Firefox will save downloads to your desktop – unless otherwise configured.

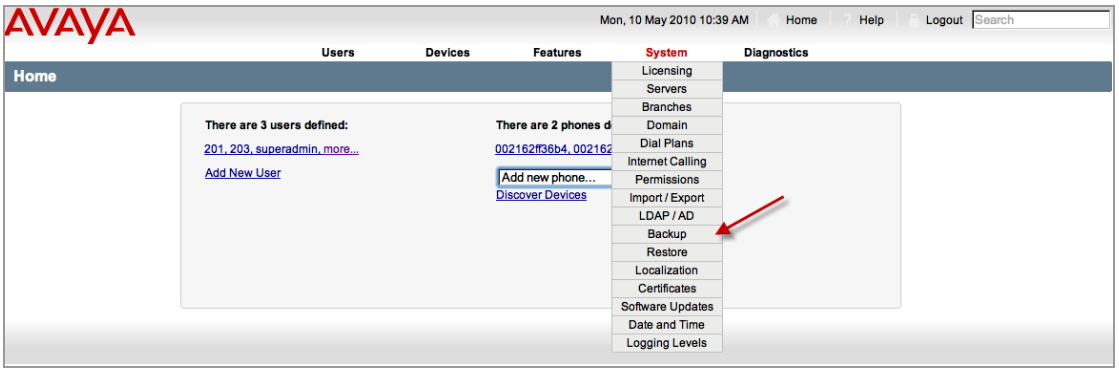


Backup is complete. Archive files are now stored on the SCS server and in your secondary location.

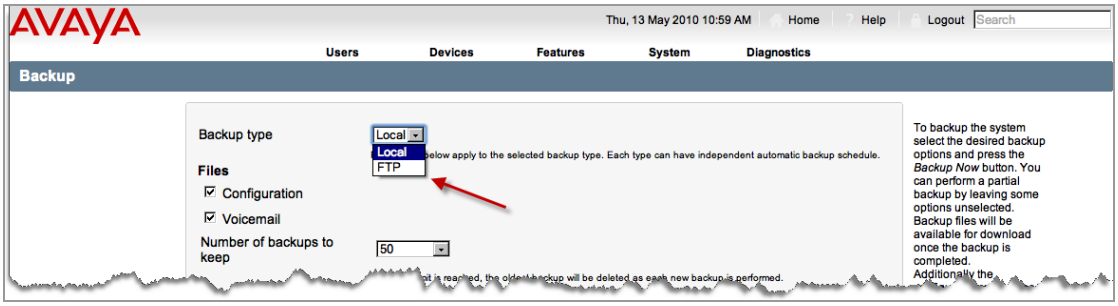
Manual Backups – To FTP

To create a backup that is automatically transferred to a preferred FTP location:

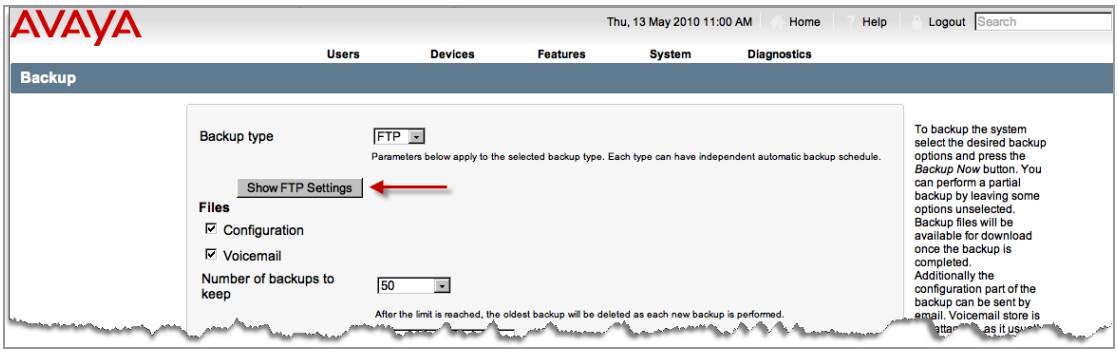
1. Open the **System** menu and select **Backup**.



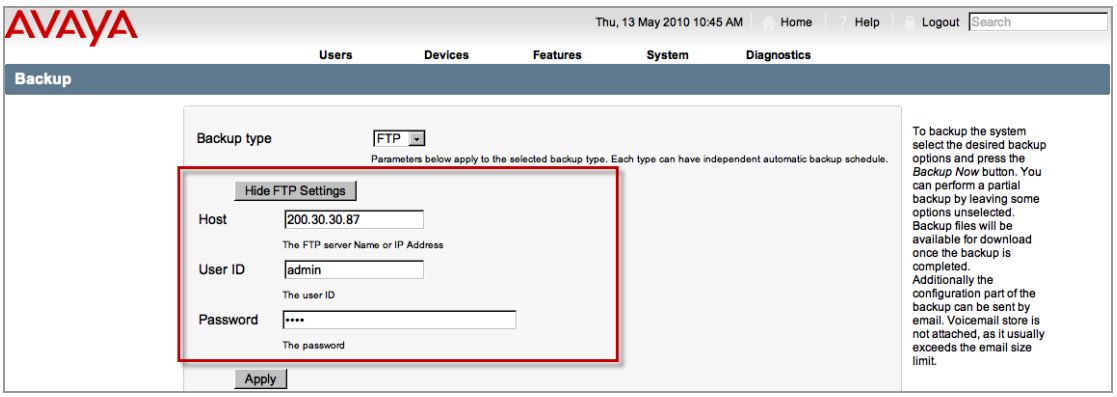
2. Open the drop-down menu at the top of the screen and select **FTP**.



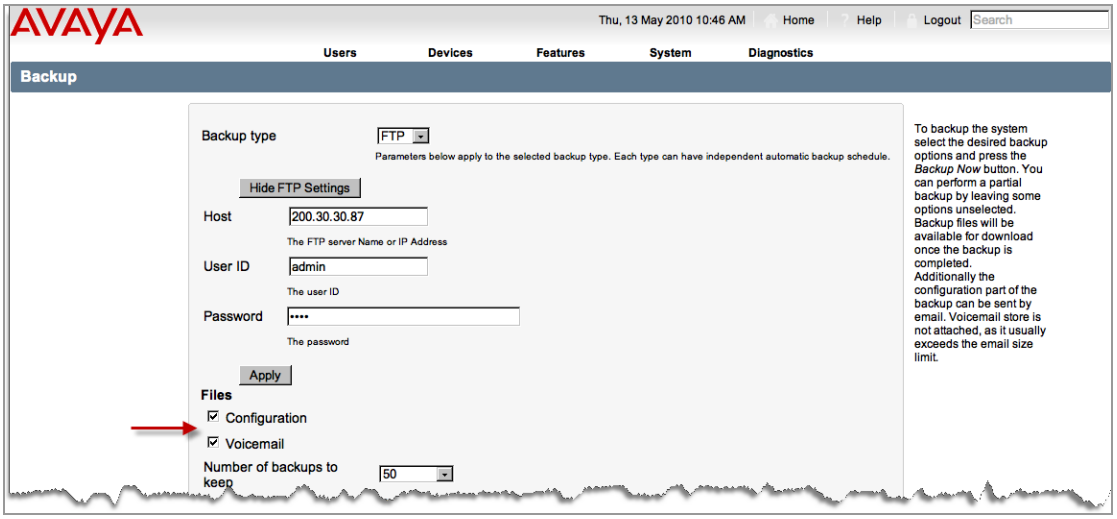
3. To configure FTP settings, click on **Show FTP Settings**.



4. Set the FTP server name or IP address, username, and password. Then click the **Apply** button.



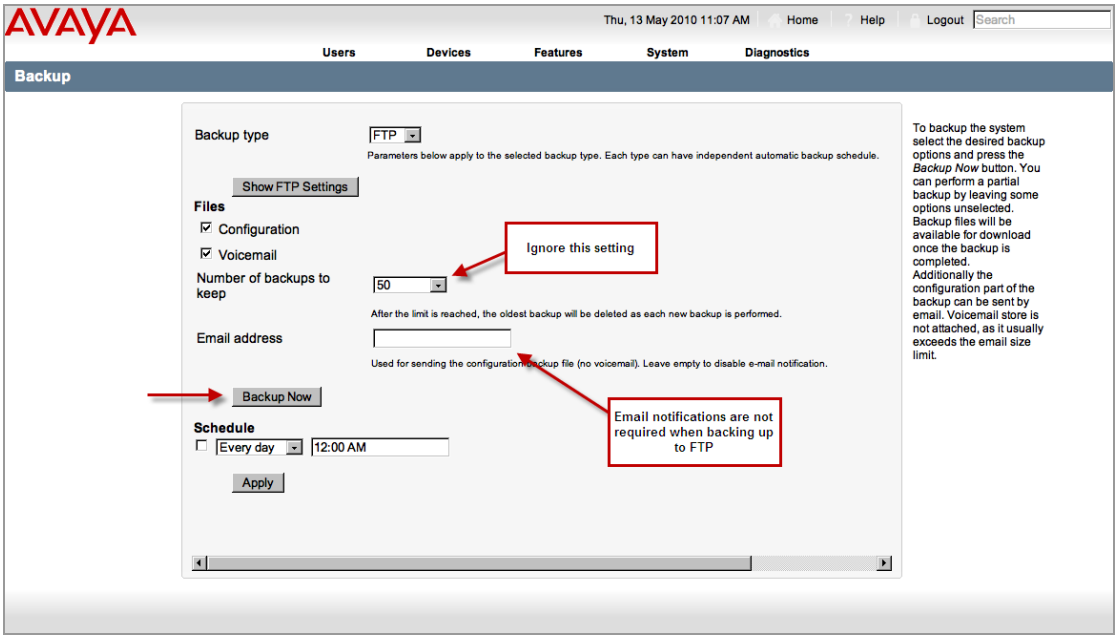
5. Using the check-boxes, choose which SCS components you would like to backup. Choose from configuration files and/or voicemail files. Configuration archives will contain SCS configuration data, while voicemail archives will contain just messages.



6. When using the FTP facility, the SCS will not store copies of backup files on its own internal storage, you therefore can ignore the 'Number of backups to keep' option.

7. Leave the email text box blank, since the backup is already being transferred to a secondary location.

8. Click the **Backup Now** button.



User Profile Exports

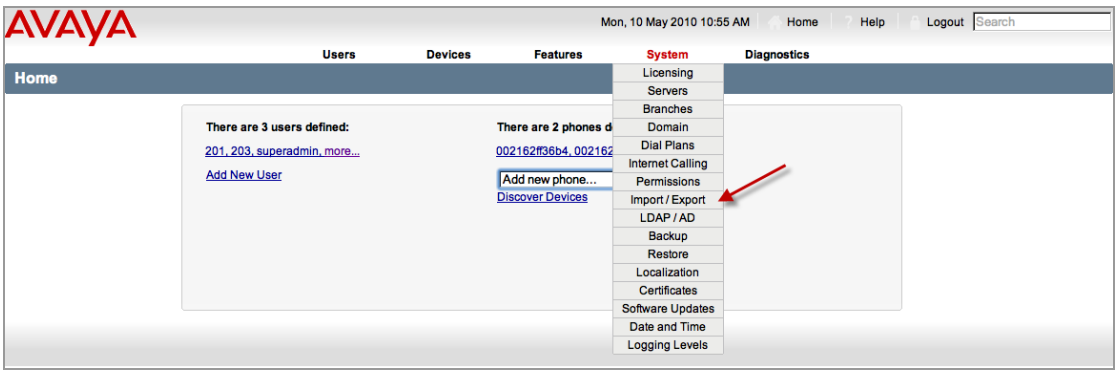
A useful habit to form early in the life of the SCS is that of regularly exporting the user database to a CSV file. An up-to-date CSV record of all user profiles (including associated phone types and MAC addresses) will prove invaluable should you need to recover the SCS and are without a recent Backup archive

or Programming Record. The SCS provides a simple Import/Export function that is capable of creating a CSV export in seconds.

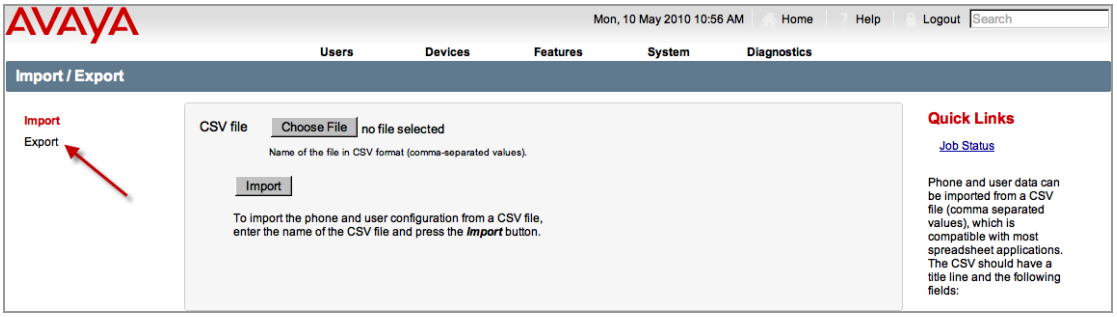
Always store the CSV export and the Programming Record in a safe place.

To create a CSV export from your current user profile and phone profile configuration:

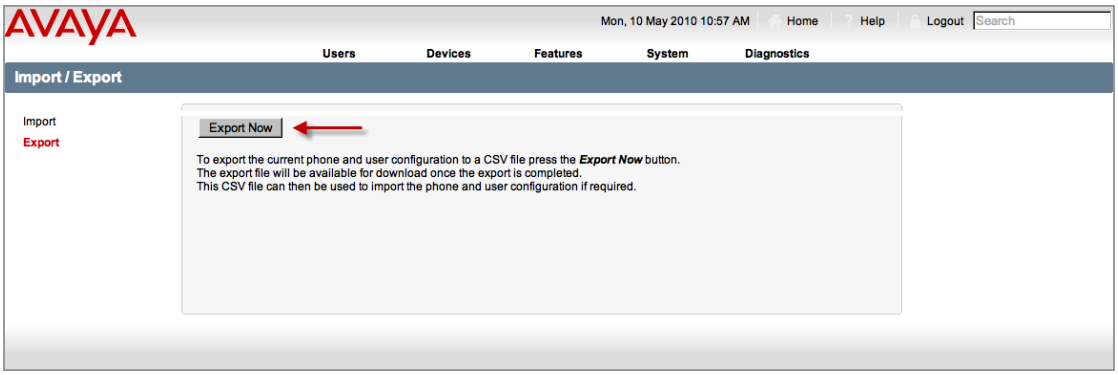
1. Place the mouse pointer over the **System Menu** and select **Import / Export**.



2. Click on **Export**.



3. Click the **Export Now** button.



4. When the export is complete, a file link is displayed. Click on the file link to open a Save dialogue.



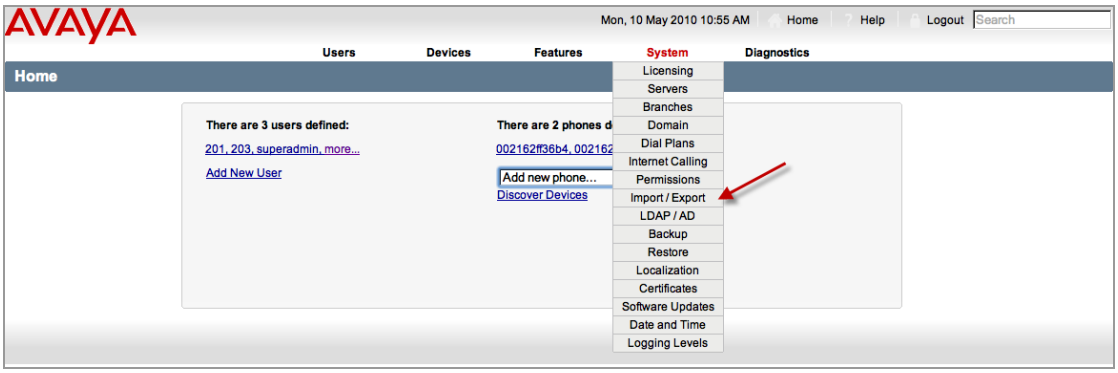
5. Follow your browser's Save instructions to save the export CSV to a suitable location.

6. Export to CSV is complete.

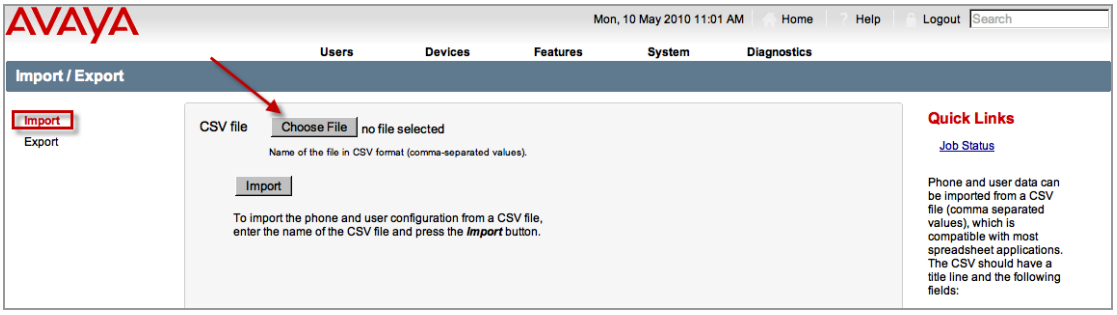
Importing from a CSV File

To import user profiles from a CSV file, log in to the SCS administrator account and then:

1. Place the mouse pointer over the **System** menu and select **Import / Export**.

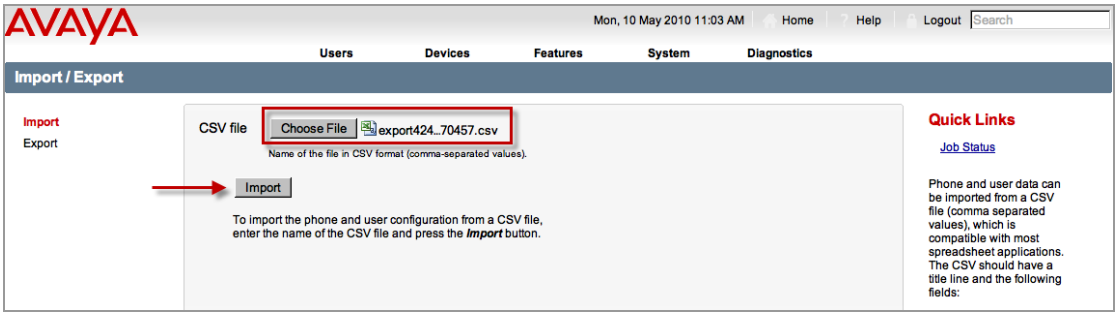


2. The Import/Export screen will automatically be at the Import option. Click on the **Choose file / Browse** button to navigate to the CSV file.

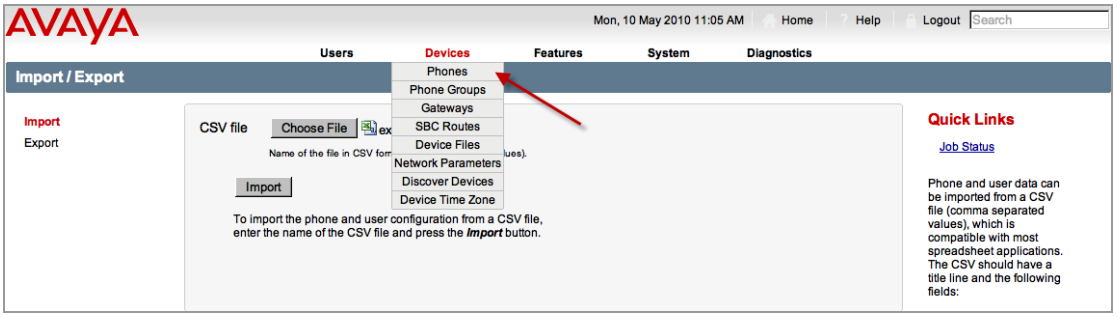


3. Click the **Import** button

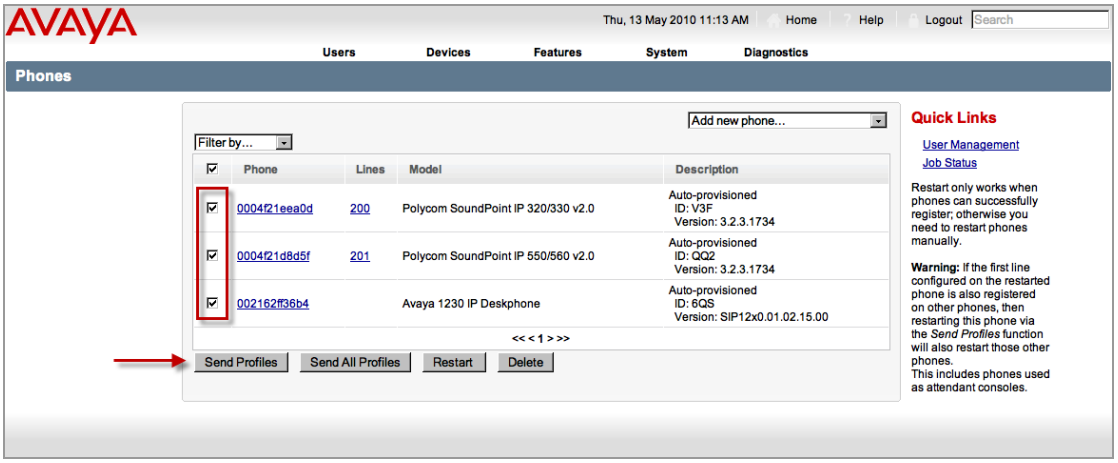
Note: To view the status of the import, open the **Diagnostics** menu and select **Job Status**.



4. Place the mouse pointer over the **Devices** menu and select **Phones**.



5. A list of all the phones added to the SCS is displayed. Using the check-boxes, select the phones imported from the CSV file.



6. Click **Send Profiles** to send user and configuration data to each phone.

Recovering the SCS System

System recovery might imply either of these courses of action:

- System restore, during which a backup archive is used to undo an unfavourable configuration change, or a system error.

- Complete system rebuild, during which the SCS server is formatted, the software is reinstalled and reconfigured, and any backup archives are restored.

The coming sections will deal with both of these scenarios, guiding you through the process of recovering not just the SCS system, but also all services. Because not all networks will have High Availability (HA) configured, rebuilding an HA system is treated as a separate topic to single server configuration.

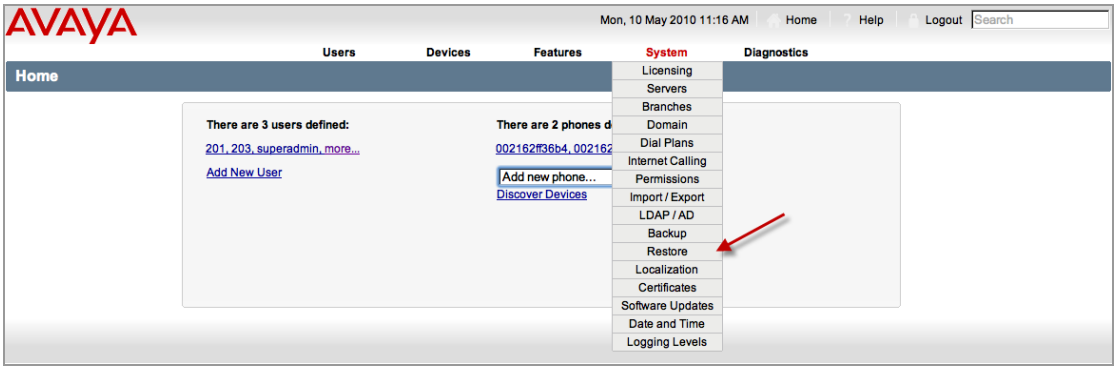
System Restore

Note: Archive restoration can only be performed on exactly the same hardware and software version.

Sometimes it may be the case that you need to return the SCS to a previous configuration. If a regular backup schedule is in place, then system restoration should be a simple matter of importing the archive through the SCS's Restore function. If regular backups are not a feature of your IT policy then you may have to resort to the SCS Programming Record. If the Programming Record has not been completed, then it may be necessary to perform a complete system rebuild, which is covered later in this guide.

Working on the assumption that you have a recent backup archive to hand, you can use it to restore your configuration in the following way:

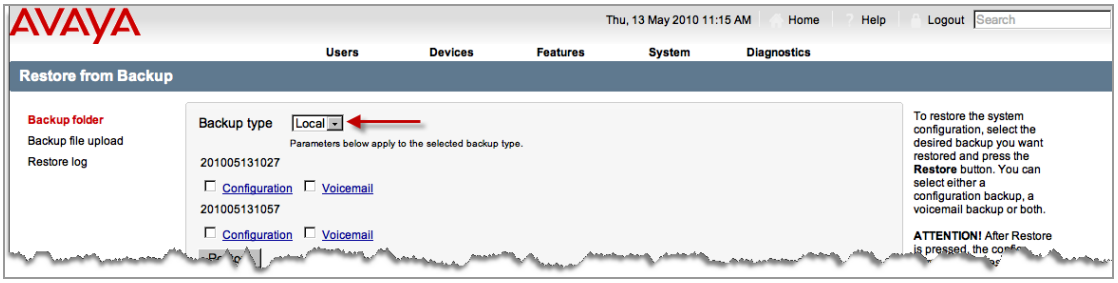
Open the **System** menu and select **Restore**, then choose between an 'archive' restore (using the SCS's own backup archive), an 'upload' restore (using backup files from your secondary location), or an FTP upload.



Restoring from the Server Archive

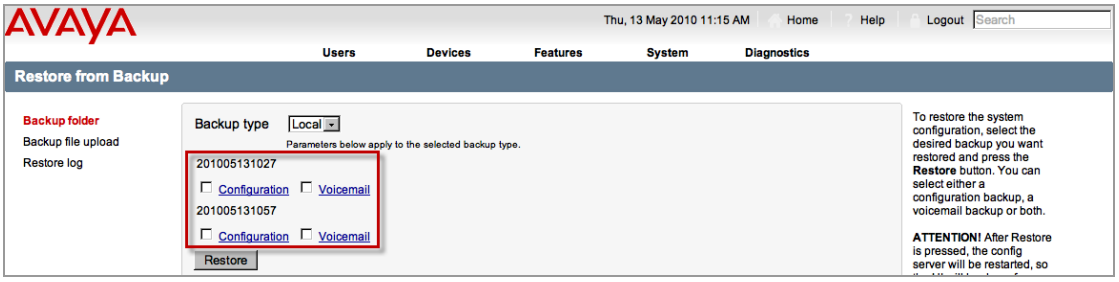
1. By default, when you open the restore window you have the option of restoring from the local archive store on the SCS or your chosen FTP server. Use the drop-down menu to select **Local** or **FTP**.

   To restore from another source, click on the **Backup file upload** menu option on the left-hand side and follow the instructions found in the following section, 'Restoring by File Upload'.



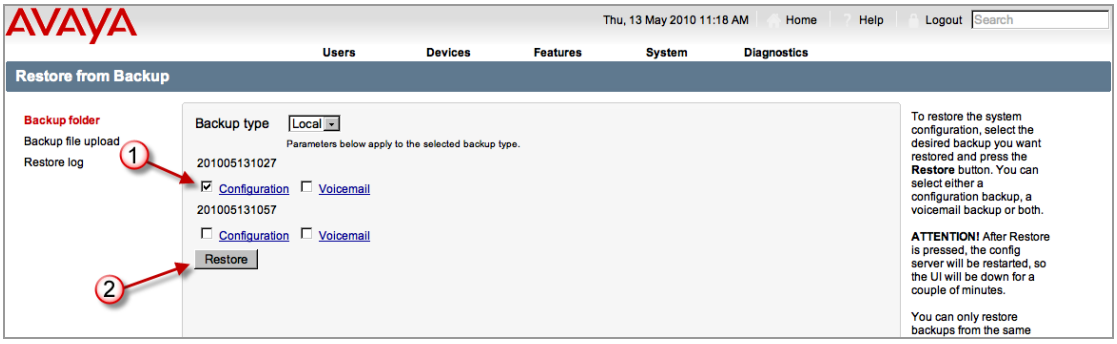
2. The screen is populated by a list of configuration dates and associated archives.

   If you selected FTP in step 1 you may have to configure FTP settings in order for your files to appear. In this instance, click on **Show FTP Settings** to configure server name, username and password values, and then click **Apply**.



Note: Any of the backup files listed on this page can be saved to another location by clicking on the relevant link, e.g., **Configuration** or **Voicemail**.

3. Select the archive you would like to restore by ticking the corresponding check-box.



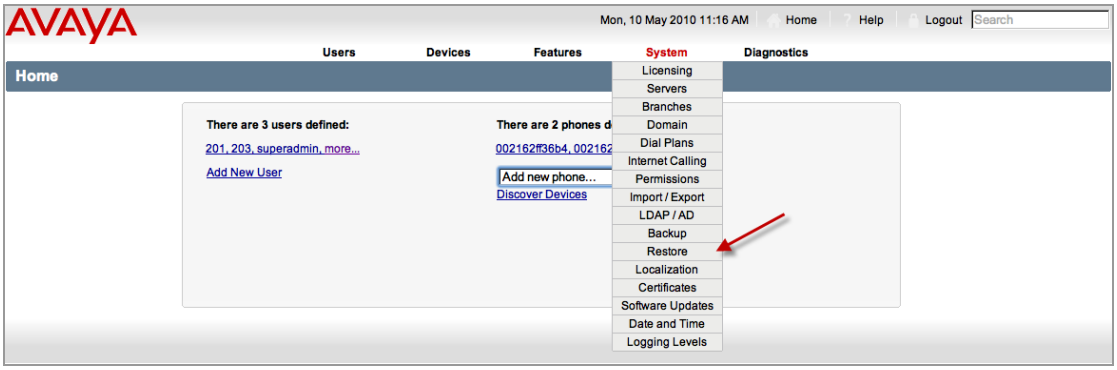
4. Click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

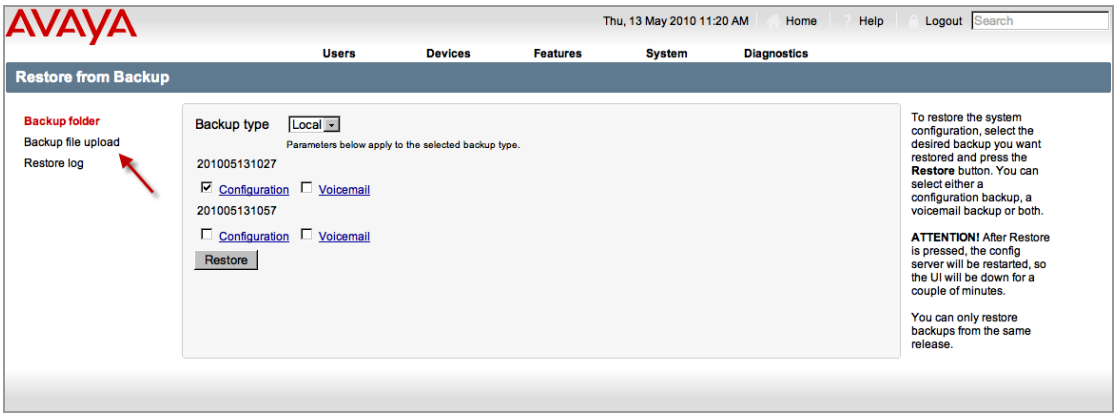
Restoring by File Upload

In the absence of an FTP server, it is still possible to save backup archives to a secondary location for safe keeping. To restore archives from this secondary location follow these steps:

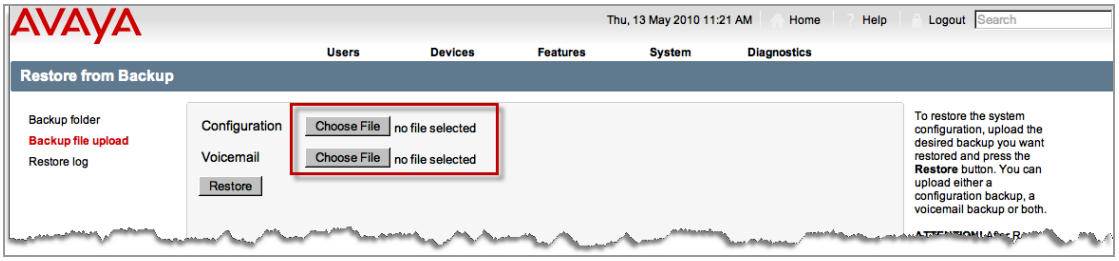
1. Open the **System** menu and select **Restore**.



2. Click on **Backup file upload**.



3. To restore a Configuration file, click on the corresponding **Choose file / Browse** button, to restore a Voicemail file, click on the corresponding **Choose file / Browse** button.



Note: the interface will display an error message if you attempt to enter a voicemail file in the **Configuration** text box and vice versa.



4. When you are ready to continue, click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

System Rebuild (without High Availability)

Note: Before formatting the SCS server, ensure that you have saved any important data such as voicemail backups and user profile lists.

Formatting the Server and Reinstalling the SCS Software

If the SCS server fails it may not be enough to simply restore an earlier configuration backup. In such circumstances a server 'rebuild' will be necessary to recover the system. Once the system has been recovered, a configuration restore can be performed to restore all previous settings.

The following instructions will guide you through these processes:

- Creating a bootable SCS installation CD
- Formatting the SCS server
- Reinstalling the SCS software
- Configuring LAN settings on the SCS server

If the system you are attempting to rebuild was configured with High Availability (dual server fault tolerance and load balancing), please see the 'System Rebuild (with High Availability)' section of this guide.

Creating an SCS Installation Build

Before you can configure your SCS server you will need to download and install the SCS software. You will need:

- Internet access
- Writable DVD/USB thumb drive
- DVD burning software capable of creating a bootable DVD from the ISO image – for example *Infra Recorder*.

Downloading the SCS ISO File

The SCS software is contained in an ISO file, which can be obtained from the Avaya website at http://support.avaya.com. Once downloaded, the ISO file should be burnt to a DVD using a DVD burning package that is capable of creating bootable discs, or written to a bootable USB thumb drive.

Burning the ISO File to DVD

Once you have downloaded the ISO file to a suitable location, you must burn it to a DVD. The DVD will then be used to format the server and install the SCS software. For this reason, it is not enough to simply copy the file to a DVD. The file must be burnt to the DVD and the DVD must be made **bootable** using a disc burning application – such as *Infra Recorder*.

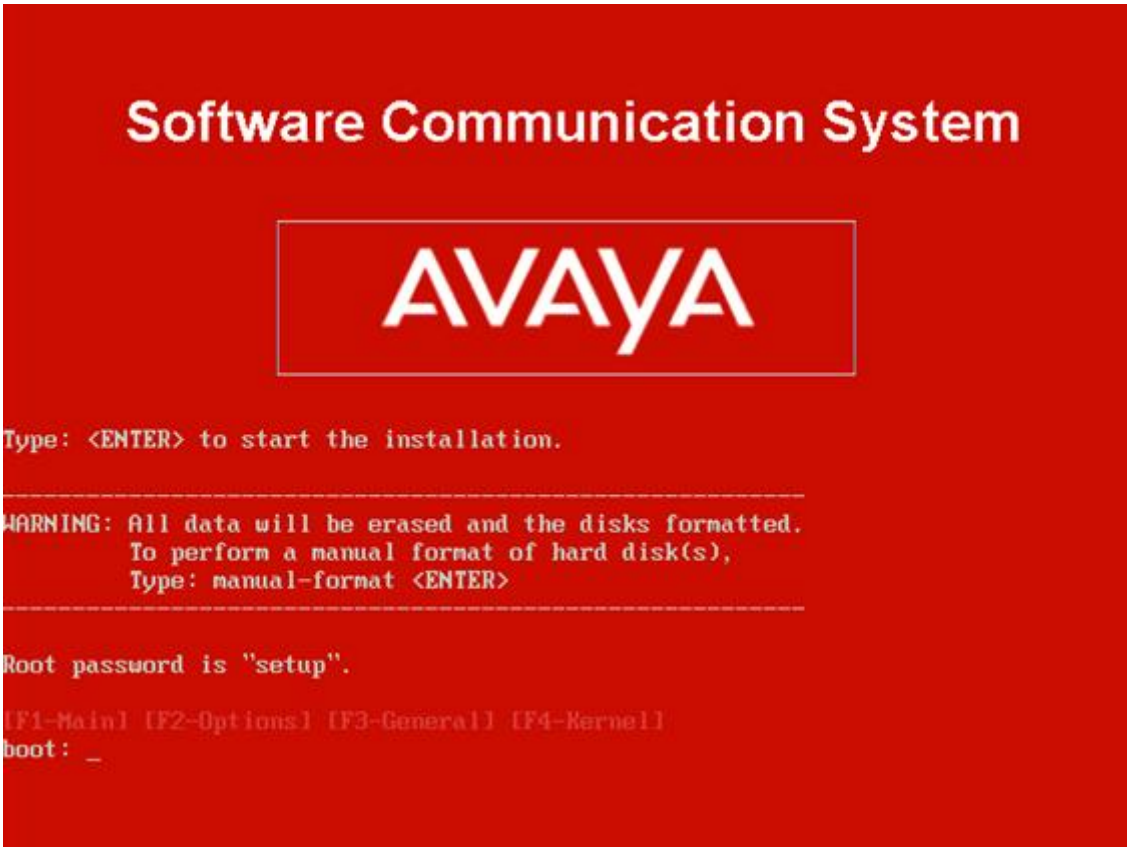
Note: Alternatively, you can copy the SCS installation file to a USB drive and boot from that. See 'Creating a Bootable USB Image'.

In order to install the SCS software you might need to configure the boot settings so that the server reads the CD drive at power up. This is achieved in the following way:

Note: If your server already boots from the CD drive, simply place the installation DVD in the CD tray, close it and reboot the system.

1. Press the **Power** button to switch the server on.
2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.
3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.
4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.
5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **Onboard or USB CD-ROM Drive**.
6. Use **U** to move it to the top of the list (if the CD-ROM drive is already at the top of the list ignore this step).
7. Press the **Enter** key.
8. Open the CD-ROM tray and insert the SCS installation DVD.
9. Close the tray.
10. Press the **ESC** key to exit System Configuration.
11. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
12. Press the **Enter** key.

The server will reboot from the DVD and automatically launch the format utility. When the Software Communication System screen is displayed, press the **Enter** key to confirm that you would like to format the hard drive and install the SCS software.



The format and installation process takes approximately 10 minutes, when it is complete the CD tray will eject and the system will reboot to the login screen, from where you can begin the installation process. Continue to 'Configuring LAN and SIP Settings' for guidance on configuring the server.

Creating a Bootable USB Image

Instead of creating a bootable installation DVD you could instead create a bootable USB image. This will involve:

- Writing the SCS ISO image to a 'bootable' USB thumb drive using an application called *ISO2USB*, which can be obtained at http://iso2usb.sourceforge.net
- Re-ordering the boot sequence of the Dell server.

Note: The USB thumb drive must have a capacity of 1GB or more.

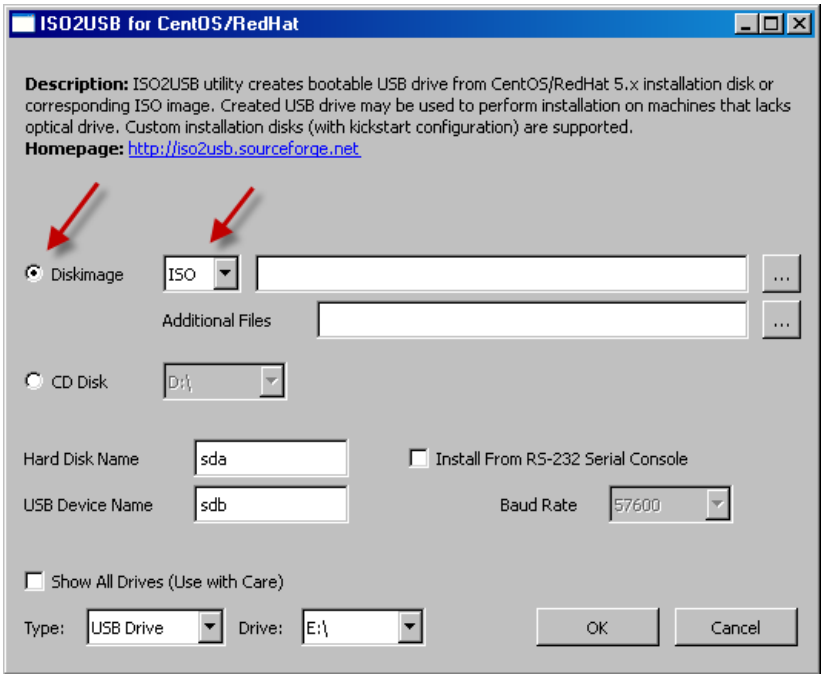
To create a bootable USB drive:

1. Insert a USB thumb drive (ensure that you this is a drive that has no important data on it).

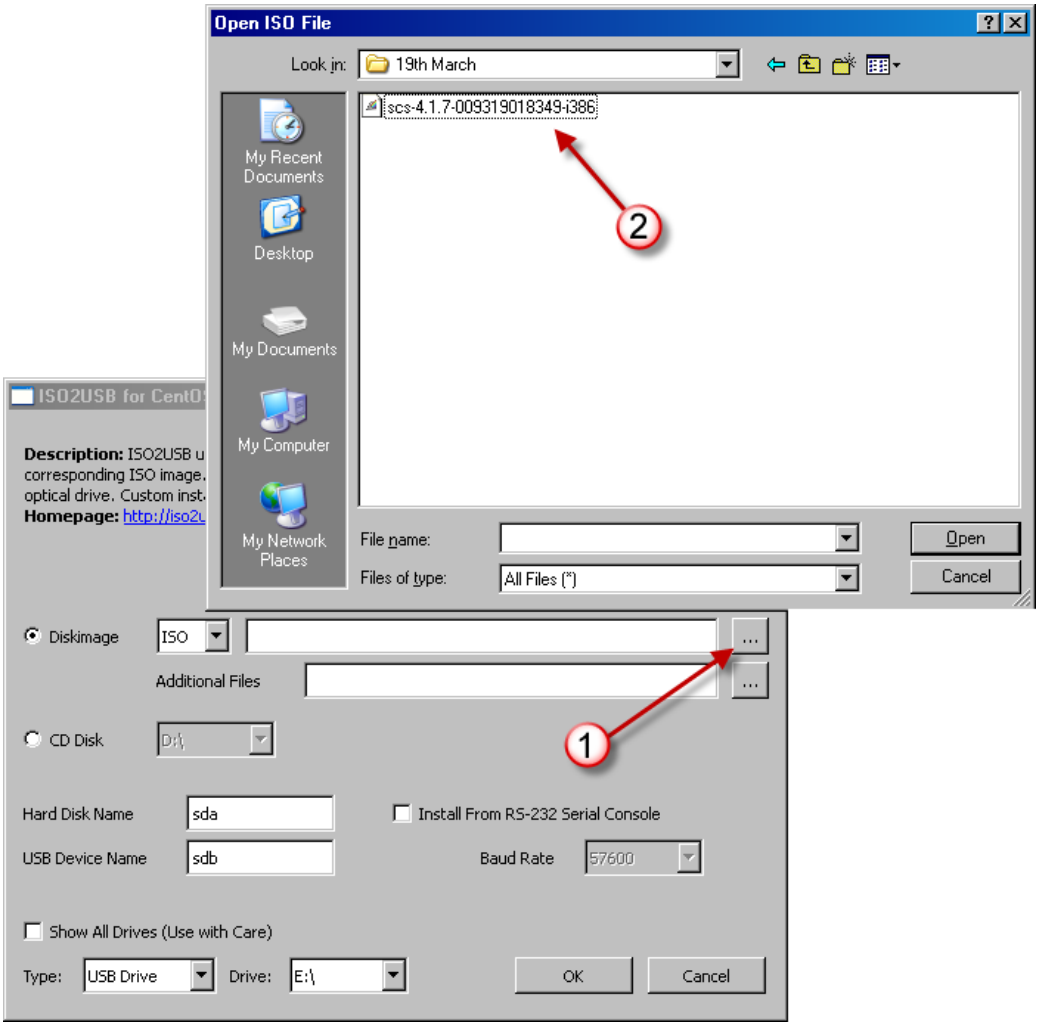
2. Download *ISO2USB*.

3. The package downloads as a ZIP file. Extract the contents and then double-click on **iso2usb.exe** to launch the application.

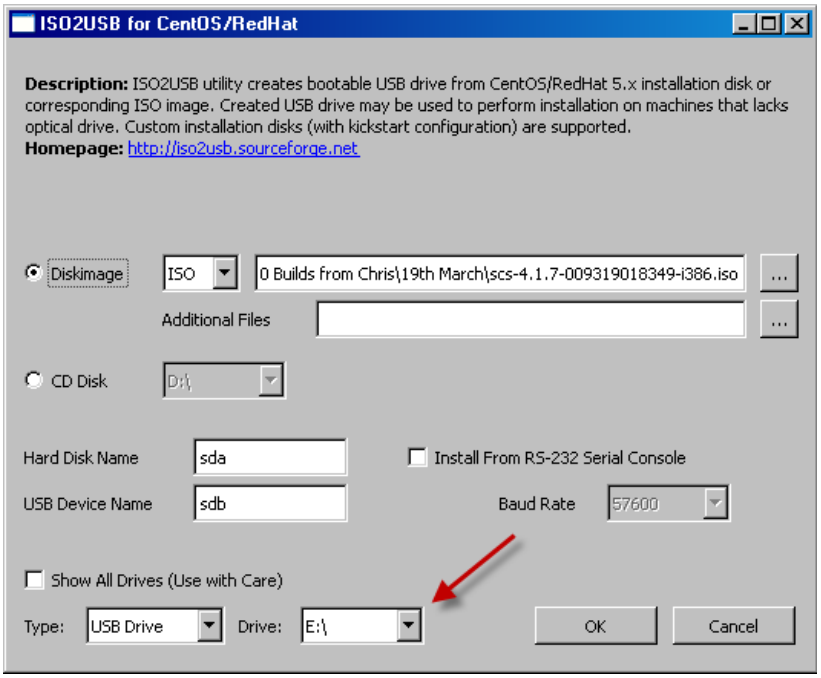
4. Ensure that the **Diskimage** radio button is selected and that **ISO** is selected in the top drop-down menu.



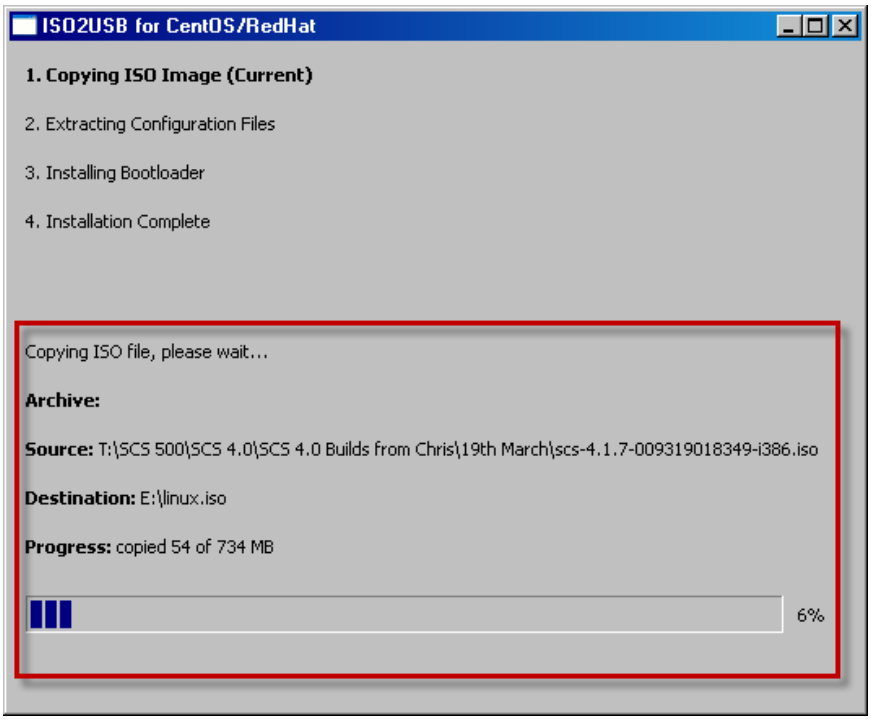
5. Navigate to the location of the SCS ISO image and select it.



6. Select the USB drive from the **Drive** drop-down menu at the bottom of the window and then click **OK**.



7. The image is written to the USB drive.



8. When copying is complete, click the **Exit** button.

You have now created a bootable SCS installation USB drive. Next re-order the boot sequence on the server.

In order to install the SCS software you will need to configure the boot settings so that the server reads the USB drive at power up. This is achieved in the following way:

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **USB Device**.

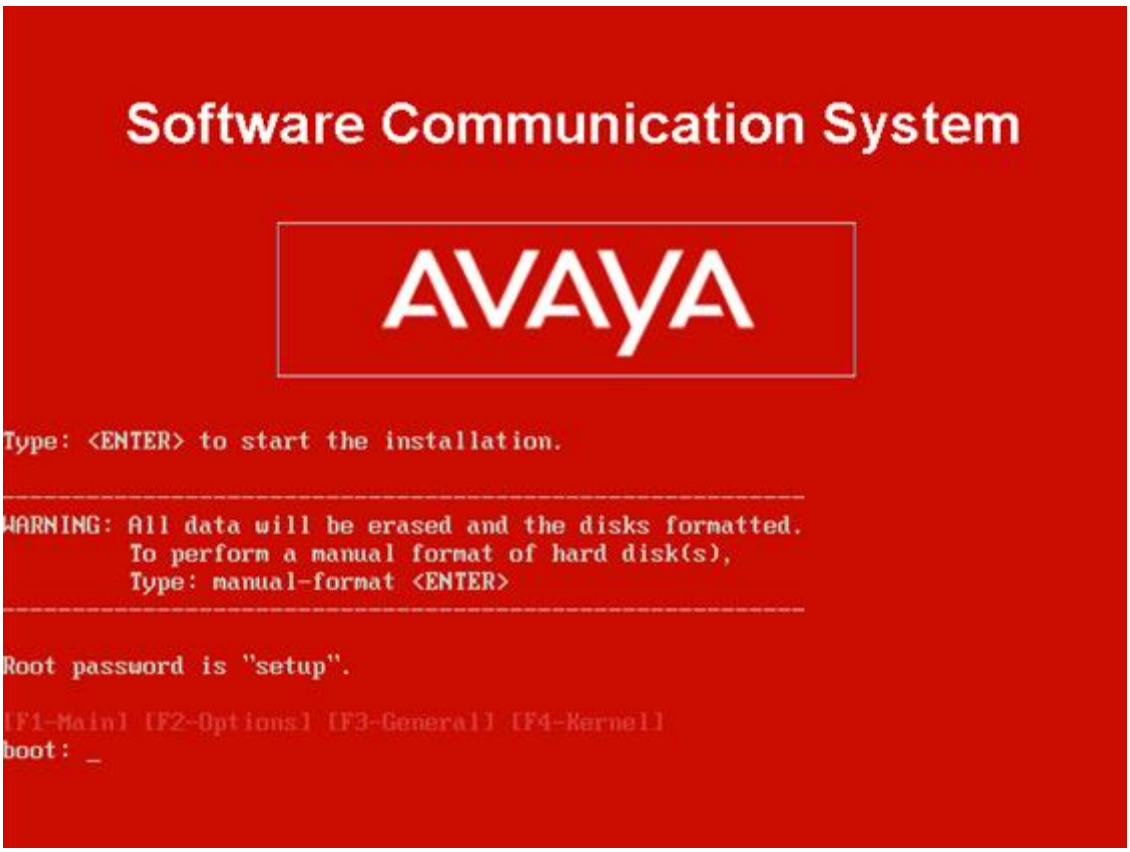
6. Use **U** to move it to the top of the list

    a. On some servers it may be necessary to ‘enable’ the USB device as a boot option. Press the **Space** bar if **USB Device** does not have a priority number next to it. A ‘**1**’ should appear next to the drive.

7. Press the **Enter** key.
8. Insert the USB thumb drive
9. Press the **ESC** key to exit System Configuration.
10. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
11. Press the **Enter** key.

The server will reboot from the USB drive.

When the red Avaya screen is displayed press **Enter**.



A ‘kickstart’ error will be displayed, this is normal. Simply use the **down** cursor key on your keyboard to highlight the **OK** button and press **Enter** to launch the format utility. When formatting is complete the SCS software will be copied to the server’s hard drive.

The format and installation process takes approximately 5 minutes, when it is complete the system will announce a reboot – **Ensure that the USB drive is removed from the USB port before the reboot begins otherwise the system will reboot from the thumb drive again**. If you are unable to remove the USB thumb device before the system reboots, wait for the red Avaya

screen to appear, remove the thumb drive and then **press CTRL-ALT-DEL** to reboot the server.

The system will boot to a login screen

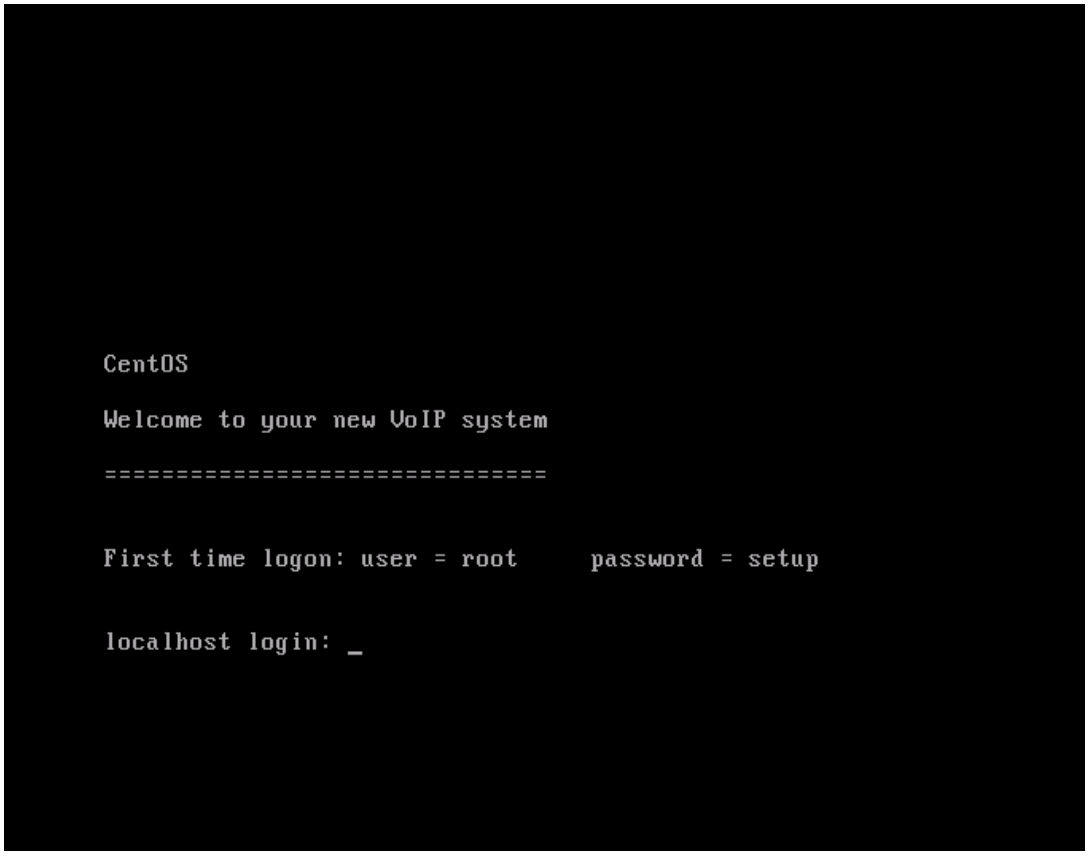
Configuring LAN and SIP Settings

Note: Ensure that the SCS server has a physical connection to the host network before you begin the configuration process; this is required during installation because the server will search for NTP servers on the Internet when you come to set system time. If there is an NTP server within the network that you would rather use, ensure that the SCS is connected and can 'see' this server.

When powered on for the first time, the SCS server boots to the CentOS login screen.

1. To begin the setup process, enter the following username and password to access the configuration utility:

   Localhost Login: `root`
   Password: `setup`

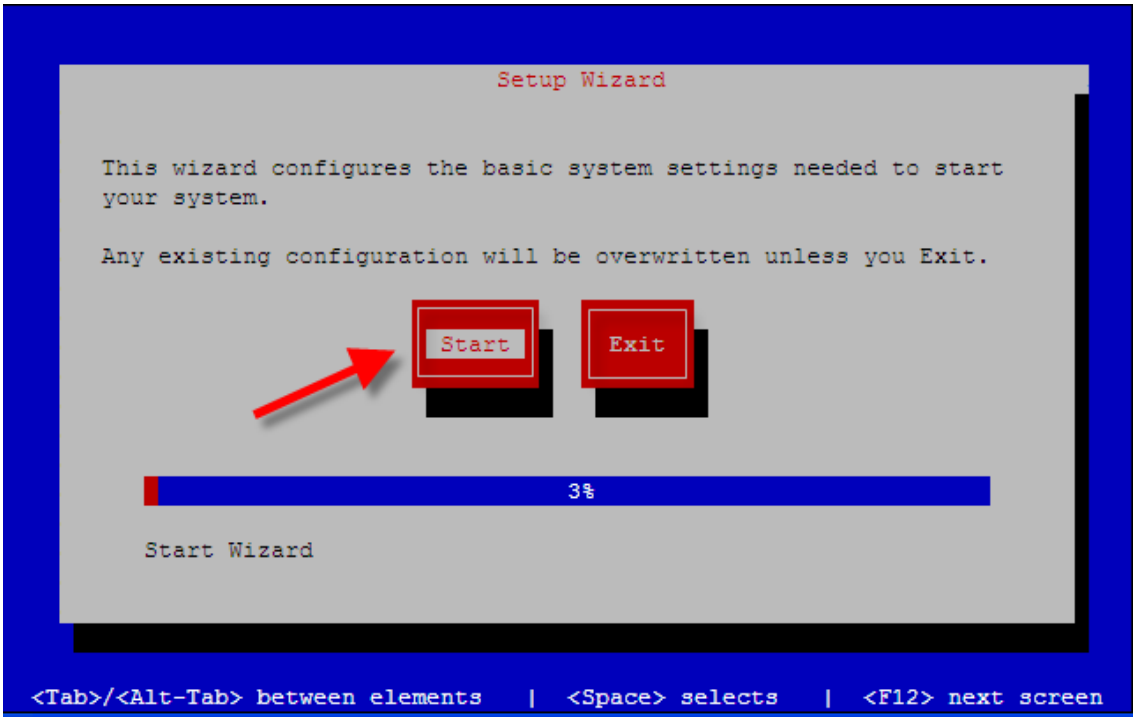


   If at any time during the setup process you make an error, reboot the server and log in using the same username and password. At the

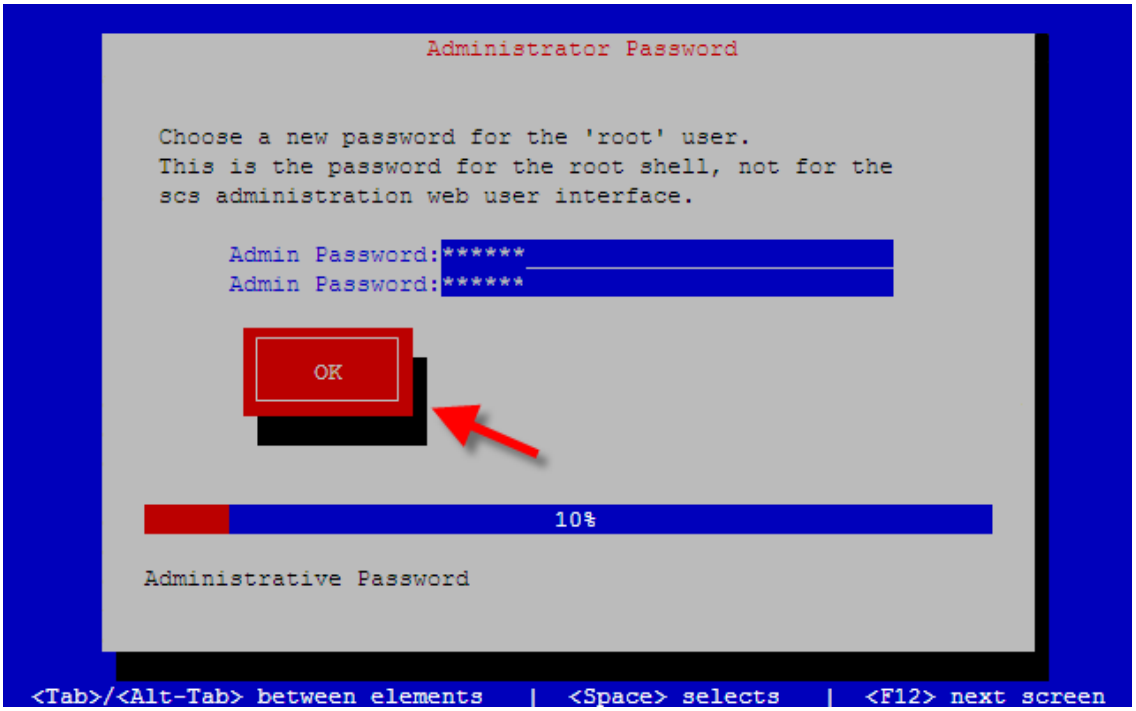
command prompt type **`sipxecs-setup-system`** and press **Enter** to reload the configuration utility from the start.

Note: The SCS domain cannot be changed by running sipxecs-setup-system. The only way to reconfigure the domain is to access the **Domain** facility from the administrator GUI.

2. When the configuration utility has finished loading, highlight the **Start** button and press **Enter**.



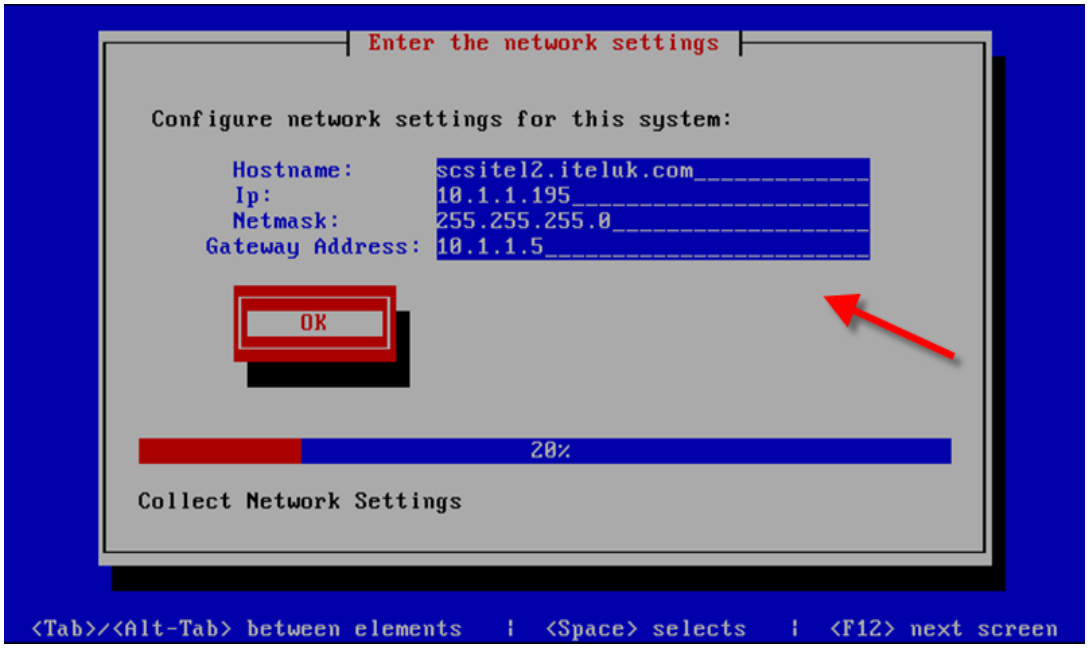
3. Enter the **Admin Password** twice. This is the password that engineers and administrators will enter to gain access to the SCS server locally via the Linux operating system (where you are now). Highlight the **OK** button and press **Enter** when you are ready to continue.



4. Enter the following LAN settings:

    a. **Hostname** – This is the fully qualified domain name (FQDN) of the SCS server as defined in the DNS records.
    b. **IP** – The IP address that has been assigned for use with the SCS. Again, this must be consistent with the address defined in the DNS settings.
    c. **Netmask** – The network's subnet mask.
    d. **Gateway Address** – The address of the default router providing access to the Internet.

    If you are unsure of any of these settings, see the network administrator.



5. The installation wizard will now query whether or not you have DNS configured on the network. The SCS can be configured to function as a DNS server on the network if you do not have DNS or are unable to configure the required records. To enable the SCS onboard DNS, select **No xxx.xxx.xxx should be my DNS server**.

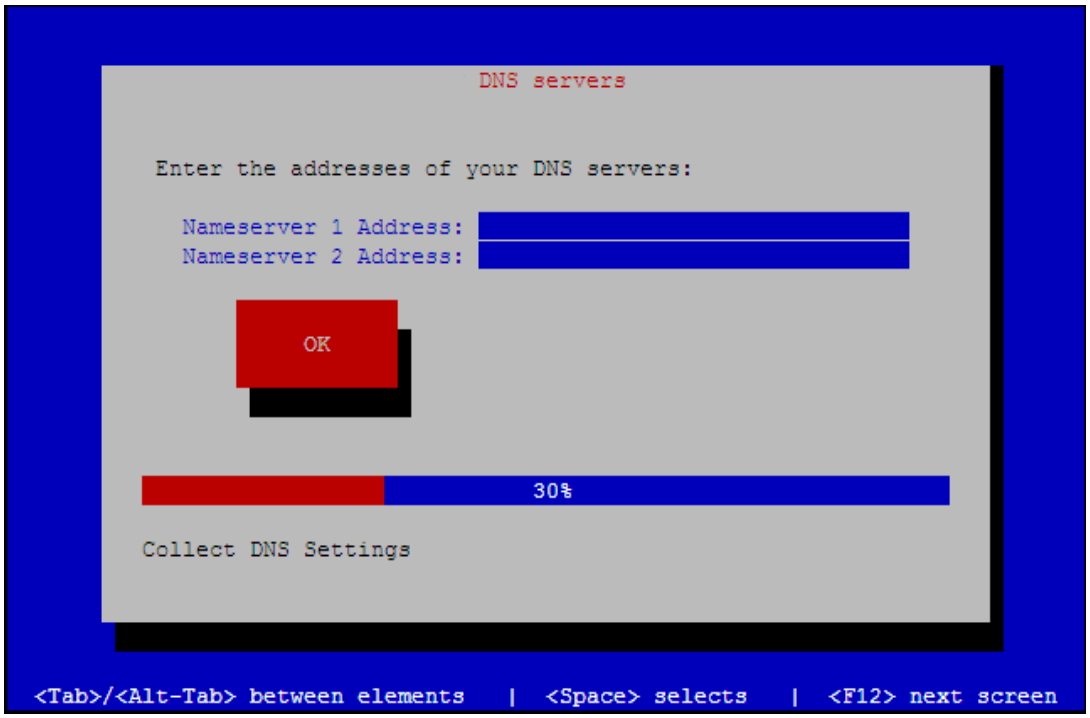
Note: The onboard DNS service automatically configures all required A Records and SRV records. This means you will not have to define a fully qualified domain name when it comes to configuring the SIP domain later in the installation process.

Note: The DNS service will replicate on the secondary server if you choose to add a High Availability fault tolerance server later.

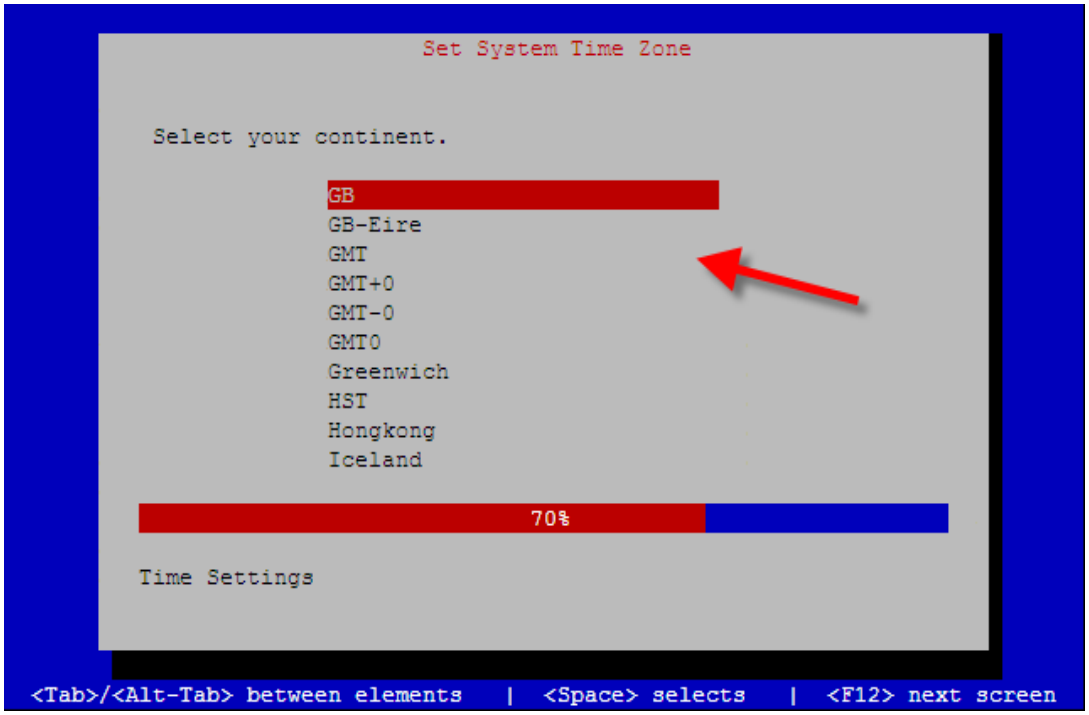
Note: If you elect to enable the SCS's onboard DNS the next screen will offer you the opportunity to define upstream DNS servers if you wish. If the network utilizes Intranet DNS or DNS from an IP service provider then these server addresses can be entered on the next screen. Note that this is an optional configuration step and the fields can be left blank if required, however without these addresses, name and address resolution may prove difficult since the SCS will not be able to resolve *all* DNS queries..



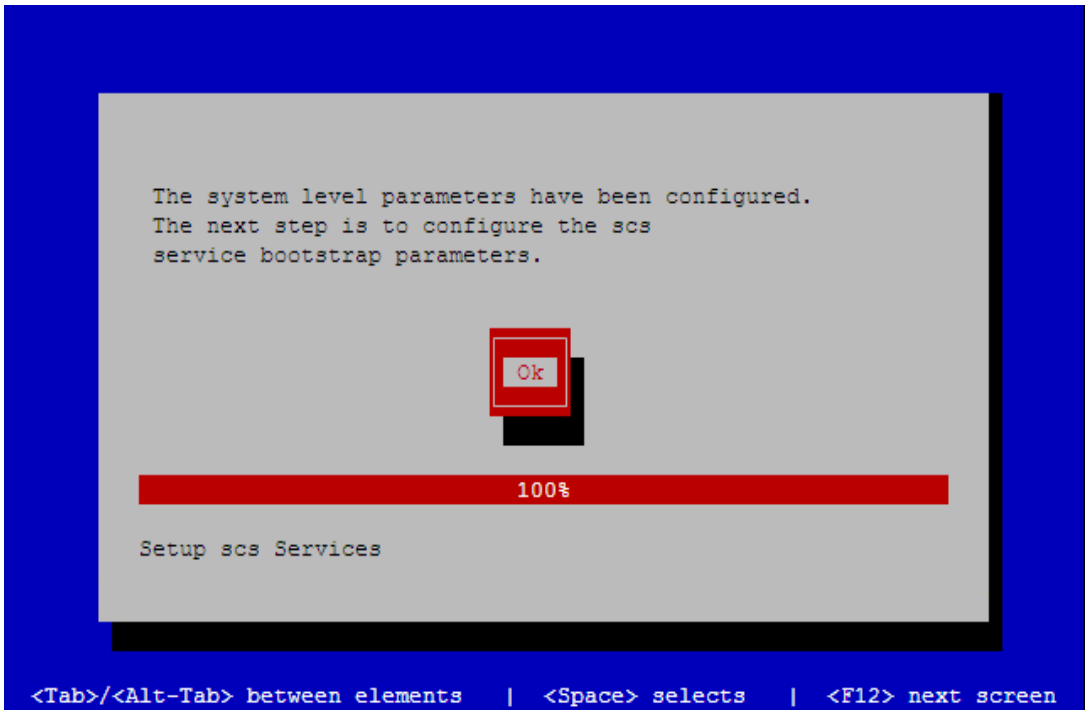
If you already have DNS configured for the SCS select **Yes**. Note that in this instance the next screen will ask you to configure the address of the primary and secondary DNS server.



6. Select a region or country to set the time zone in which the SCS is situated – if you pick a region, such as ‘Europe’, you will be prompted to then define an area within that region, for example, ‘London’.



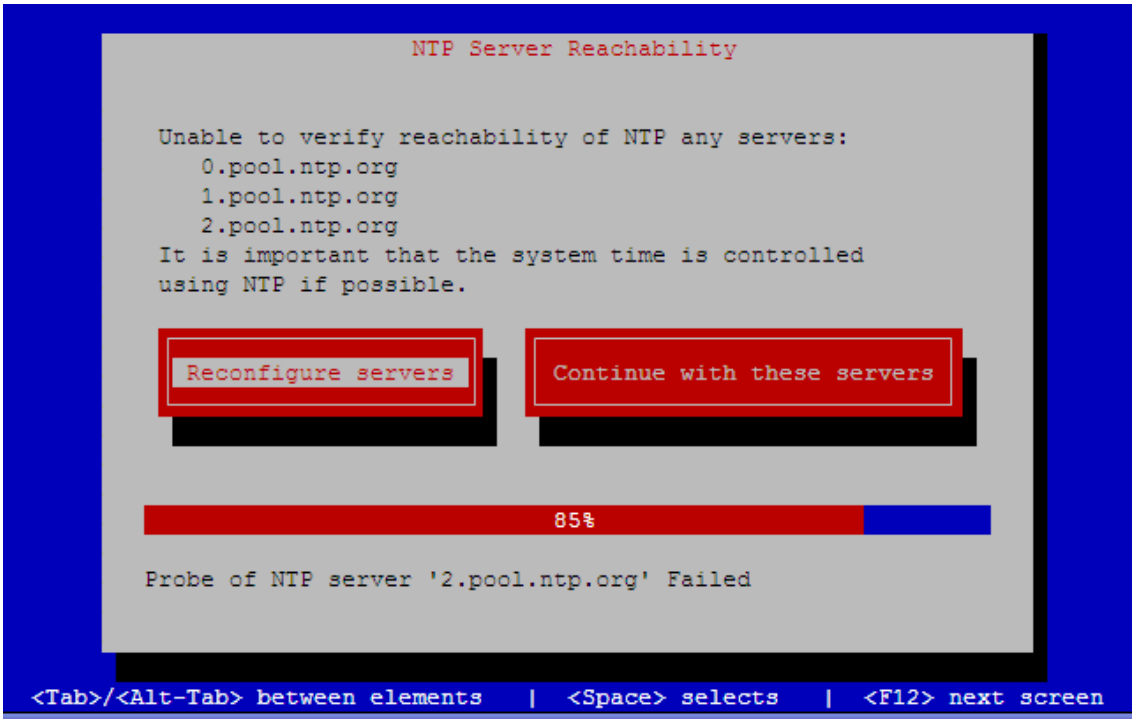
7. The system will now search for NTP servers in order to set system time. By default the SCS is programmed to attempt a connection to a series of Internet-based time servers – an internet connection is required for this stage of the configuration. If the SCS is unable to connect to any of these servers you will be asked to either: 1) move on with the current time server configuration, in which case you will have to set the time manually - see Step 7b; 2) configure the address of a different time server. If the SCS successfully gathers NTP data the following message will be displayed:



Press **Enter** and continue to Step 8 if you see this message.

Note: The NTP server search can take a while. Do not power off or disconnect the SCS during this process, even if it seems that nothing is happening.

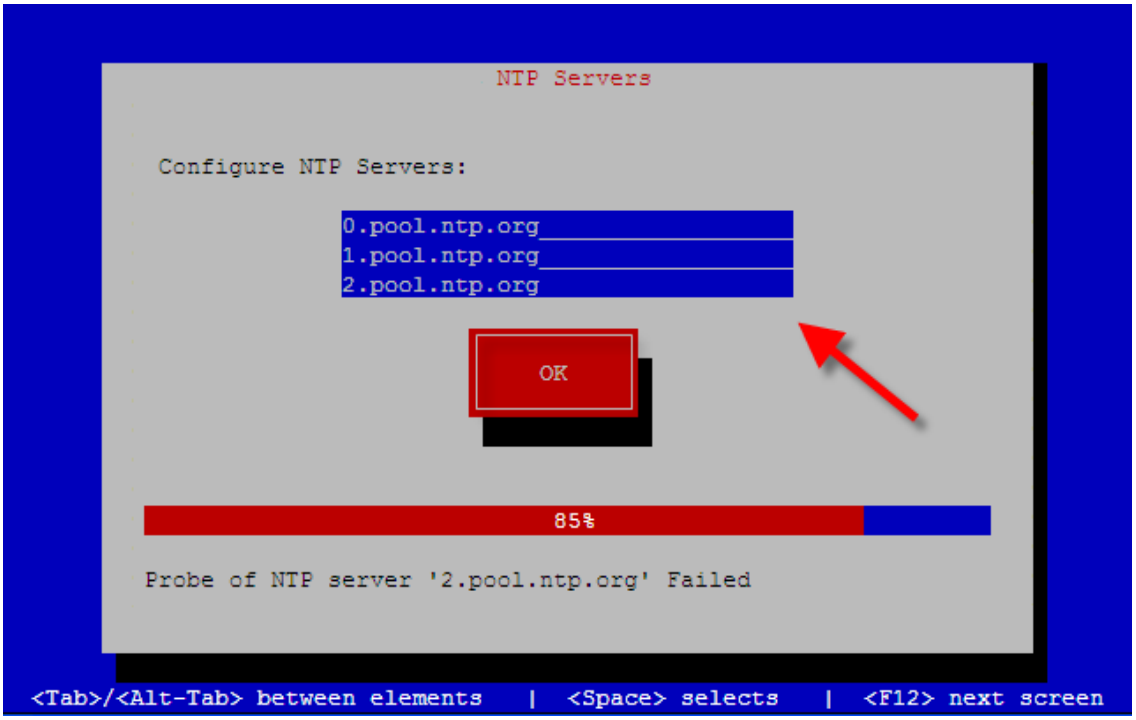
If you see the message below regarding NTP servers continue to Step 7a.



a. You now have the choice of configuring a different set of NTP servers or continuing with the default settings and configuring the time manually on the next screen.

    i. To set new NTP servers, highlight **Reconfigure servers** and press the **Enter** key.

    ii. Enter the new NTP addresses and then highlight the **OK** button and press **Enter**.



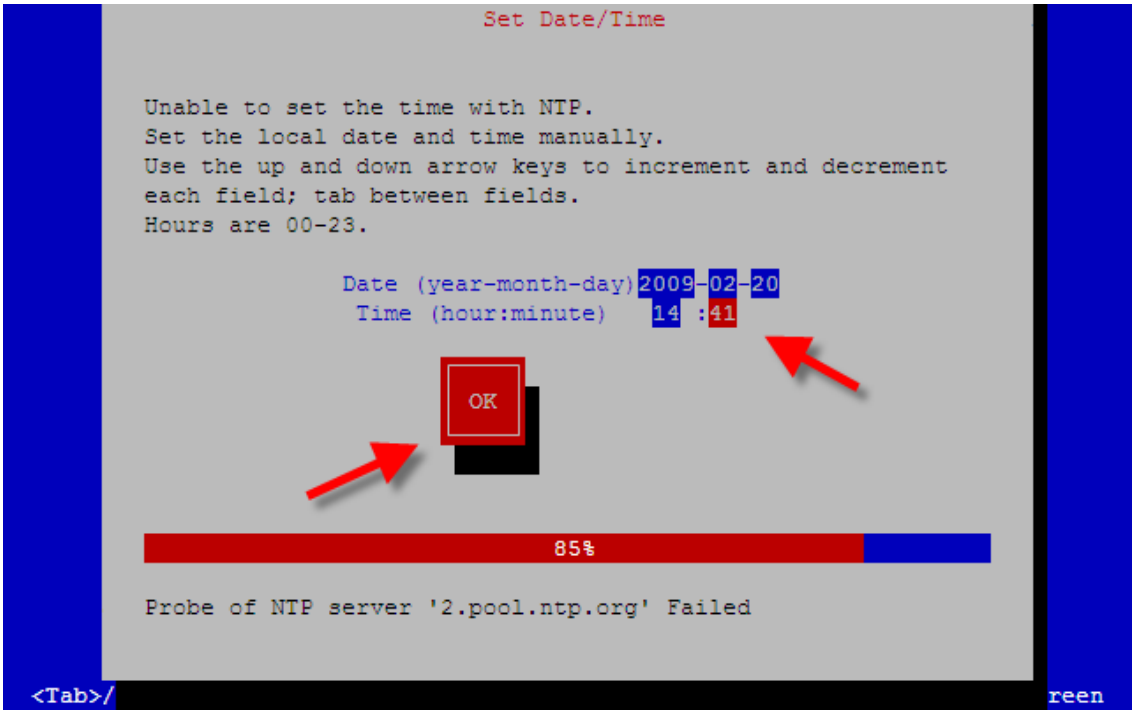
iii. The SCS will attempt to connect to the defined NTP servers.

iv. When a connection is successful press **Enter** to clear the confirmation screen and then continue to Step 8.

b. Instead of configuring alternative NTP servers you can set the time manually – **although the recommended course is to configure NTP**.

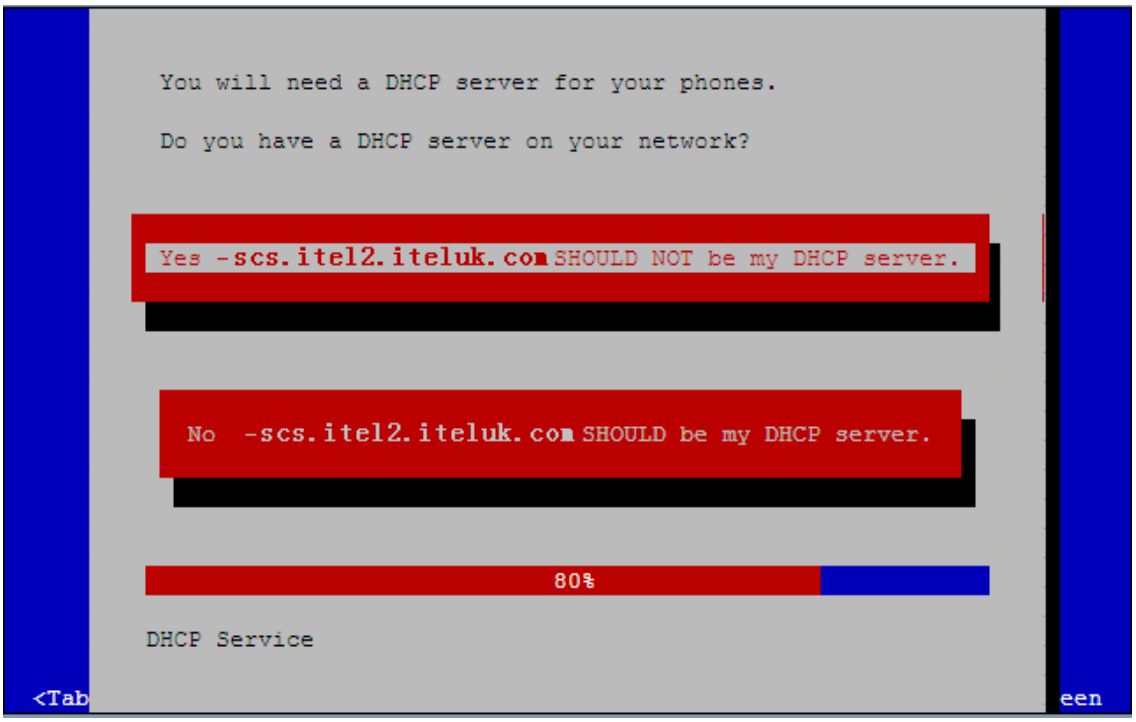
i. Highlight **Continue with these servers** and press **Enter**.

ii. To set the time, use the **left** and **right** cursor keys to move between the fields and the **up** and **down** cursor keys to adjust each value. The time should be set in 24-hour format. Highlight the **OK** button and press **Enter** to continue.



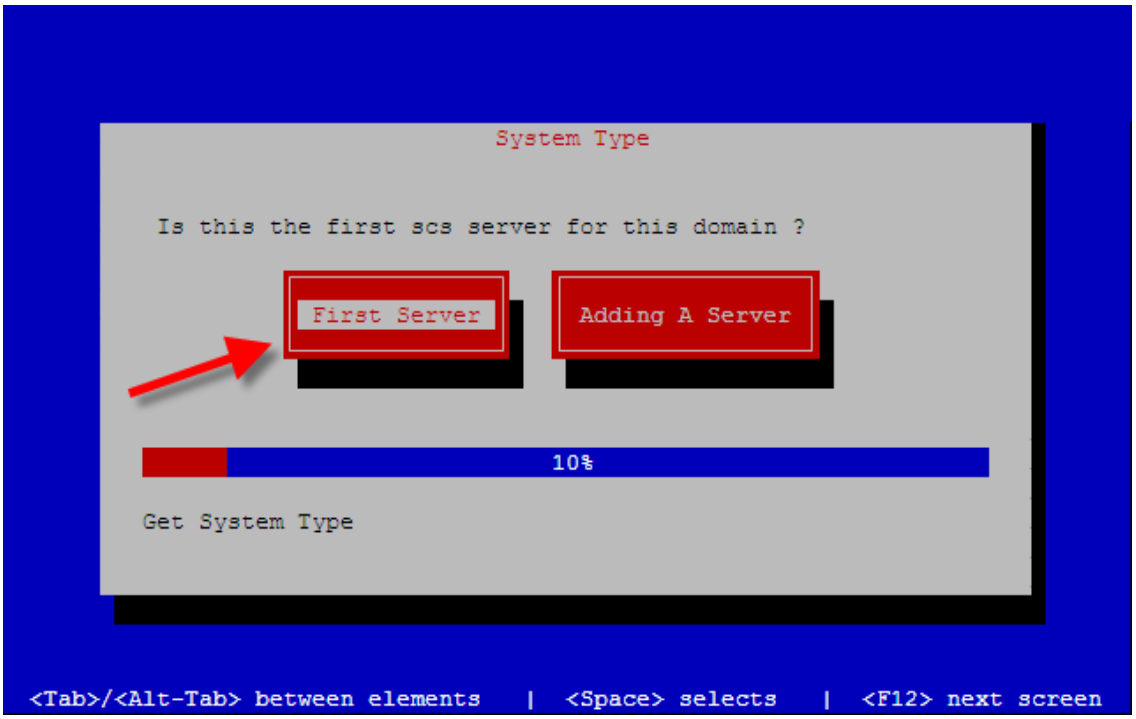
iii. Continue to Step 8.

8. The SCS can provide a DHCP service in order to provide devices joining the network with IP addresses. To enable the DHCP service select **No – xxx.xxx.xxx should not be my DHCP server**.



Note: If a DHCP service is already active on the network **do not** enable the onboard DHCP service since this will cause a conflict.

9. You now need to configure some settings that will define this server as your primary SIP server. First, define the server as your 'First Server'. Highlight **First Server** and press the **Enter** key.



10. Next set the SIP Domain. Knowledge of your network configuration is vital at this stage. You need to know how DNS is configured. Find out from the network administrator whether DNS **A Records** or **A Records *and* SRV Records** have been configured for the SCS. The presence or absence of SRV records determines the structure of the SIP domain:

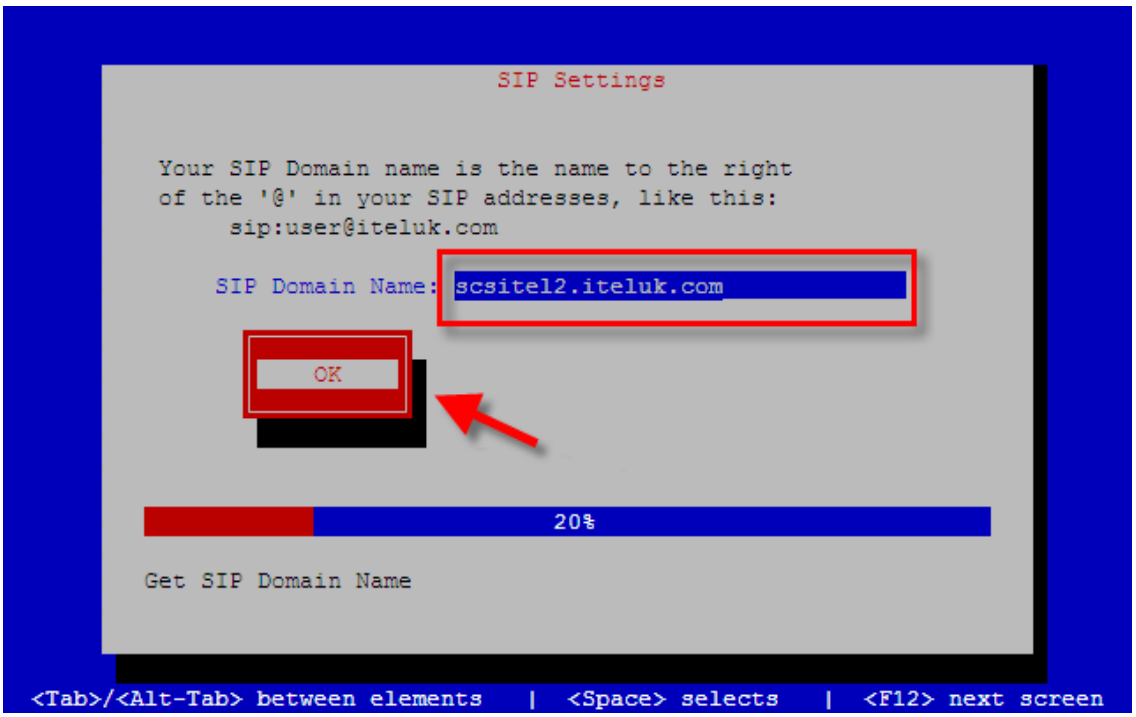
    If the DNS is configured with **just** A records you will need to include the SCS server name in the SIP Domain. If you look at the default entry you will see that the SIP Domain has been entered as just a domain name, e.g., *scsdomain.com*. This is insufficient if there are no SRV Records configured on the DNS server. **Therefore, if DNS is configured with only A Records, enter the host name *and* domain name of the SCS server (known as a fully qualified domain name). Example: *scshost.scsdomain.com*.**

    If DNS is configured with A Records **and** SRV Records you will **not** need to include the server name. Therefore, the default entry (pre-entered by the wizard) will be sufficient. This is because SRV records will automatically direct all SIP traffic within the domain to the SCS. **So, if SRV records exist the SIP domain will look like this**: ***scsdomain.com*.**

    In the example illustrated below I have included the SCS server name in the SIP domain because on my network we only use A Records.

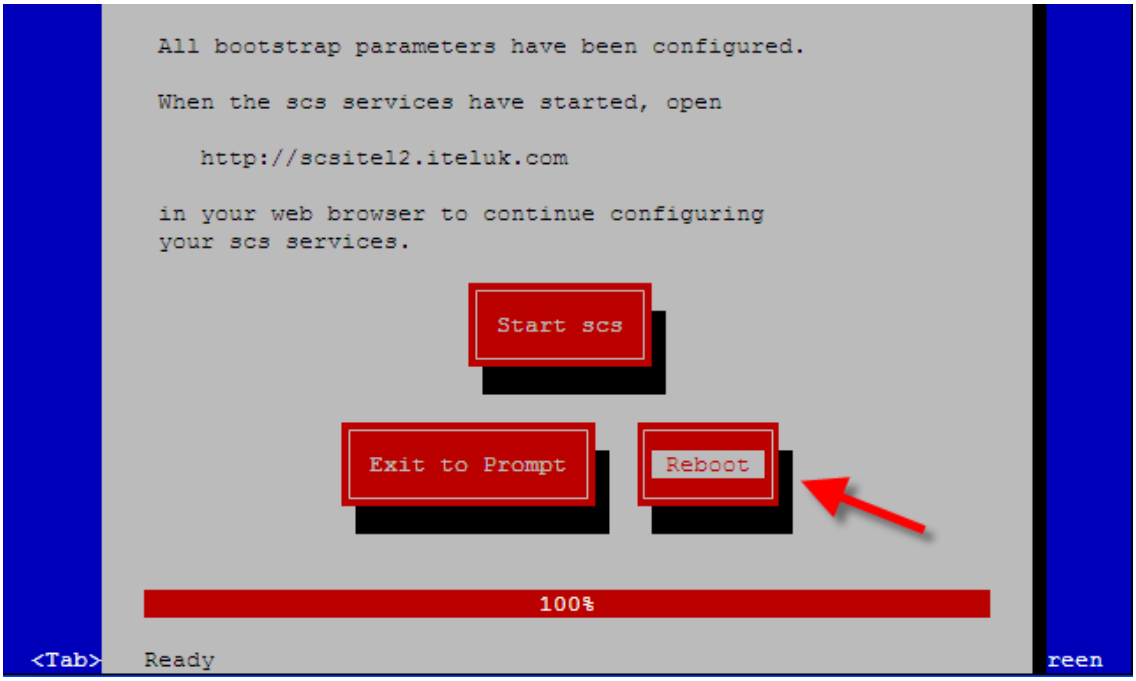
Note: If you elected to activate the SCS's own onboard DNS, SRV records will be created automatically, you should therefore leave the SIP Domain entry as the default entry.

Highlight the **OK** button and press the **Enter** key when you are ready to continue.



Note: Full instructions on how to configure Windows DNS for use with the SCS can be found in the 'Configuring DNS and DHCP for Windows Server 2003' guide

11. Configuration of the SCS server is now complete. Highlight the **Reboot** button and press the **Enter** key to restart the server.

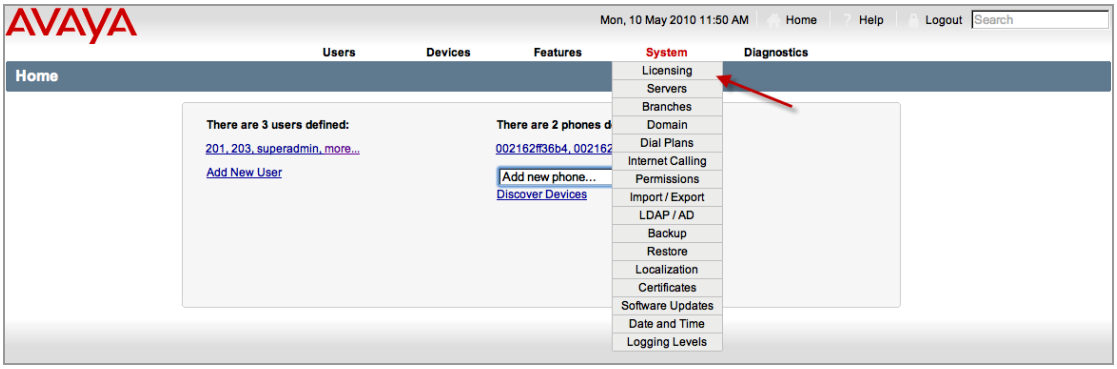


When the server has restarted, administration of the system can be carried out via the web-browser interface, which can be accessed from a remote workstation/laptop by navigating to the server's address or host and domain name in a web browser.

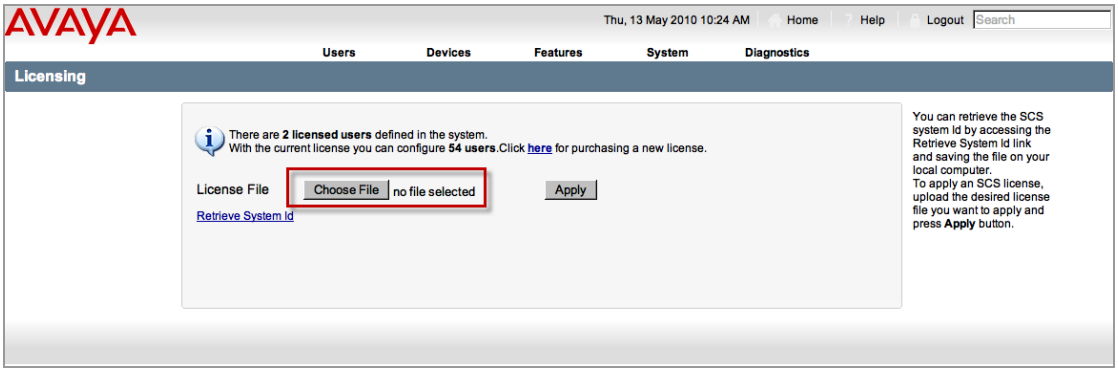
Activation and Restore

To quickly restore your configuration and voicemail backups, first log into the Administrator Interface (by opening a web browser and navigating to the IP address of the SCS server) and activate the system using your license code (the same license that was used for the previous build can be reused as long as you have reinstalled the SCS software on exactly the same hardware):

1. Place the mouse pointer over the **System** menu and select **Licensing**.



2. To apply your license file, click the **Choose file / Browse** button and browse to the location of the file. When you have selected a file, click the **Apply** button.



3. The license file will be applied to the SCS system, enabling the configuration of users based on the number of users purchased.

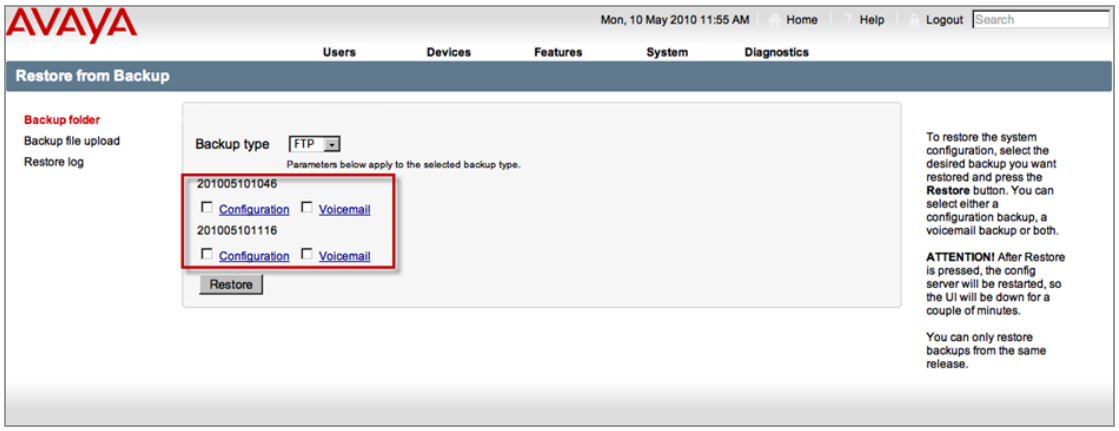
You are now ready to restore your configuration and voicemail backups. Backup archives can be restored from FTP sites, local storage, or an alternative storage medium.

Restoring from FTP

Note: The Restore function is version specific. Restore archives must be consistent with the installation version, i.e., you cannot restore files that were backed up using one SCS version to a later or earlier version.

1. By default, when you open the restore window you have the option of restoring from the local archive store on the SCS or your chosen FTP server. In this scenario the local storage no longer exists because the system has been rebuilt, so let's first look at the **FTP** option. Use the drop-down menu to select **FTP**.

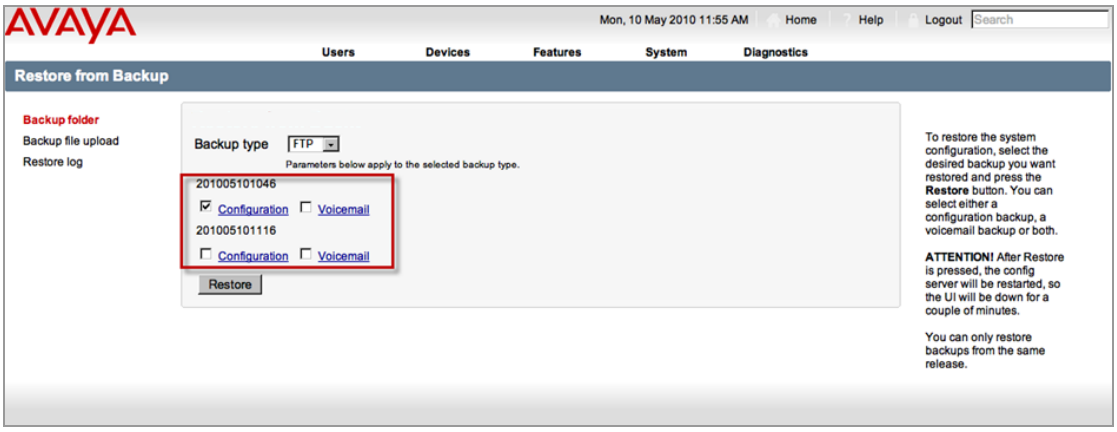
   To restore from another source, click on the **Backup file upload** menu option on the left-hand side and follow the instruction found in the following section, 'Restore by File Upload'.



2. The screen is populated by a list of configuration dates and associated archives.

You may have to configure FTP settings in order for your files to appear. In this instance, click on **Show FTP Settings** to configure server name, username and password values, and then click **Apply**.

3. Select the archive you would like to restore by ticking the corresponding check-box.



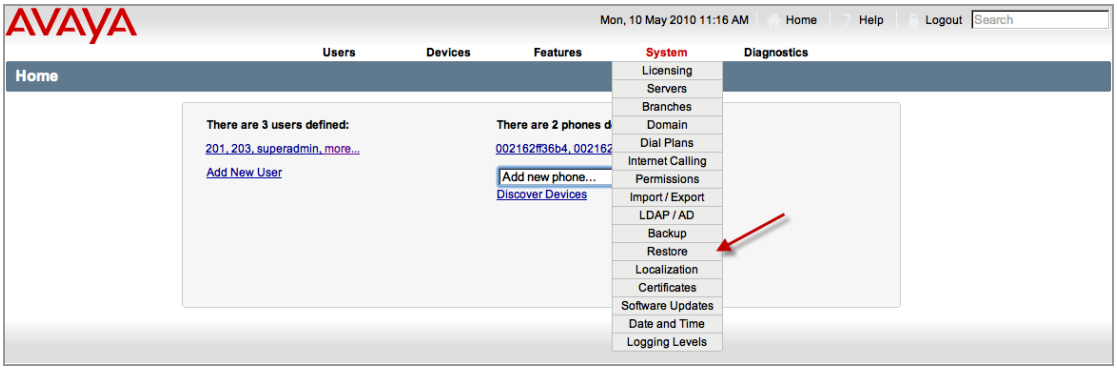
4. Click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

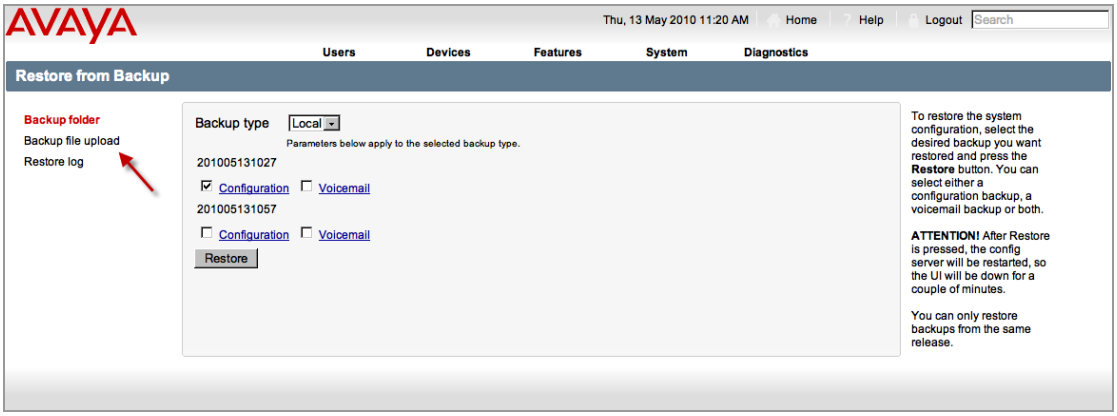
Restoring by File Upload

In the absence of an FTP server, it is still possible to save backup archives to a secondary location for safe keeping. To restore archives from this secondary location follow these steps:

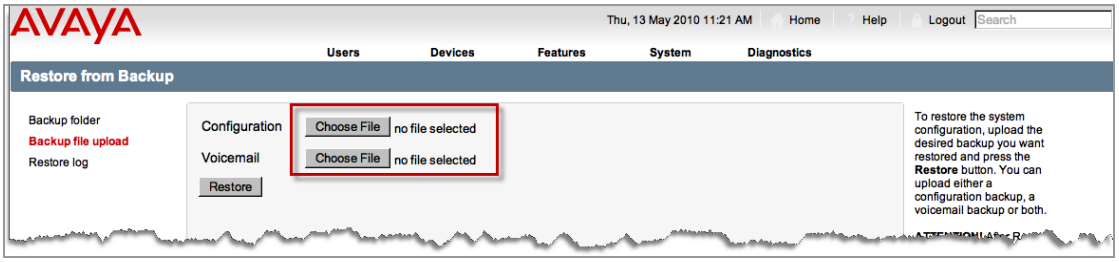
1. Open the **System** menu and select **Restore**.



2. Click on **Backup file upload**.



3. To restore a Configuration file, click on the corresponding **Choose file / Browse** button, to restore a Voicemail file, click on the corresponding **Choose file / Browse** button.



Note: the interface will display an error message if you attempt to enter a voicemail file in the **Configuration** text box and vice versa.

4. When you are ready to continue, click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

The SCS server is now re-installed and restored.

System Rebuild (with High Availability)

If you have configured a High Availability (HA) server configuration, call handling will continue through the distributed system in the absence of the master server. However, features such as voicemail, auto attendant services and conferencing will discontinue. **In the event of master system failure, the distributed system will only perform call handling tasks.**

There might be occasions when it is necessary to rebuild your SCS master server, distributed server, or both. Whether or not you possess a recent backup archive is a decisive factor in how you approach the rebuild. The aim of this part of the guide is to discuss several different rebuild scenarios in an effort to cover the widest possible base and provide the largest number of SCS administrators with the information needed to get systems up and running again. The following scenarios are outlined in this section:

- Rebuilding the master server (no backup)
- Rebuilding the master server (with a backup)
- Restoring a local archive to undo a configuration change
- Rebuilding the secondary server

Scenario 1: Rebuilding the Master Server (no backup)

In the event that you are forced to rebuild the master server and you do not have a recent configuration backup, the quickest way to achieve service continuity quickly and efficiently is to rebuild the master server and re-synchronise it with the distributed system. However, in this case, the newly rebuilt master system's TLS/SSL certificate information will not match that of the distributed system. Ordinarily, a configuration backup would contain the previous system's certificate information, but since a backup does not exist in this scenario you will have to manually synchronise the distributed system with the newly rebuilt master by 1) creating a new secondary server profile on the master server; and 2) running through some setup screens on the distributed server.



Create an Install DVD/USB

Configure server to boot from DVD



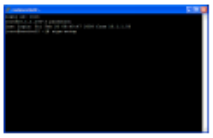
Install SCS software on master server and run Install Wizard

License master server

Create secondary server profile



Log in to secondary server



Launch 'sipx-setup'

Reboot secondary server

Send profile to secondary server

End

Note: To avoid DNS and connectivity issues, ensure that both the master and the distributed system are configured with the same LAN settings as before.

During the course of this solution we will perform the following tasks:

- Create an install disk or USB thumb drive by downloading the SCS software from the Avaya website.
- Configure the master server's boot sequence to ensure that it is capable of booting from the install source.
- Configure the master server.
- License the master server.
- Create a secondary server (redundant server) profile on the master server.
- Run 'sipxecs-setup' on the secondary server to synchronise with the master.
- Send the secondary server profile from the master to the secondary server.

Creating an SCS Installation Build

Before you can configure your SCS server you will need to download and install the SCS software. You will need:

- Internet access
- Writable DVD/USB thumb drive
- DVD burning software capable of creating a bootable DVD from the ISO image – for example *Infra Recorder*.

Downloading the SCS ISO File

The SCS software is contained in an ISO file, which can be obtained from the Avaya website at http://support.avaya.com. Once downloaded, the ISO file should be burnt to a DVD using a DVD burning package that is capable of creating bootable discs, or written to a bootable USB thumb drive.

Burning the ISO File to DVD

Once you have downloaded the ISO file to a suitable location, you must burn it to a DVD. The DVD will then be used to format the server and install the SCS software. For this reason, it is not enough to simply copy the file to a DVD. The file must be burnt to the DVD and the DVD must be made **bootable** using a disc burning application – such as *Infra Recorder*.

Note: Alternatively, you can copy the SCS installation file to a USB drive and boot from that. See 'Creating a Bootable USB Image'.

In order to install the SCS software you might need to configure the boot settings so that the server reads the CD drive at power up. This is achieved in the following way:

Note: If your server already boots from the CD drive, simply place the installation DVD in the CD tray, close it and reboot the system.

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **Onboard or USB CD-ROM Drive**.

6. Use **U** to move it to the top of the list (if the CD-ROM drive is already at the top of the list ignore this step).

7. Press the **Enter** key.

8. Open the CD-ROM tray and insert the SCS installation DVD.

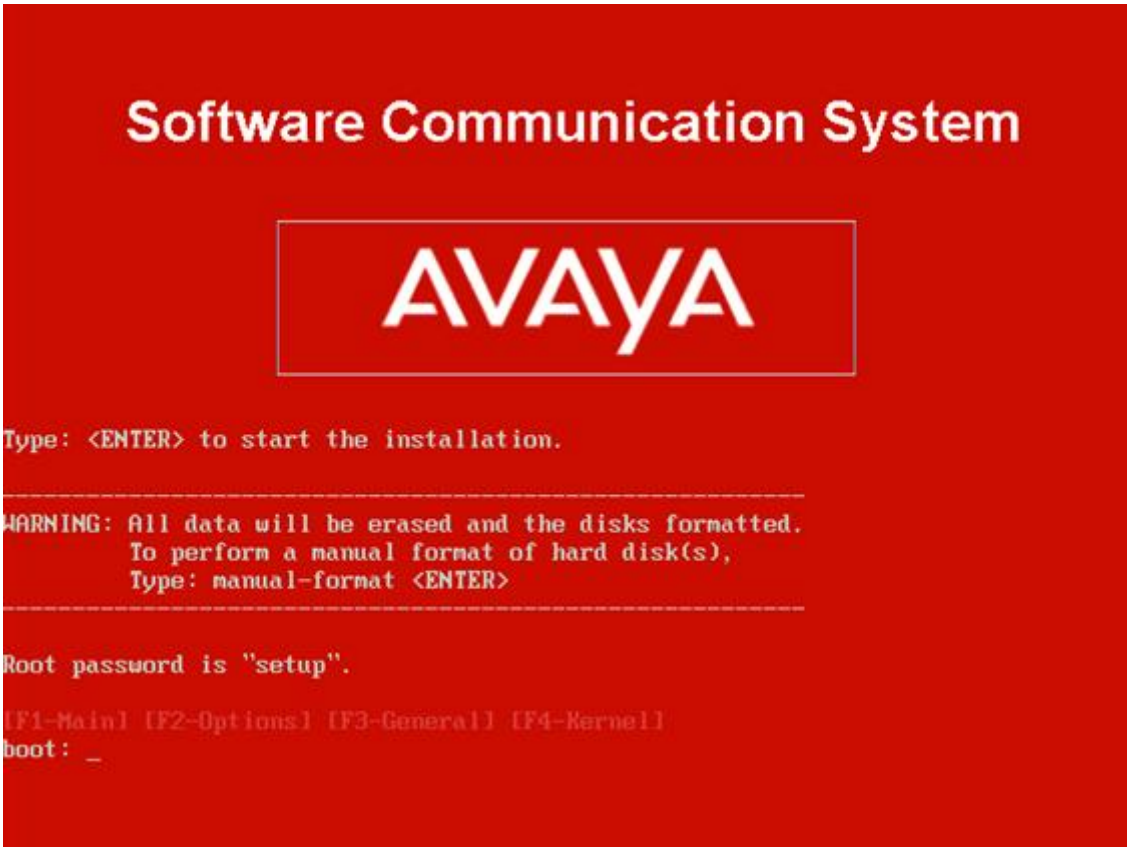
9. Close the tray.

10. Press the **ESC** key to exit System Configuration.

11. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.

12. Press the **Enter** key.

The server will reboot from the DVD and automatically launch the format utility. When the Software Communication System screen is displayed, press the **Enter** key to confirm that you would like to format the hard drive and install the SCS software.



The format and installation process takes approximately 10 minutes, when it is complete the CD tray will eject and the system will reboot to the login screen, from where you can begin the installation process. Continue to 'Configuring the SCS Master Server' for guidance on configuring the server.

Creating a Bootable USB Image

Instead of creating a bootable installation DVD you could instead create a bootable USB image. This will involve:

- Writing the SCS ISO image to a 'bootable' USB thumb drive using an application called *ISO2USB*, which can be obtained at http://iso2usb.sourceforge.net
- Re-ordering the boot sequence of the Dell server.

Note: The USB thumb drive must have a capacity of 1GB or more.

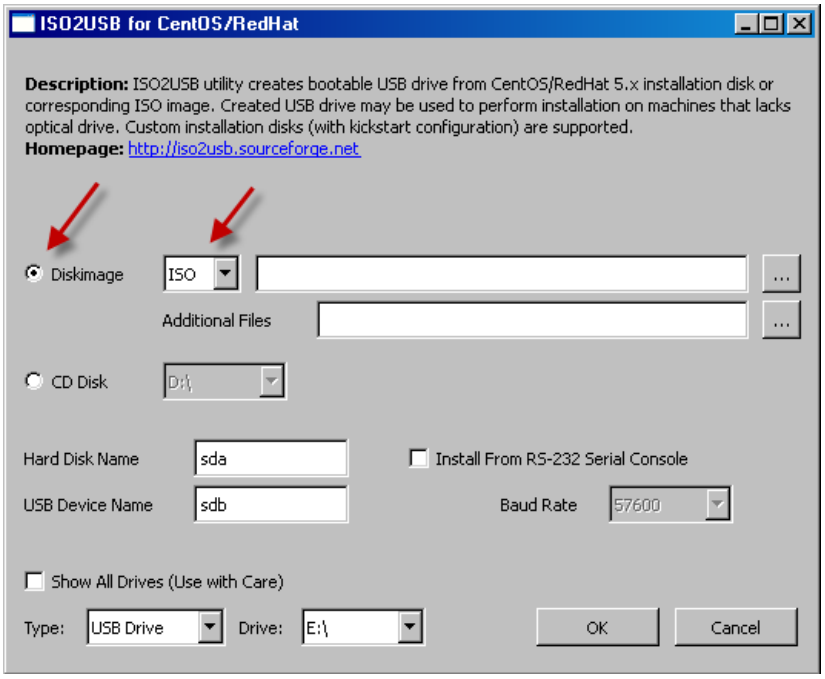
To create a bootable USB drive:

1. Insert a USB thumb drive (ensure that you this is a drive that has no important data on it).

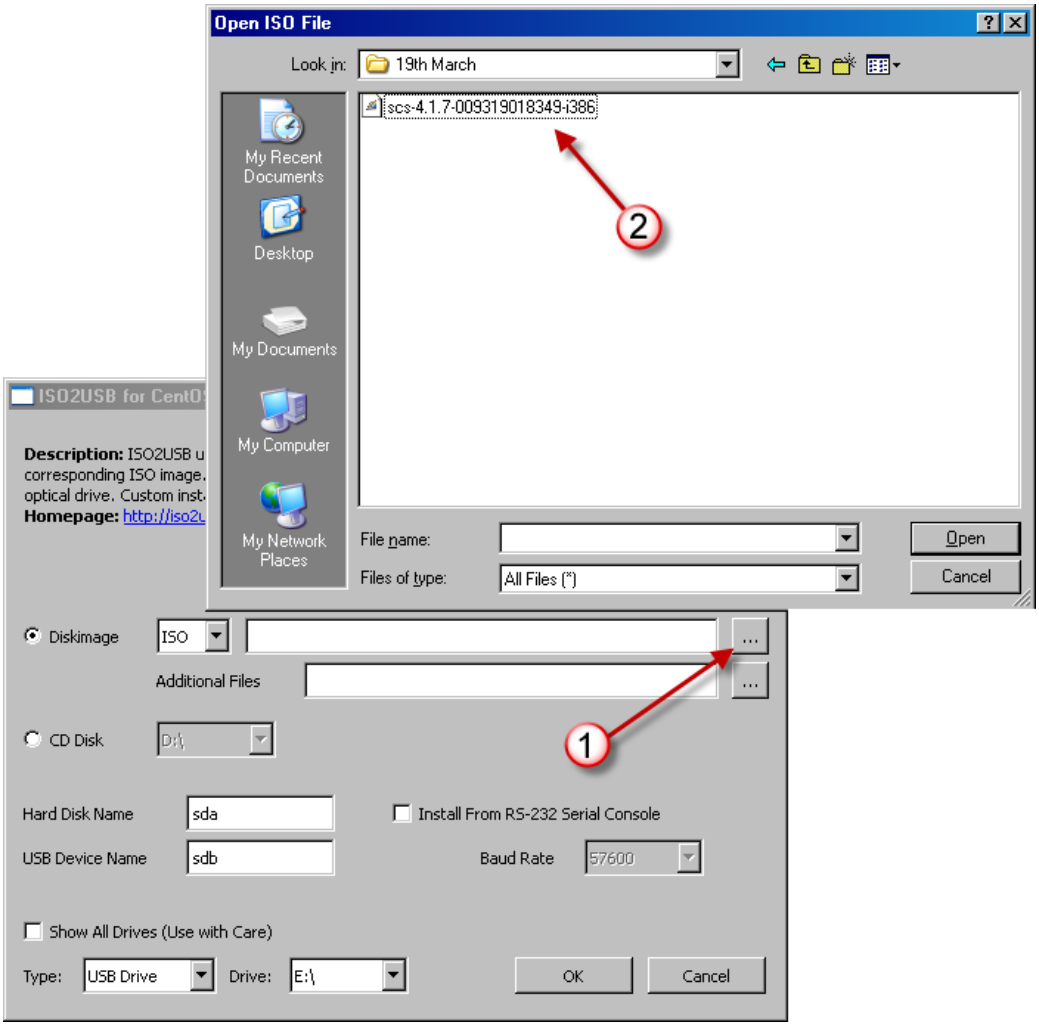
2. Download *ISO2USB*.

3. The package downloads as a ZIP file. Extract the contents and then double-click on **iso2usb.exe** to launch the application.

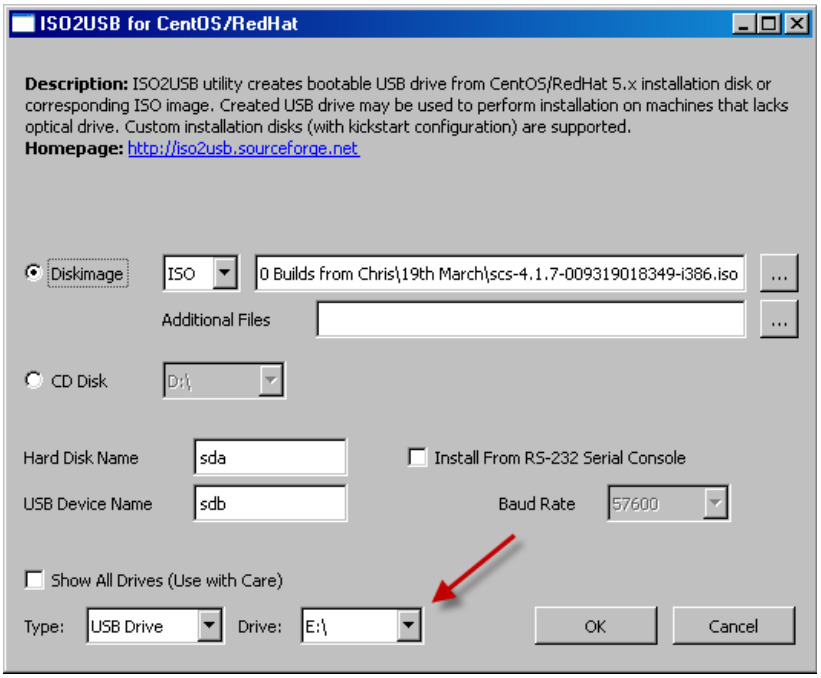
4. Ensure that the **Diskimage** radio button is selected and that **ISO** is selected in the top drop-down menu.



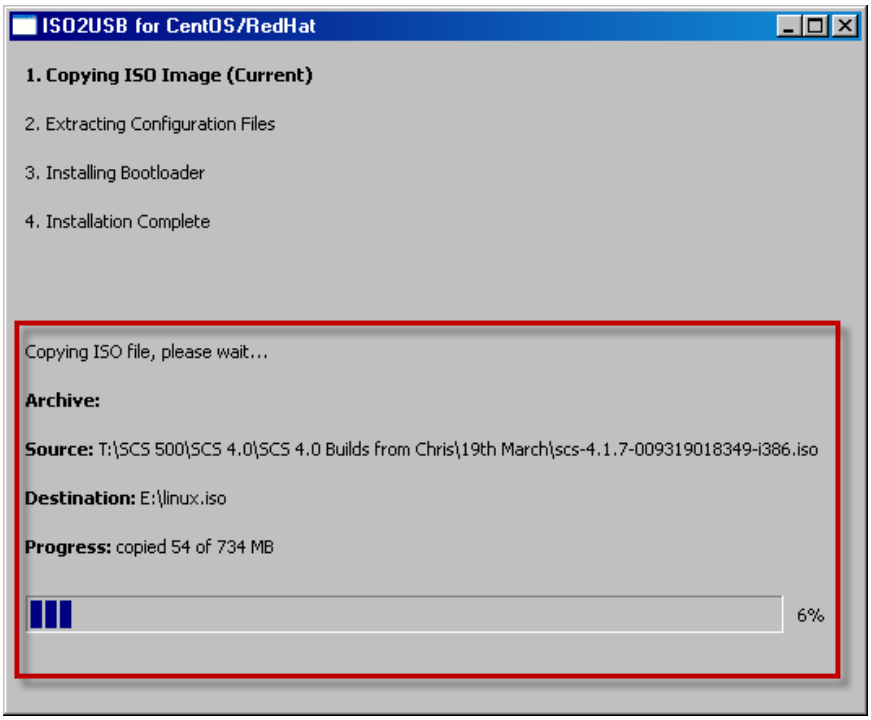
5. Navigate to the location of the SCS ISO image and select it.



6. Select the USB drive from the **Drive** drop-down menu at the bottom of the window and then click **OK**.



7. The image is written to the USB drive.



8. When copying is complete, click the **Exit** button.

You have now created a bootable SCS installation USB drive. Next re-order the boot sequence on the server.

In order to install the SCS software you will need to configure the boot settings so that the server reads the USB drive at power up. This is achieved in the following way:

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **USB Device**.

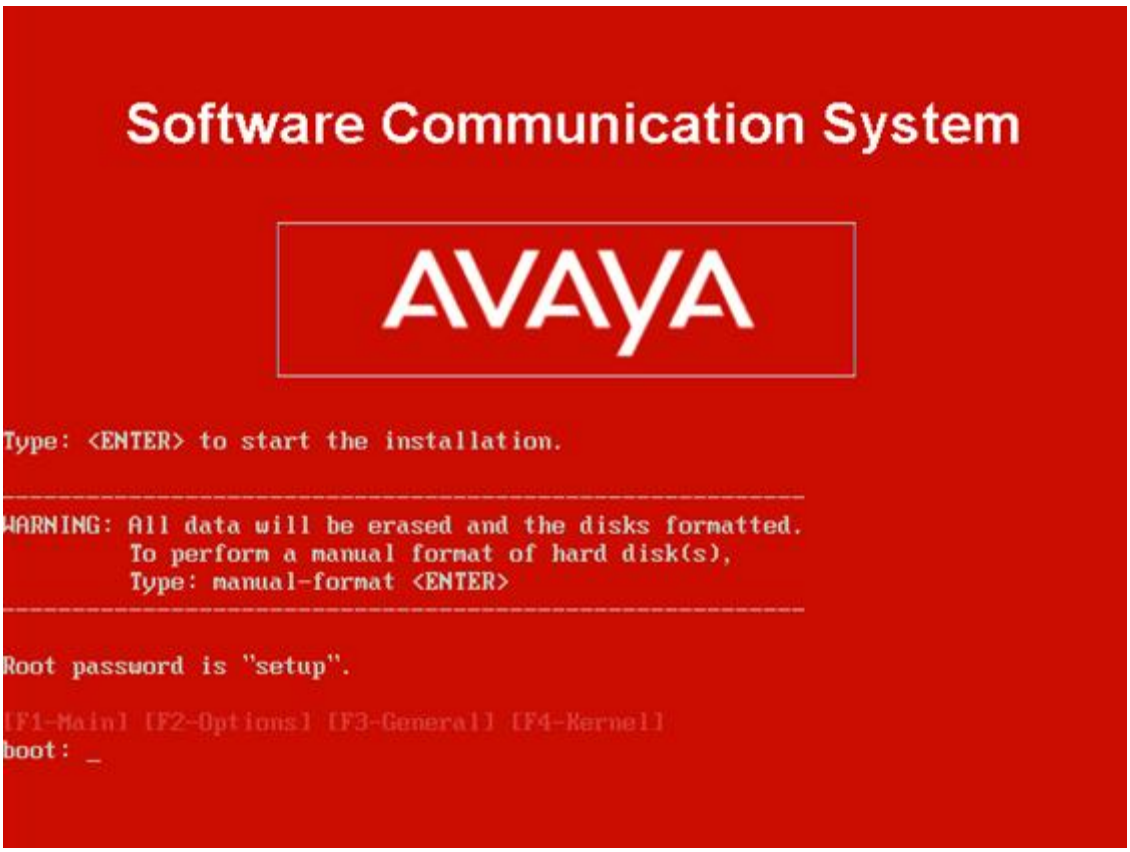
6. Use **U** to move it to the top of the list

    a. On some servers it may be necessary to ‘enable’ the USB device as a boot option. Press the **Space** bar if **USB Device** does not have a priority number next to it. A ‘**1**’ should appear next to the drive.

7. Press the **Enter** key.
8. Insert the USB thumb drive
9. Press the **ESC** key to exit System Configuration.
10. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
11. Press the **Enter** key.

The server will reboot from the USB drive.

When the red Avaya screen is displayed press **Enter**.



A ‘kickstart’ error will be displayed, this is normal. Simply use the **down** cursor key on your keyboard to highlight the **OK** button and press **Enter** to launch the format utility. When formatting is complete the SCS software will be copied to the server’s hard drive.

The format and installation process takes approximately 5 minutes, when it is complete the system will announce a reboot – **Ensure that the USB drive is removed from the USB port before the reboot begins otherwise the system will reboot from the thumb drive again**. If you are unable to remove the USB thumb device before the system reboots, wait for the red Avaya

screen to appear, remove the thumb drive and then press **CTRL-ALT-DEL** to reboot the server.

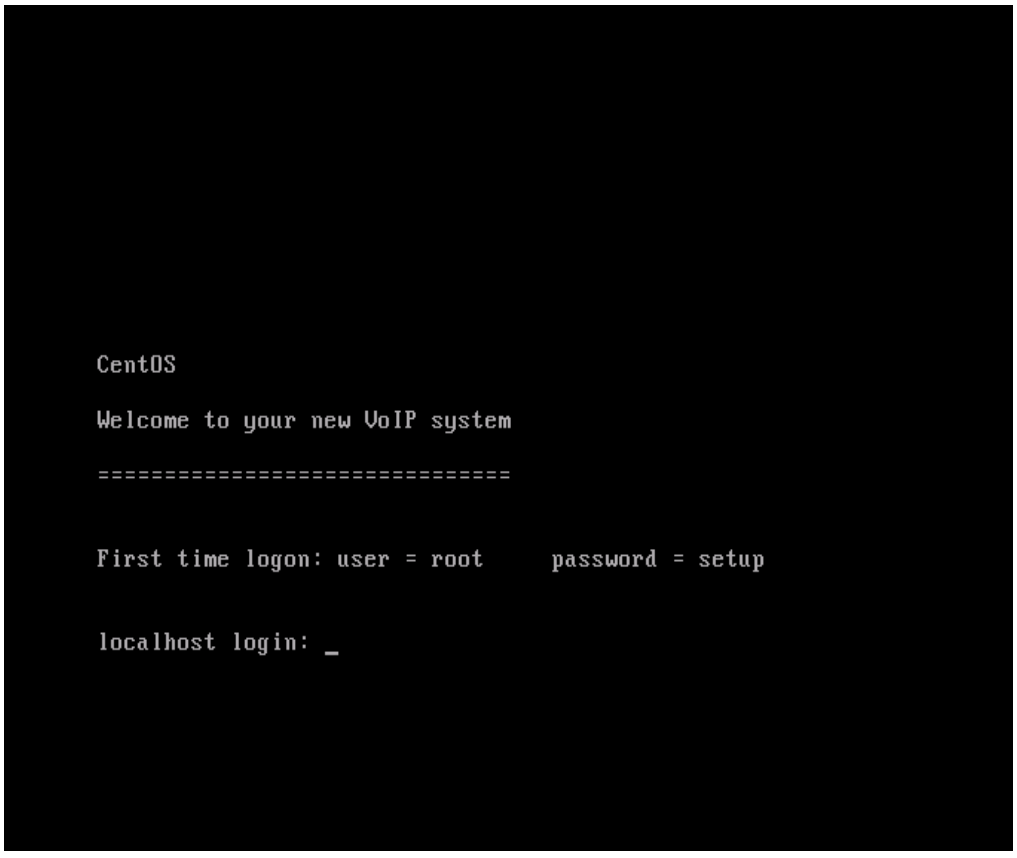
The system will boot to a login screen.

Configuring the SCS Master Server

Once installation is complete you will be presented with a login screen.

1. To begin the setup process, enter the following username and password to access the configuration utility:

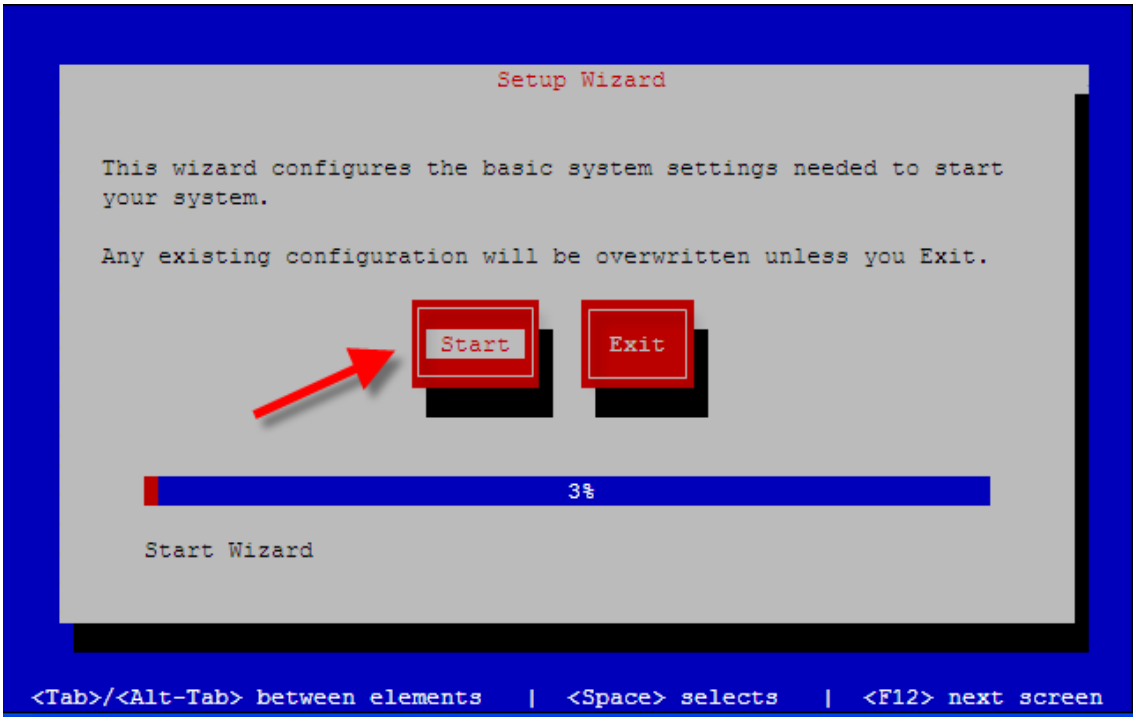
   Localhost Login: `root`
   Password: `setup`



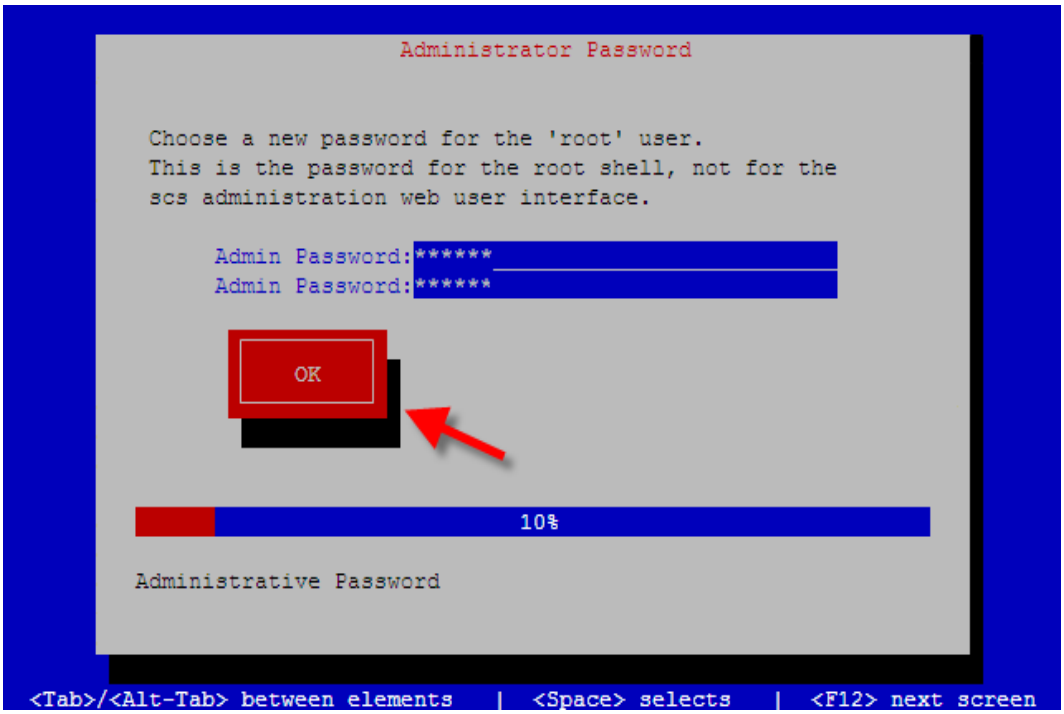
   If at any time during the setup process you make an error, reboot the server and log in using the same username and password. At the command prompt type **sipxecs-setup-system** and press **Enter** to reload the configuration utility from the start.

Note: The SCS domain cannot be changed by running sipxecs-setup-system. The only way to reconfigure the domain is to access the Domain facility from the administrator GUI.

2. When the configuration utility has finished loading, highlight the **Start** button and press **Enter**.



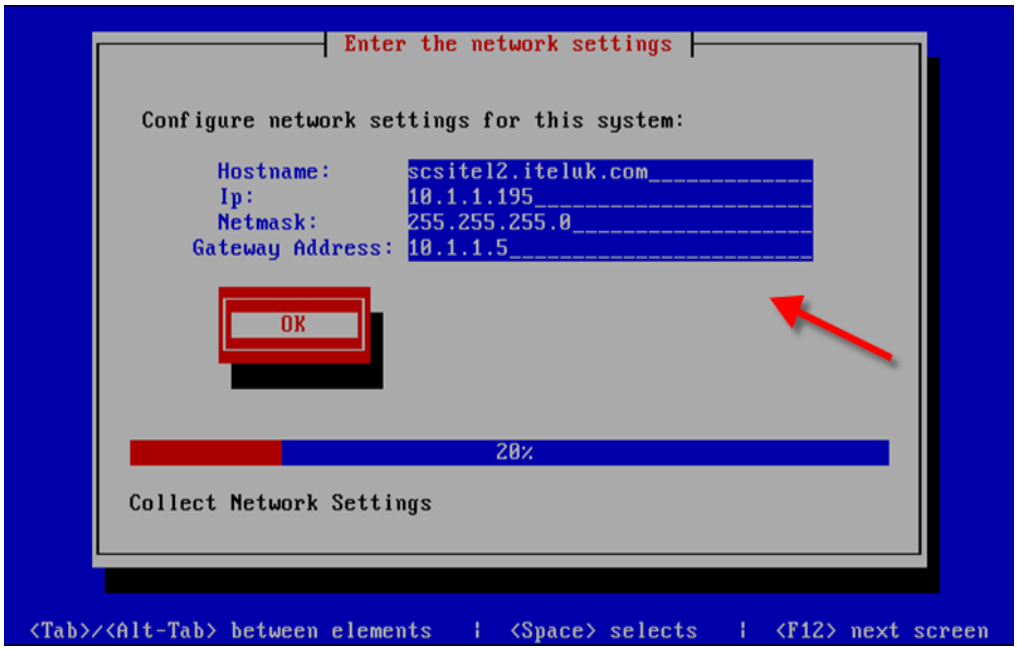
3. Enter the **Admin Password** twice. This is the password that engineers and administrators will enter to gain access to the SCS server locally via the Linux operating system (where you are now). Highlight the **OK** button and press **Enter** when you are ready to continue.



4. Enter the following LAN settings:

a. **Hostname** – This is the fully qualified domain name (FQDN) of the SCS server as defined in the DNS records.
b. **IP** – The IP address that has been assigned for use with the SCS. Again, this must be consistent with the address defined in the DNS settings.
c. **Netmask** – The network's subnet mask.
d. **Gateway Address** – The address of the default router providing access to the Internet.

If you are unsure of any of these settings, see the network administrator.

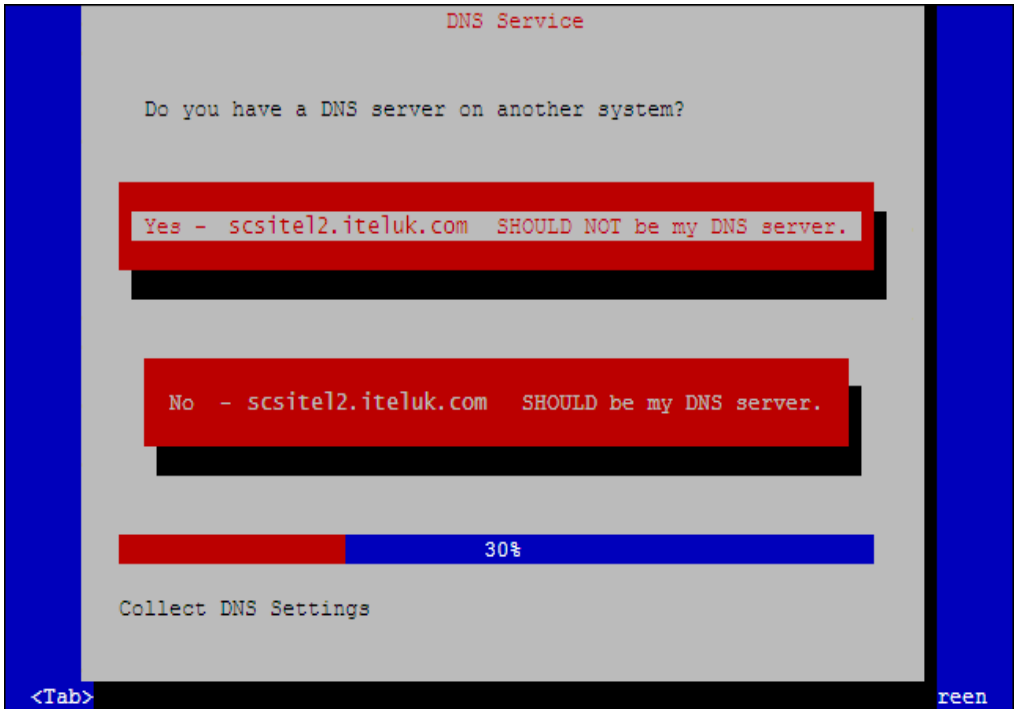


5. The installation wizard will now query whether or not you have DNS configured on the network. The SCS can be configured to function as a DNS server on the network if you do not have DNS or are unable to configure the required records. To enable the SCS onboard DNS, select **No xxx.xxx.xxx should be my DNS server**.

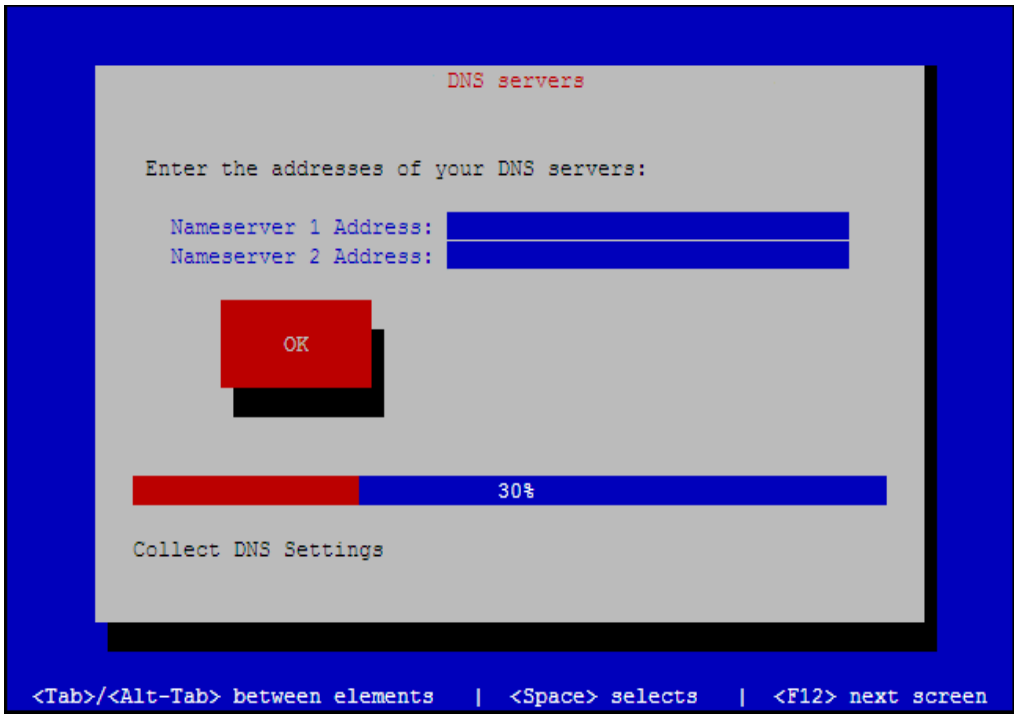
Note: If the DNS service is enabled on the first server it will replicate on the secondary server automatically.

Note: The onboard DNS will create all necessary records required by the SCS in order for it to function correctly.

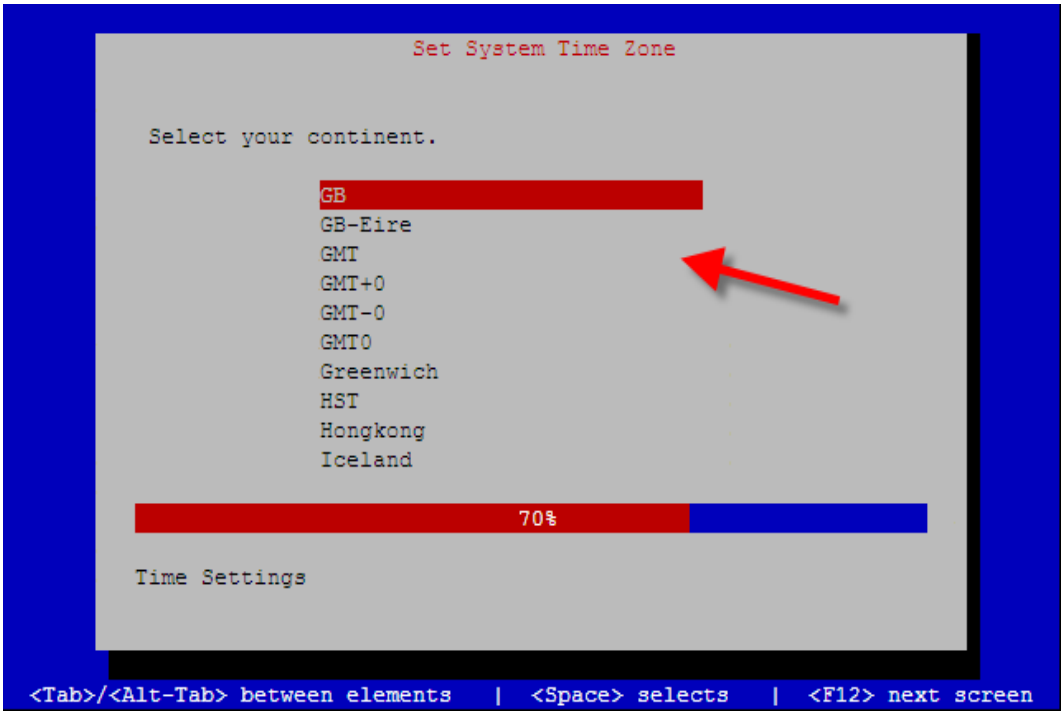
Note: If you elect to enable the SCS's onboard DNS the next screen will offer you the opportunity to define upstream DNS servers if you wish. If the network utilizes Intranet DNS or DNS from an IP service provider then these server addresses can be entered on the next screen. Note that this is an optional configuration step and the fields can be left blank if required, however without these addresses, name and address resolution may prove difficult since the SCS will not be able to resolve *all* DNS queries.



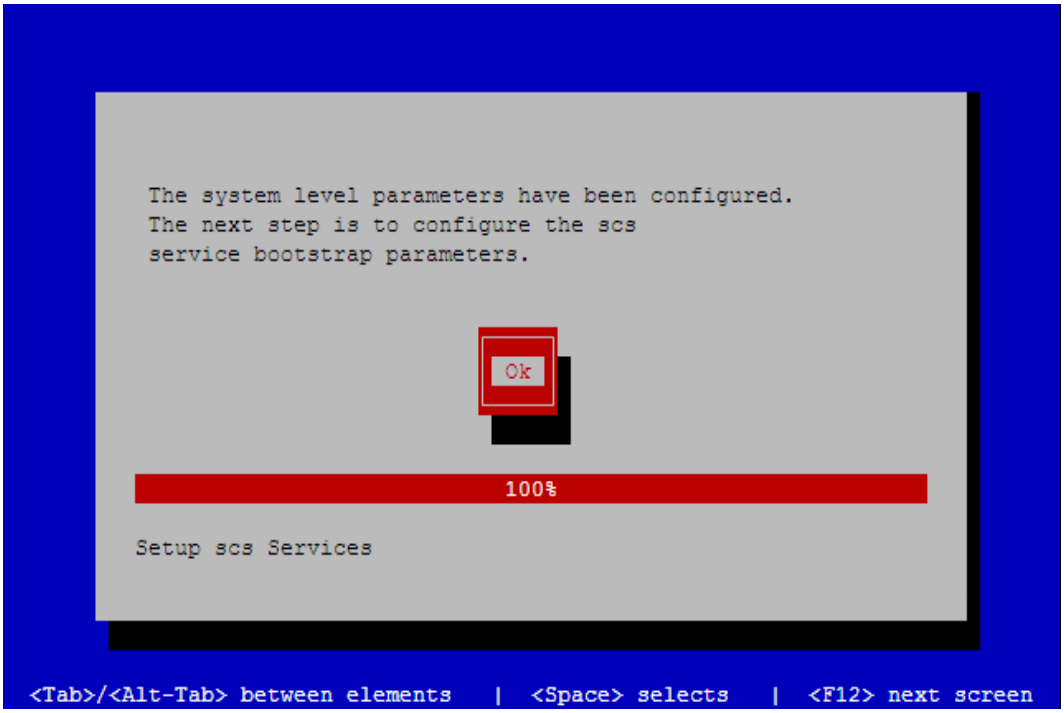
If you already have DNS configured for the SCS select **Yes xxx.xxx.xxx should not be my DNS server**. Note that in this instance the next screen will ask you to configure the address of a primary and secondary DNS server.



6. Select a region or country to set the time zone in which the SCS is situated – if you pick a region, such as ‘Europe’, you will be prompted to then define an area within that region, for example, ‘London’.



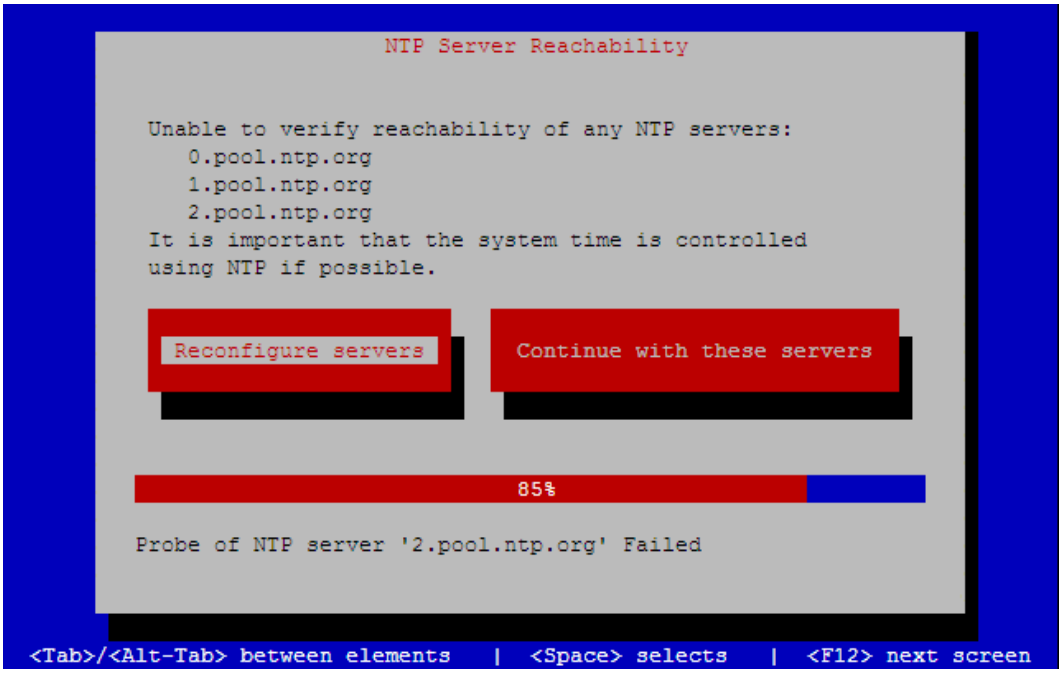
7. The system will now search for NTP servers in order to set system time. By default the SCS is programmed to attempt a connection to a series of Internet-based time servers. If it cannot connect to any of these servers you will be asked to either: 1) move on with the current time server configuration, in which case you will have to set the time manually - see Step 7b; 2) configure the address of a different time server. If the SCS successfully gathers NTP data the following message will be displayed:



Note: The NTP server search can take a while. Do not power off or disconnect the SCS during this process, even if it seems that nothing is happening.

Press **Enter** and continue to Step 8 if you see this message.

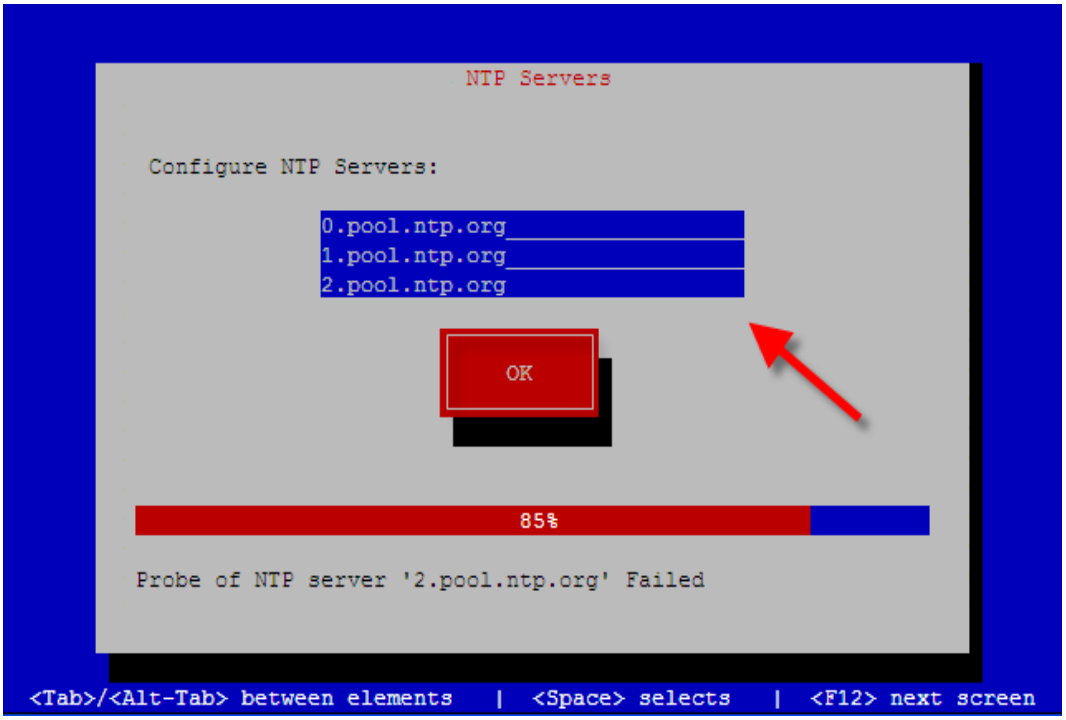
If you see the message below regarding NTP servers continue to Step 7a.



a. You now have the choice of configuring a different set of NTP servers or continuing with the default settings and configuring the time manually on the next screen.

    i. To set new NTP servers, highlight **Reconfigure servers** and press the **Enter** key.

    ii. Enter the new NTP addresses and then highlight the **OK** button and press **Enter**.



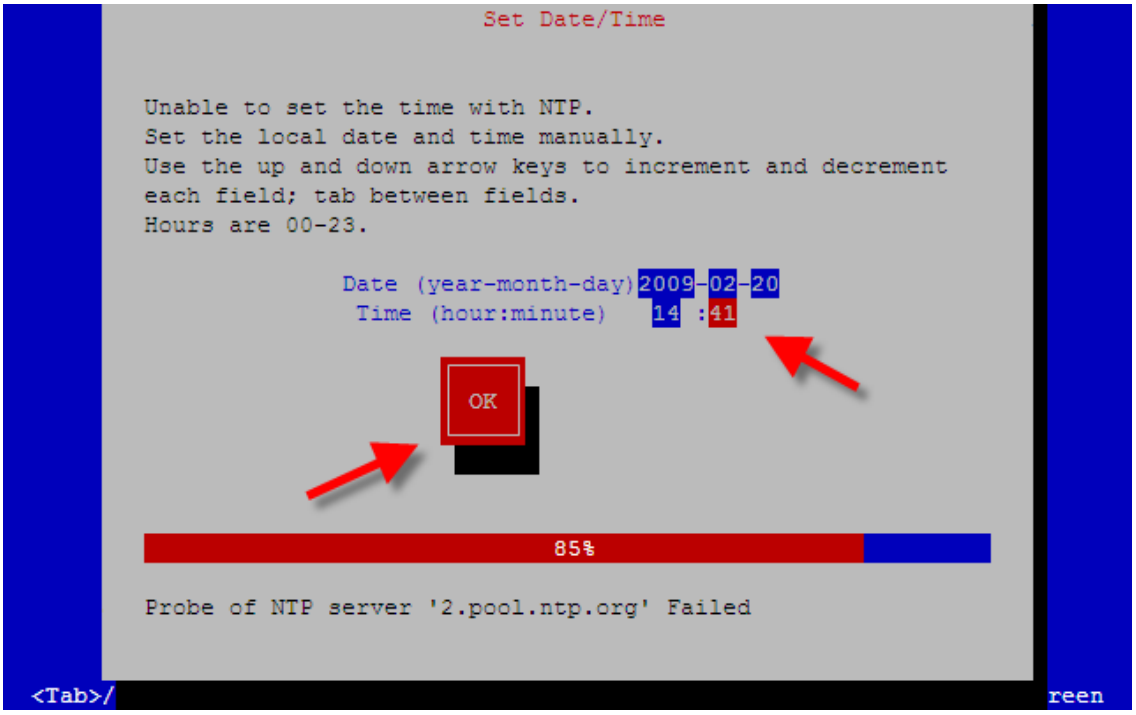
iii. The SCS will attempt to connect to the defined NTP servers.

iv. When a connection is successful press **Enter** to clear the confirmation screen and then continue to Step 8.

b. Instead of configuring alternative NTP servers you can set the time manually.

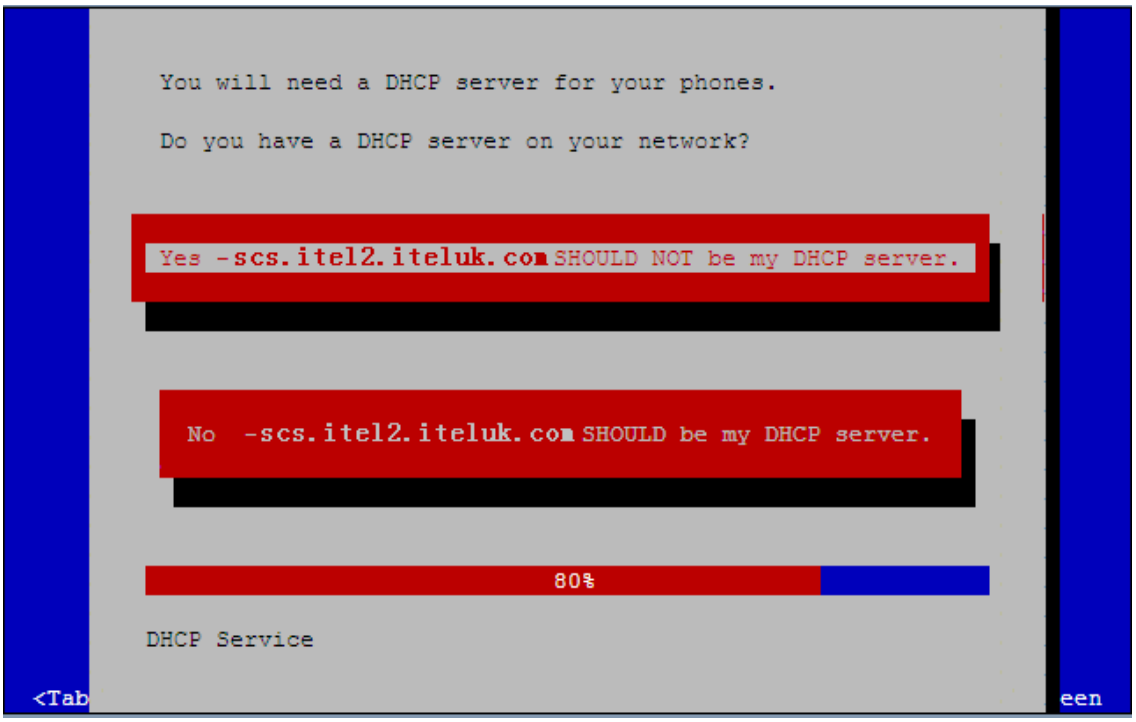
i. Highlight **Continue with these servers** and press **Enter**.

ii. To set the time, use the **left** and **right** cursor keys to move between the fields and the **up** and **down** cursor keys to adjust each value. The time should be set in 24-hour format. Highlight the **OK** button and press **Enter** to continue.



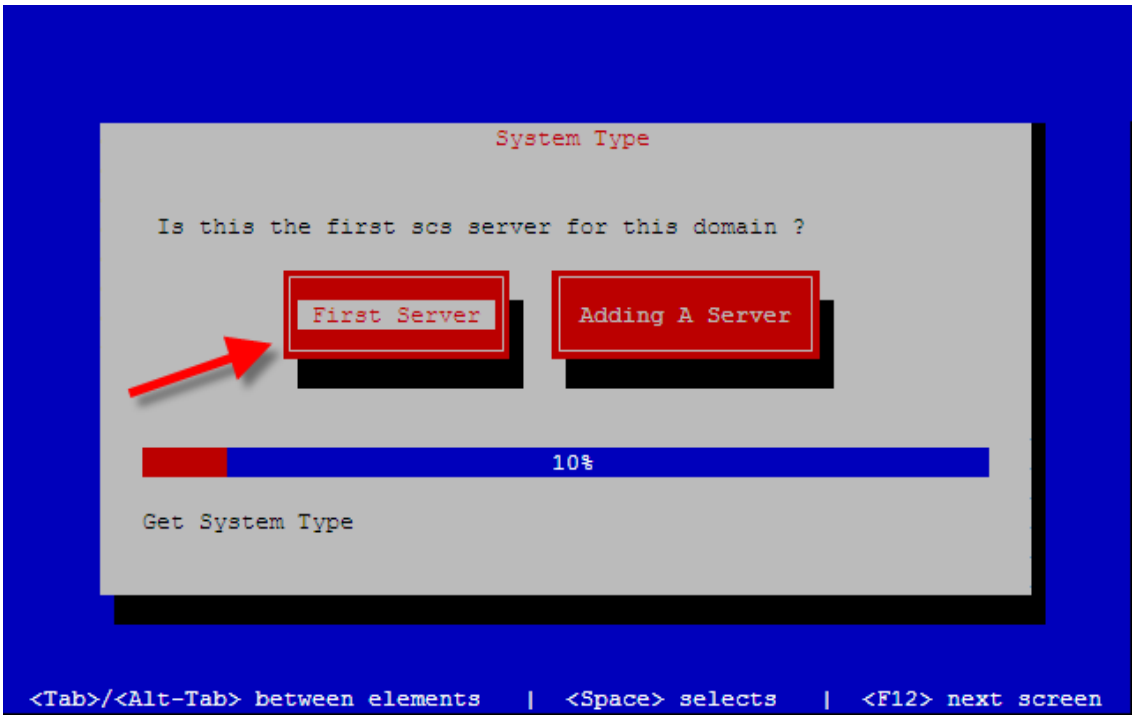
iii. Continue to Step 8.

8. The SCS can provide a DHCP service in order to provide devices joining the network with IP addresses. To enable the DHCP service select **No xxx.xxx.xxx should be my DHCP server**.



Note: If a DHCP service is already active on the network **do not** enable the onboard DHCP service since this will cause a conflict.

9. You now need to configure some settings that will define this server as your primary SIP server. First, define the server as your 'First Server'. Highlight **First Server** and press the **Enter** key.

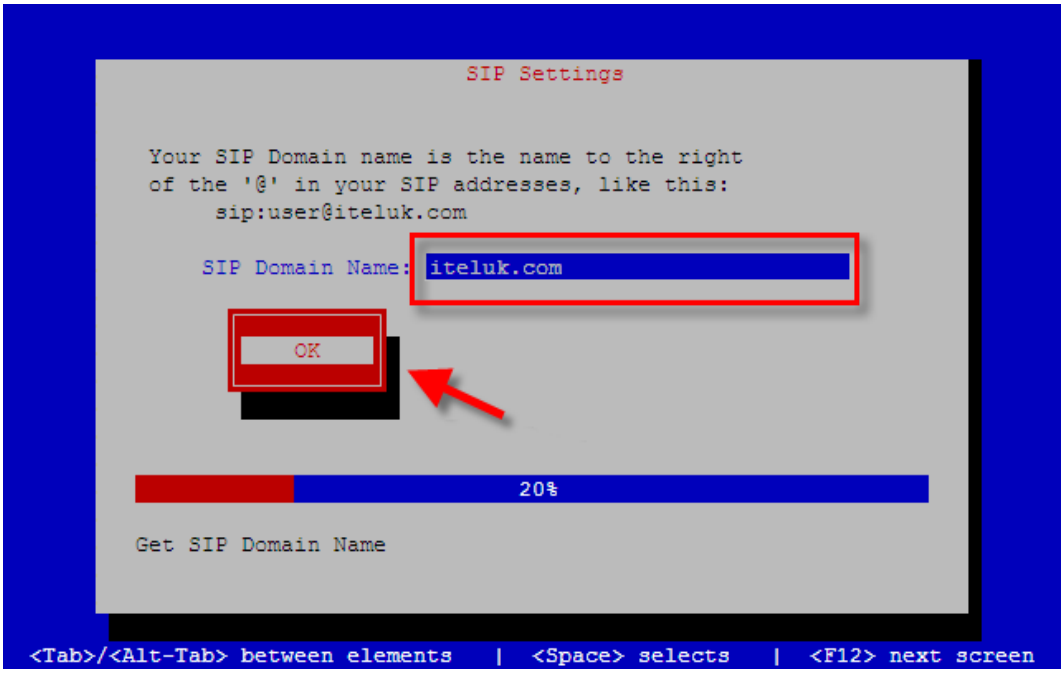


Next set the SIP Domain. Knowledge of your network configuration is vital at this stage. Because you are dealing with an HA configuration, all required DNS SRV records should already be in place, the SIP domain should simply be entered as the domain name: e.g., *scsdomain.com* (the domain name must be the same on the previous build, otherwise the archive restore will fail). In an HA scenario the SIP domain is **never** entered as a fully qualified domain name (FQDN). By default the wizard will enter the domain name in the correct format.

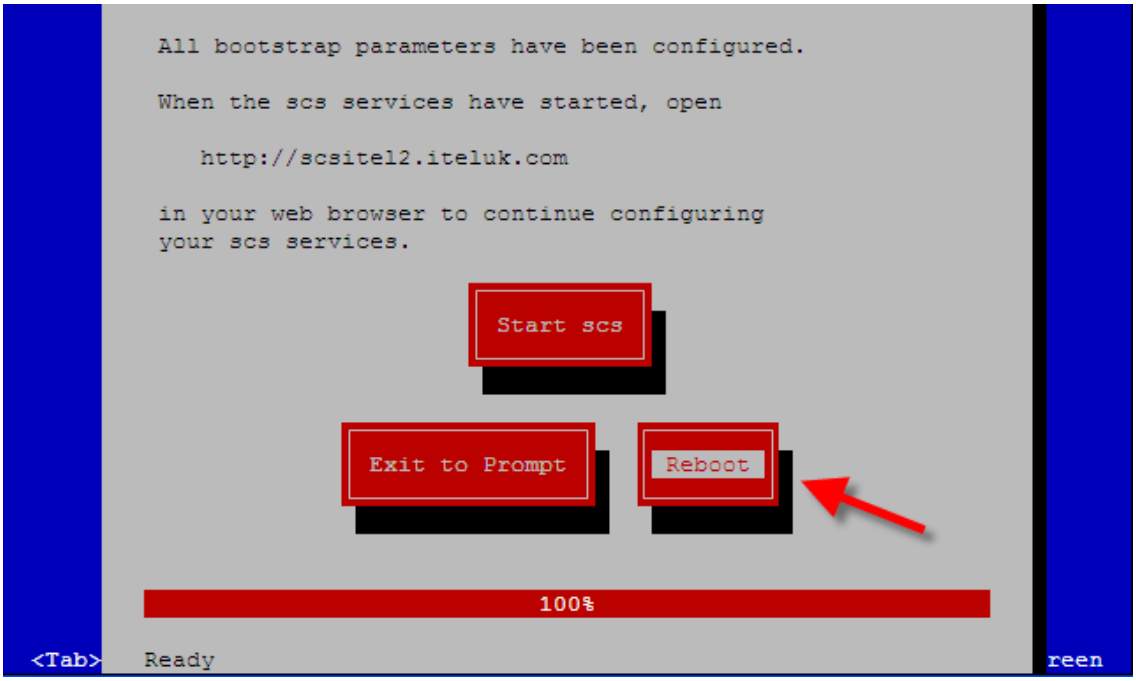
Note: If you elected to enable the SCS's own DNS then all required SRV records will be generated automatically, you should therefore leave the SIP domain as the default entry and press the **OK** button to continue.

In the example illustrated below the SIP domain has already been entered as *iteluk.com* by the wizard, this is fine because in this instance DNS SRV records are in use on the network.

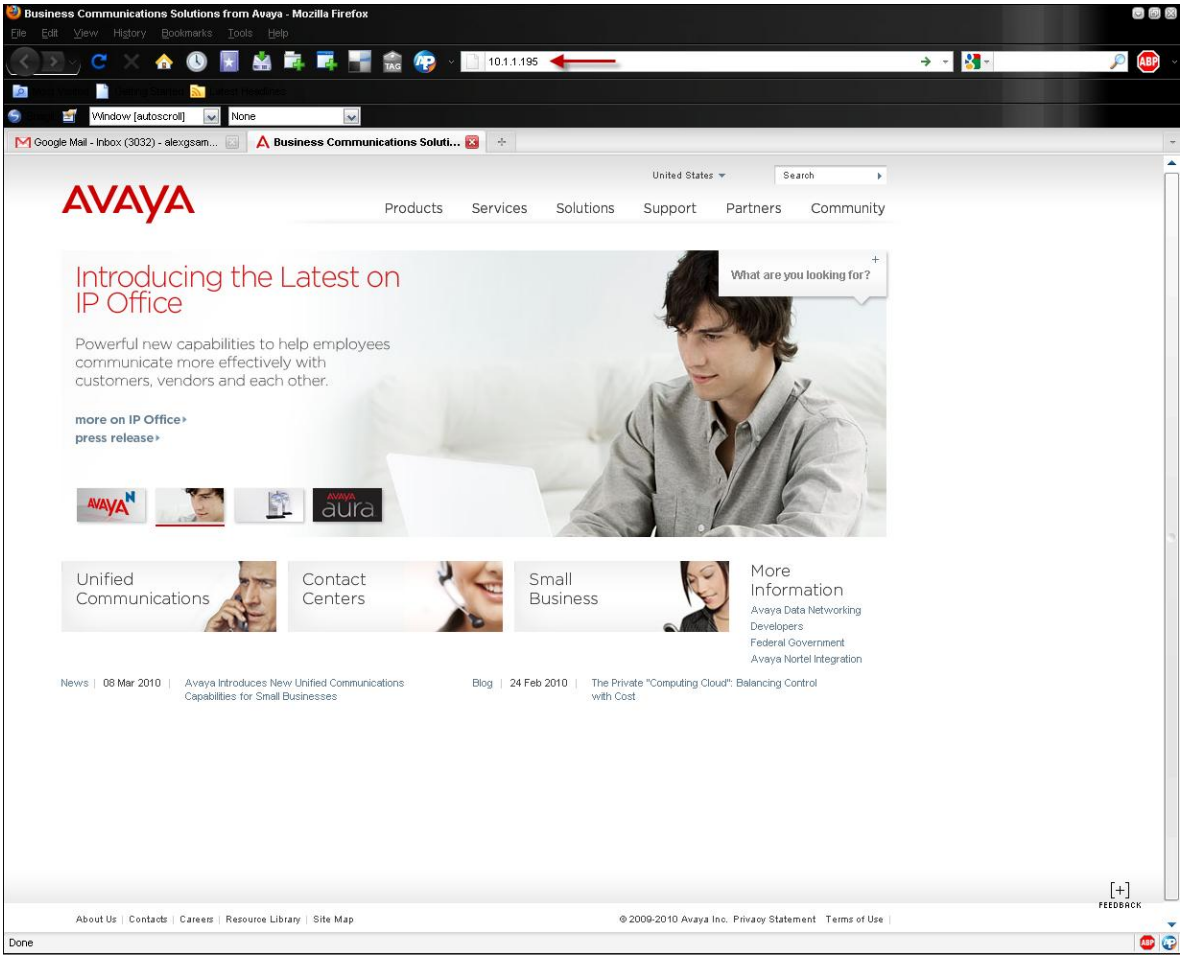
Highlight the **OK** button and press the **Enter** key when you are ready to continue.



10. Configuration of the SCS server is now complete. Highlight the **Reboot** button and press the **Enter** key to restart the server.



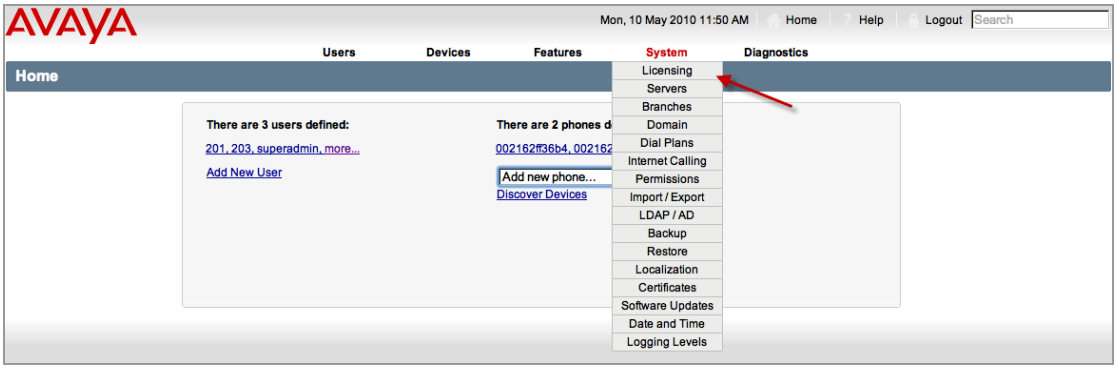
When the server has restarted, administration of the system can be carried out via the web-browser interface, which can be accessed from a remote workstation/laptop by navigating to the server's address or host and domain name in a web browser.



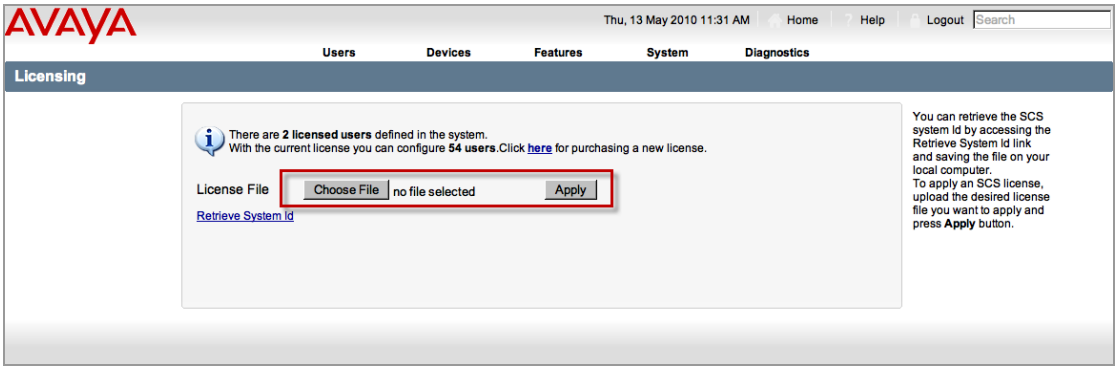
Licensing the System

Now that the Master server is installed and configured you will need to licence it before you can commence creating/restoring user and device profiles.

1. Place the mouse pointer over the **System** menu and select **Licensing**.



2. To apply your license file, click the **Choose file / Browse** button and browse to the location of the file. When you have selected a file, click the **Apply** button.



3. The license file will be applied to the SCS system, enabling the configuration of users based on the number of users purchased.

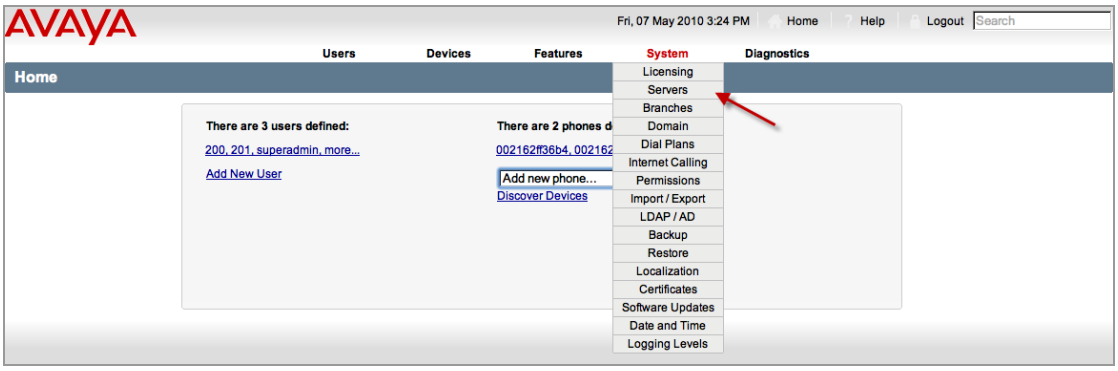
Once the system is licensed you can commence configuring user accounts and device profiles. In short, you can now bring the system back to full operating condition.

Creating the Secondary Server Profile

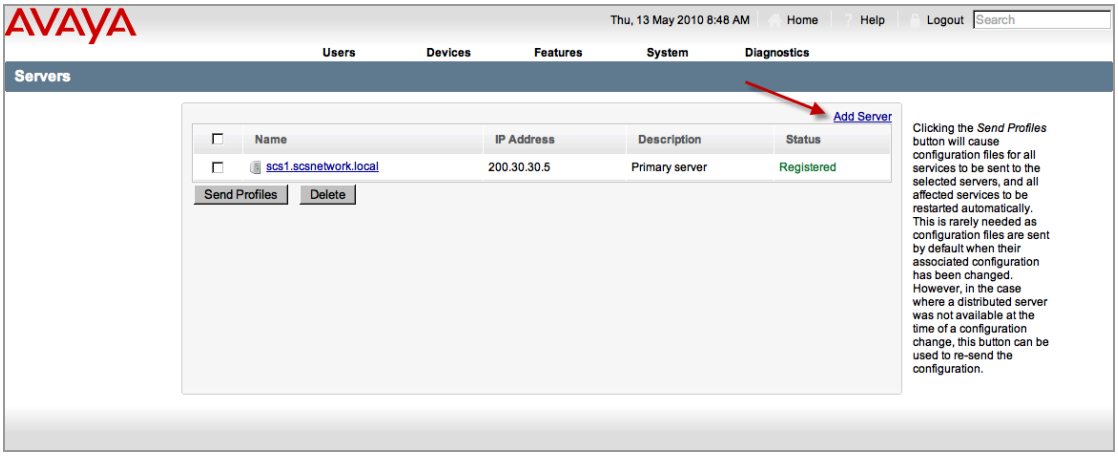
With the SCS fully configured and operating you can now reconfigure the secondary HA server to ensure call continuity in the event of future system failure. **The existing secondary server configuration will need to be replaced because its TLS/SSL certificate no longer matches that of the primary after the re-installation.**

Before you attempt to configure the second server, create a profile on the master, or Primary SIP Server:

1. Open the **System** menu and select **Servers**.



2. Click **Add Server**.



3. Enter the following details:

    a. **Hostname** – The hostname that will be applied to the redundant server when you configure it later. This must be consistent with any DNS entries that exist for this server. For help configuring DNS records for use with HA scenarios see the 'Configuring DNS and DHCP for Windows Server 2003' guide.

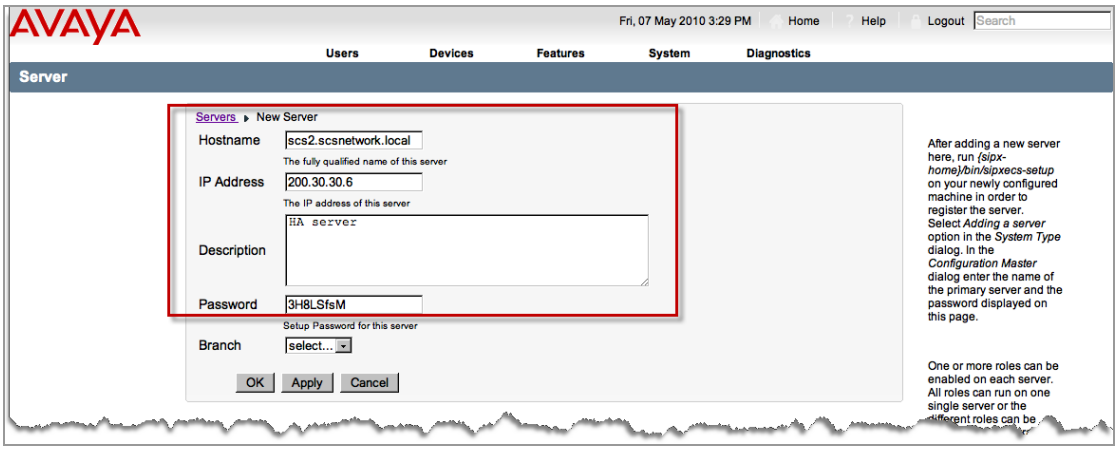
Note: Enter exactly the same details as those that were applied to the original secondary server profile.

    b. **IP Address** – The IP address reserved for the new server.

    c. **Description** – Enter a brief description of the server.

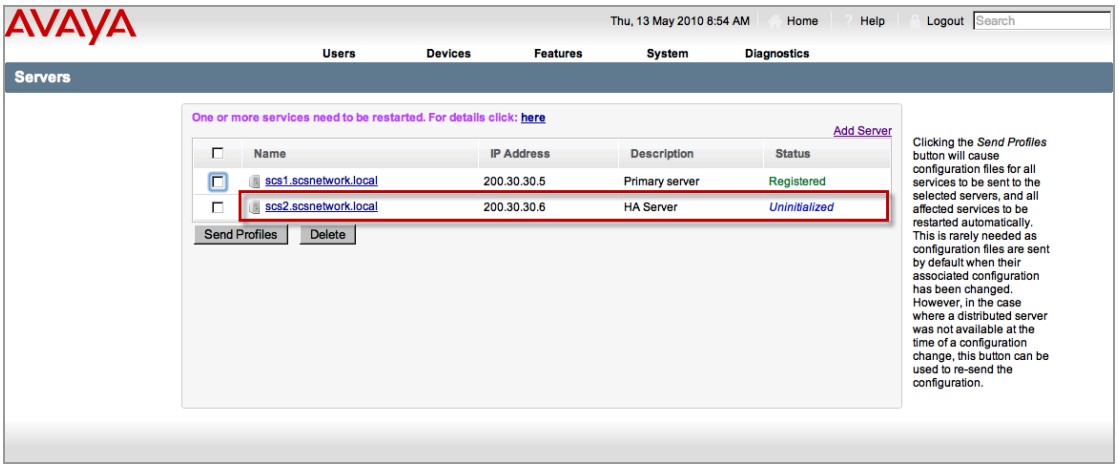
    d. **Password** – The SCS will automatically populate this field, but you may wish to enter something easier to remember because this password will be required later when you configure the secondary server. Ensure that you make a note of the password and keep it to hand for later in the process.

    e. **Branch** – Select a branch if the secondary server should route calls through a specific gateway location.



4. Click **OK**.

5. The new server profile is listed along with the primary. Note that the **Description** field aids you in identifying one server from another.



Note: At this stage the SCS will request that the Call Detail Records (CDR) service is restarted. Other services will require restarting at a later stage. You can either restart the CDR service now or restart it with the other services later.

You now need to synchronise the master server and secondary servers.

Synchronising the Servers

To synchronise the master server with the secondary server, log in locally or remotely (*Putty* can be used to access the server remotely using SSH) to the secondary server and, at the prompt, type the following command:

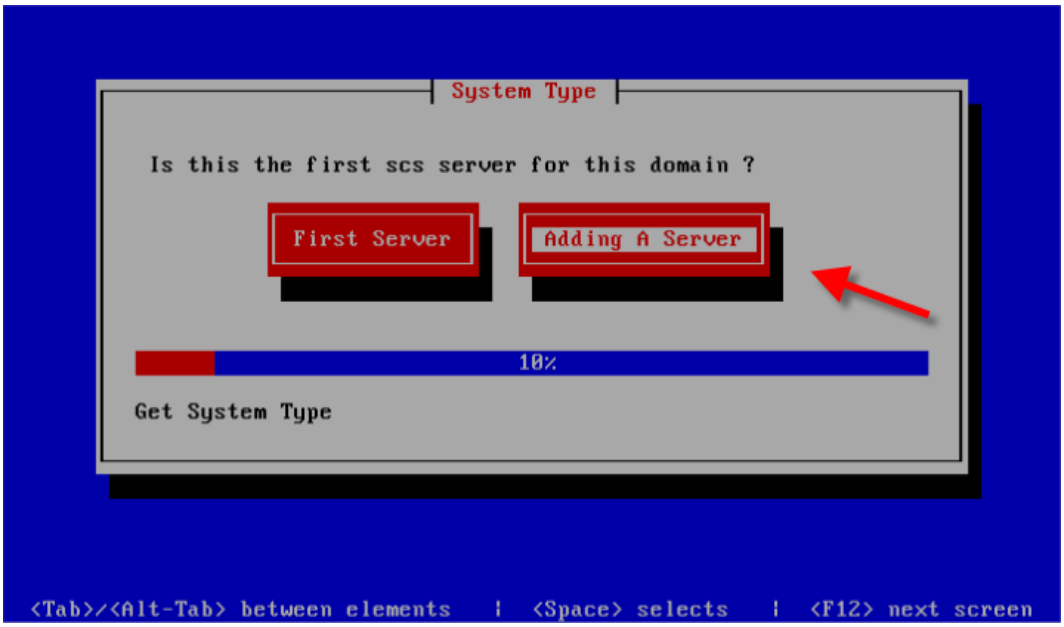
```
sipxecs-setup
```

The setup utility will load, configure the settings as follows:

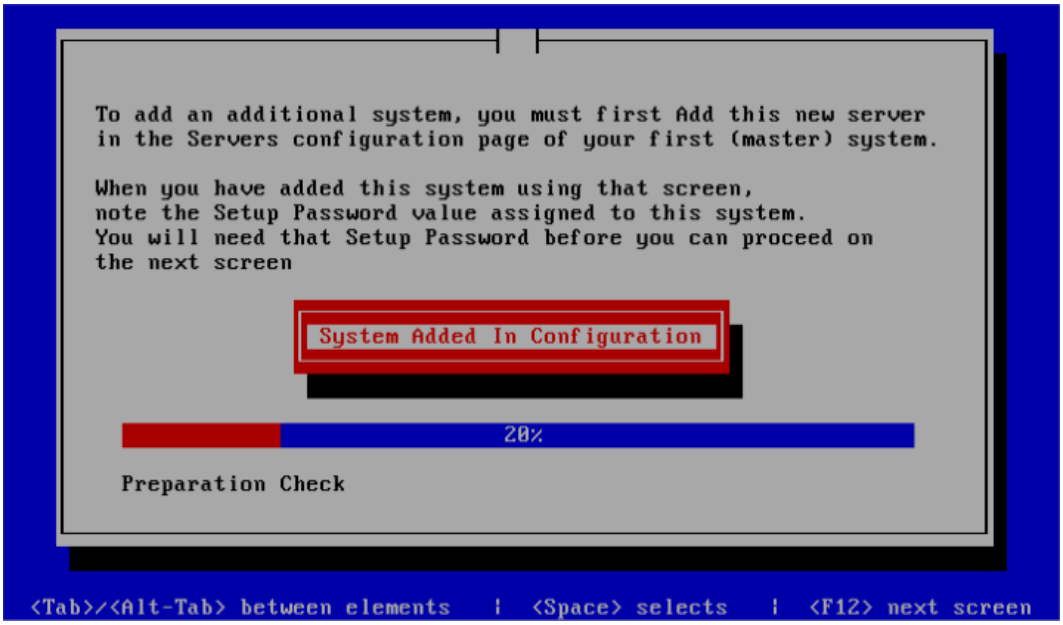
1. Press the **Enter** key to clear the introductory screen.



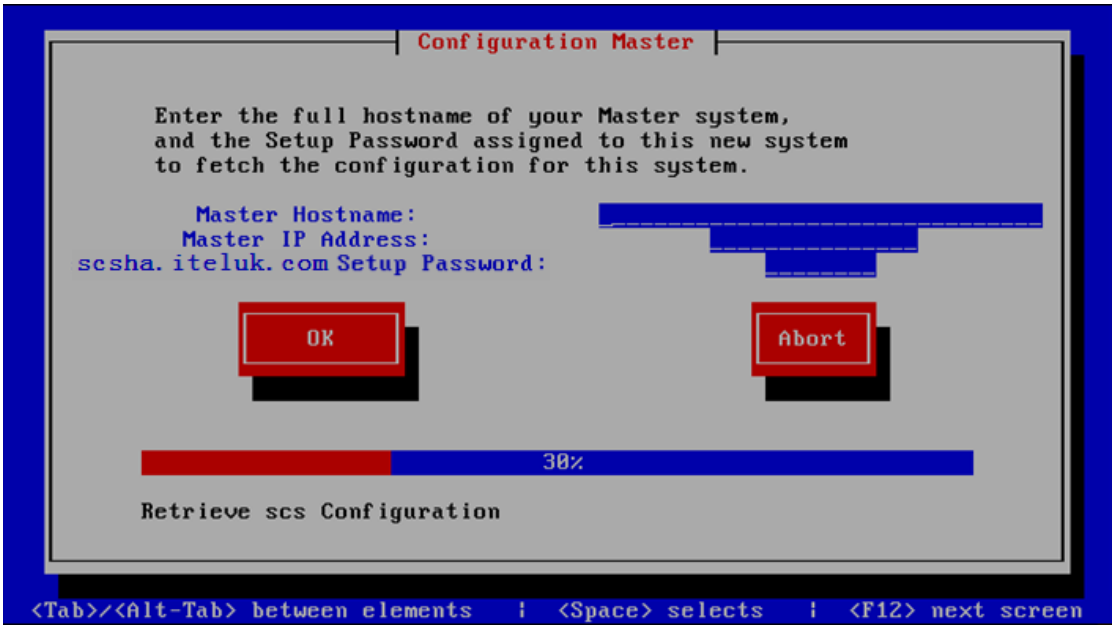
2. Select **Adding a server** and press the **Enter** key.



3. The next screen acts purely as a reminder, pointing out that before you configure the next settings you must first create a profile in the primary server's GUI. If you have already created the profile press the **Enter** key. If you have not yet created a profile for the secondary server ensure that you do before continuing.

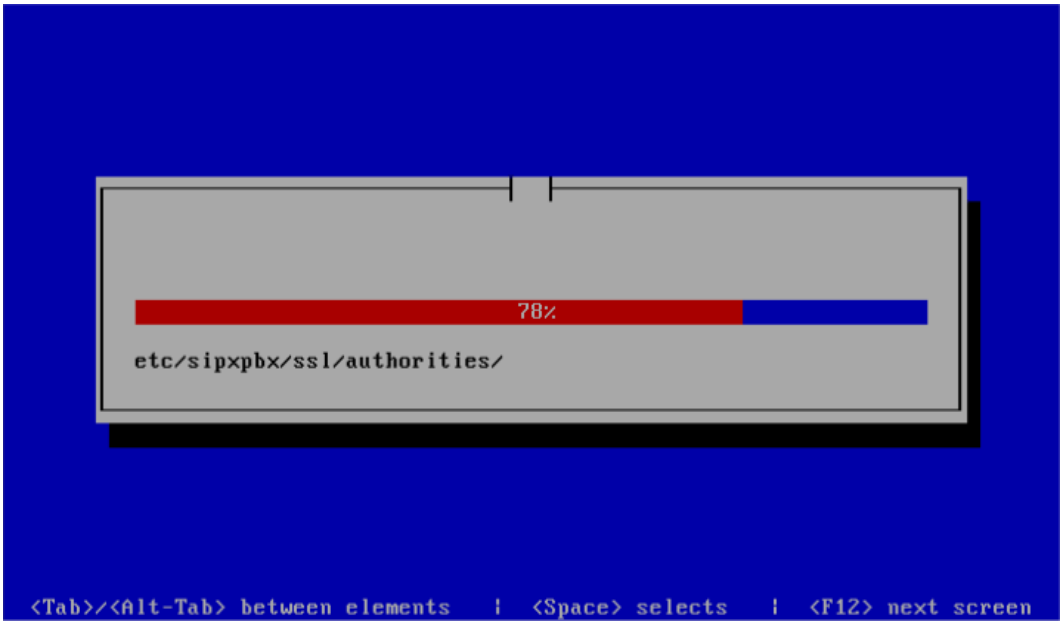


4. Enter the hostname and IP address of the **primary** server, followed by the password for the **secondary** server - created when you configured the secondary's server profile earlier.



Highlight the **OK** button and press **Enter** when you are ready to continue.

5. Wait a few moments while the server downloads settings and synchronises with the master server.

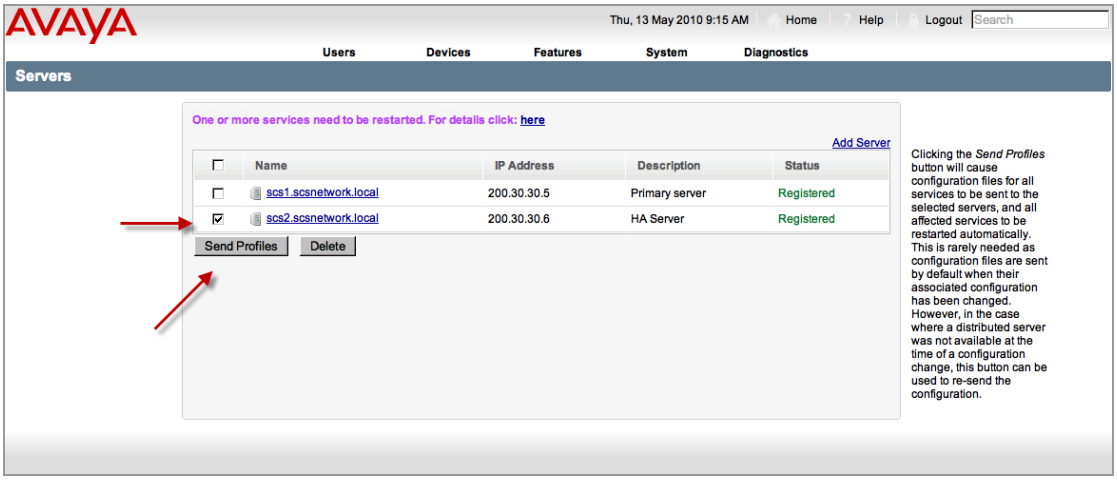


6. Finally, when configuration is complete, highlight the **Reboot** button and press the **Enter** key.

The secondary server is now connected to the network and ready for use. The status message on the right side of the screen in the admin GUI will read **Registered**.

Now send the profile that you created earlier to the secondary sever:

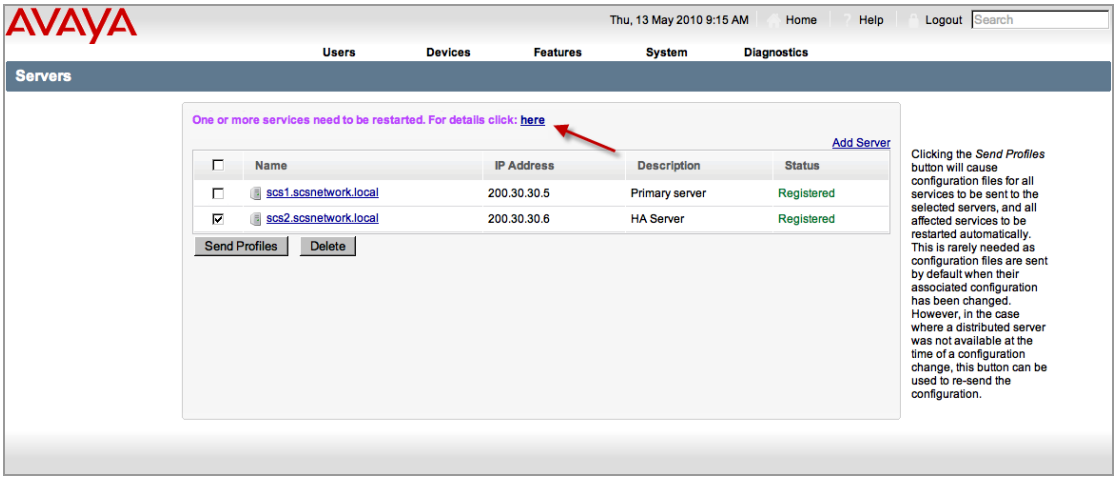
1. From within the **Servers** screen, tick the secondary server's check-box.



2. Click **Send Profiles**.

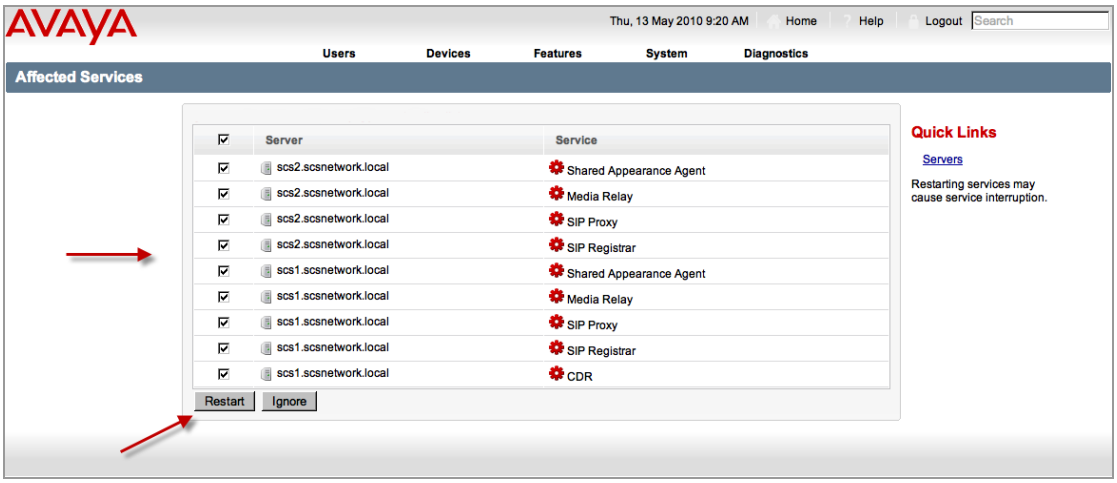
Restart all required services:

1. Click on the **here** link at the top of the screen.



2. Select all available check-boxes and then click the **Restart** button

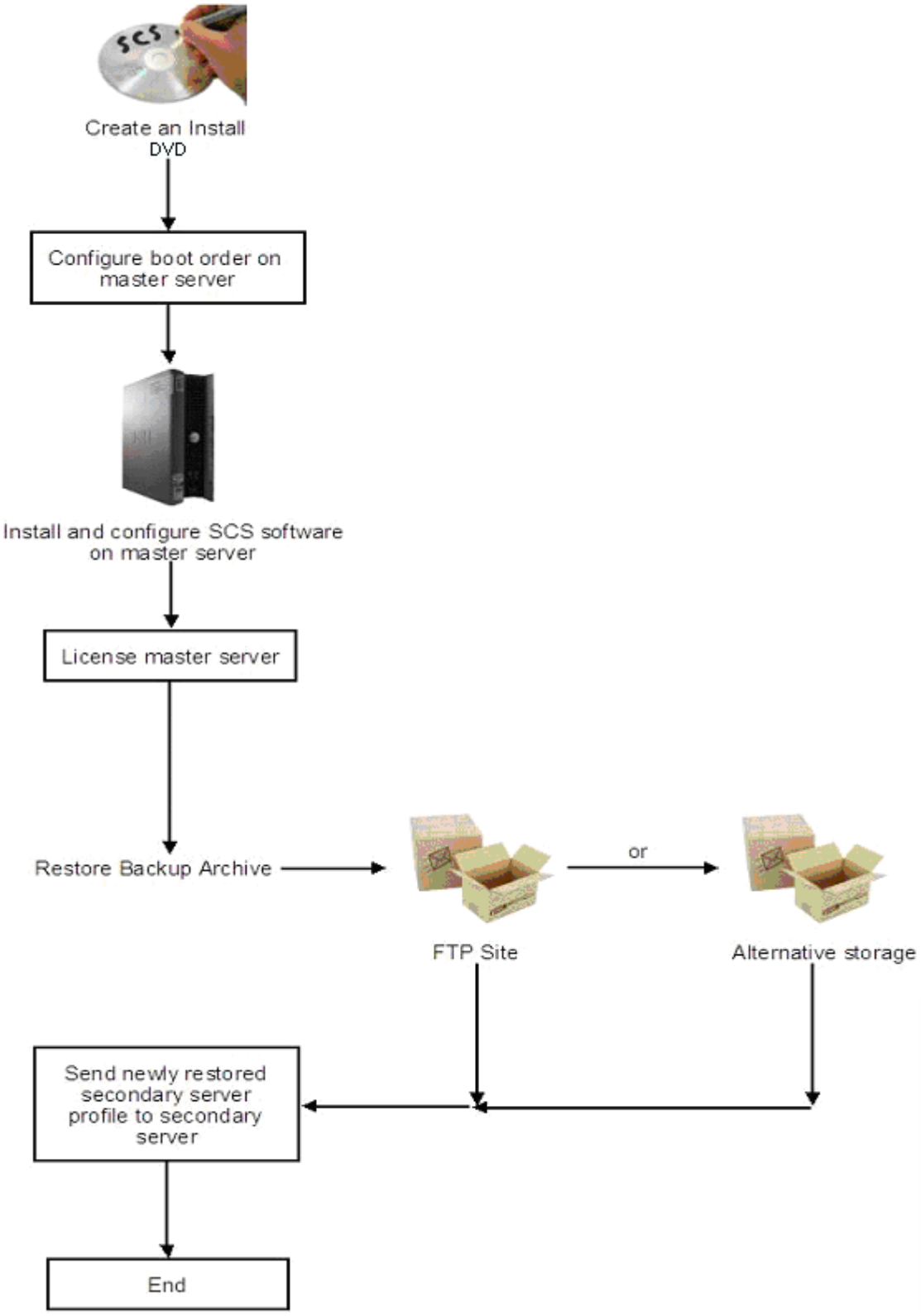
.



Redundant SCS server configuration is now complete.

The master and secondary servers are now reconfigured and synchronised. To ensure speedier recovery in future it is recommended that you implement a regular **Backup and Recovery** policy as part of your Disaster Recovery plan. See ‘Process and Procedure’ earlier in this guide or alternatively the SCS *Backup and Restore* task based guide.

Scenario 2: Rebuilding the Master Server with a Backup Archive



If a backup configuration archive exists in a safe, alternative location then you are already half way to restoring your SCS master server. Once the SCS software has been reinstalled and configured you will be able to restore the configuration archive and then 'send' the secondary server profile to the distributed server. **You will not need to recreate the secondary server profile because it will be contained in the backup archive; you will simply need to 'send' the restored profile information to the secondary server.**

Note: You will only need to send the secondary server profile if the original profile changed *after* the backup was taken but before the master failed, in which case the distributed server configuration will not match the primary server once it has been recovered.

During this solution we will perform the following tasks:

- Create an install disk/USB thumb drive by downloading the SCS software from the Nortel website.
- Configure the master server's boot sequence to ensure that it is capable of booting from the install source.
- Configure the master server.
- License the master server.
- Restore the master server configuration archive.
- Send the secondary server profile from the master to the secondary server.

Creating an SCS Installation Build

Before you can configure your SCS server you will need to download and install the SCS software. You will need:

- Internet access
- Writable DVD/USB thumb drive
- DVD burning software capable of creating a bootable DVD from the ISO image – for example *Infra Recorder*.

Downloading the SCS ISO File

The SCS software is contained in an ISO file, which can be obtained from the Avaya website at http://support.avaya.com. Once downloaded, the ISO file should be burnt to a DVD using a DVD burning package that is capable of creating bootable discs, or written to a bootable USB thumb drive.

Burning the ISO File to DVD

Once you have downloaded the ISO file to a suitable location, you must burn it to a DVD. The DVD will then be used to format the server and install the SCS software. For this reason, it is not enough to simply copy the file to a DVD. The file must be burnt to the DVD and the DVD must be made **bootable** using a disc burning application – such as *Infra Recorder*.

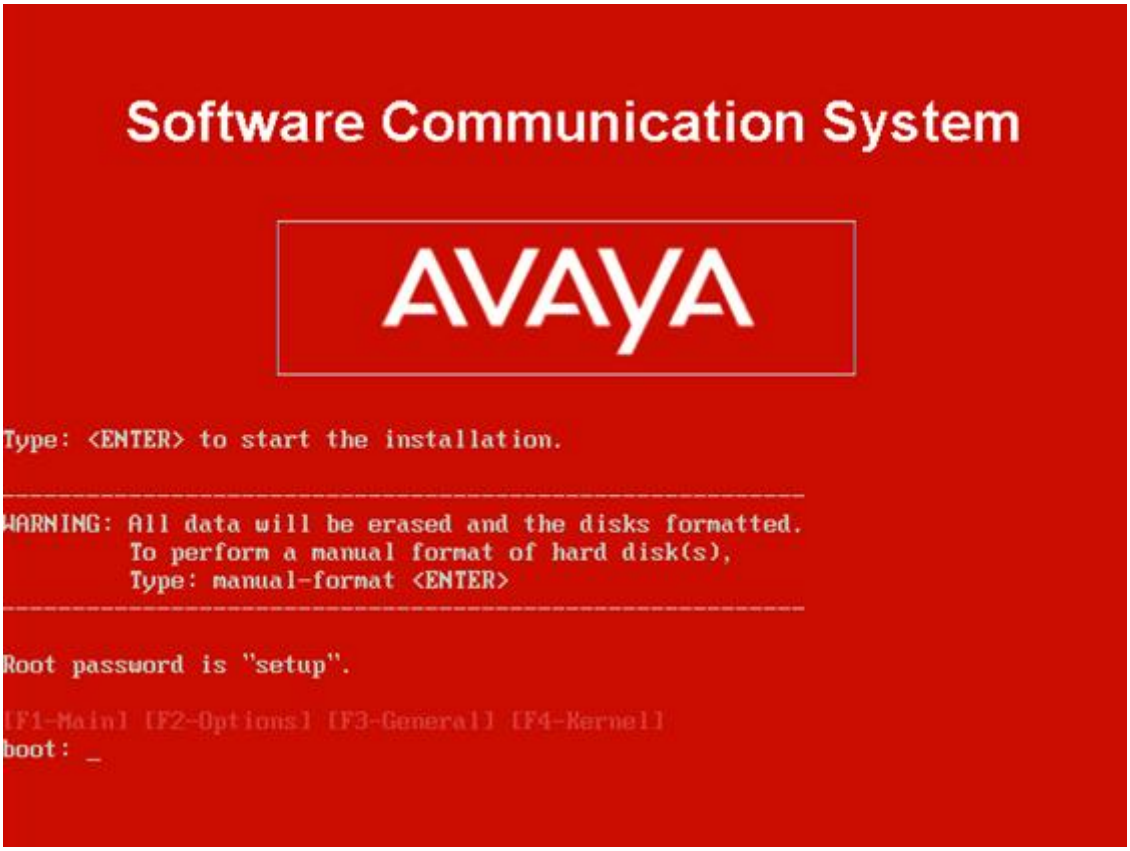
Note: Alternatively, you can copy the SCS installation file to a USB drive and boot from that. See ‘Creating a Bootable USB Image’.

In order to install the SCS software you might need to configure the boot settings so that the server reads the CD drive at power up. This is achieved in the following way:

Note: If your server already boots from the CD drive, simply place the installation DVD in the CD tray, close it and reboot the system.

1. Press the **Power** button to switch the server on.
2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.
3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.
4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.
5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **Onboard or USB CD-ROM Drive**.
6. Use **U** to move it to the top of the list (if the CD-ROM drive is already at the top of the list ignore this step).
7. Press the **Enter** key.
8. Open the CD-ROM tray and insert the SCS installation DVD.
9. Close the tray.
10. Press the **ESC** key to exit System Configuration.
11. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
12. Press the **Enter** key.

The server will reboot from the DVD and automatically launch the format utility. When the Software Communication System screen is displayed, press the **Enter** key to confirm that you would like to format the hard drive and install the SCS software.



The format and installation process takes approximately 10 minutes, when it is complete the CD tray will eject and the system will reboot to the login screen, from where you can begin the installation process. Continue to 'Configuring the SCS Master Server' for guidance on configuring the server.

Creating a Bootable USB Image

Instead of creating a bootable installation DVD you could instead create a bootable USB image. This will involve:

- Writing the SCS ISO image to a 'bootable' USB thumb drive using an application called *ISO2USB*, which can be obtained at http://iso2usb.sourceforge.net
- Re-ordering the boot sequence of the Dell server.

Note: The USB thumb drive must have a capacity of 1GB or more.

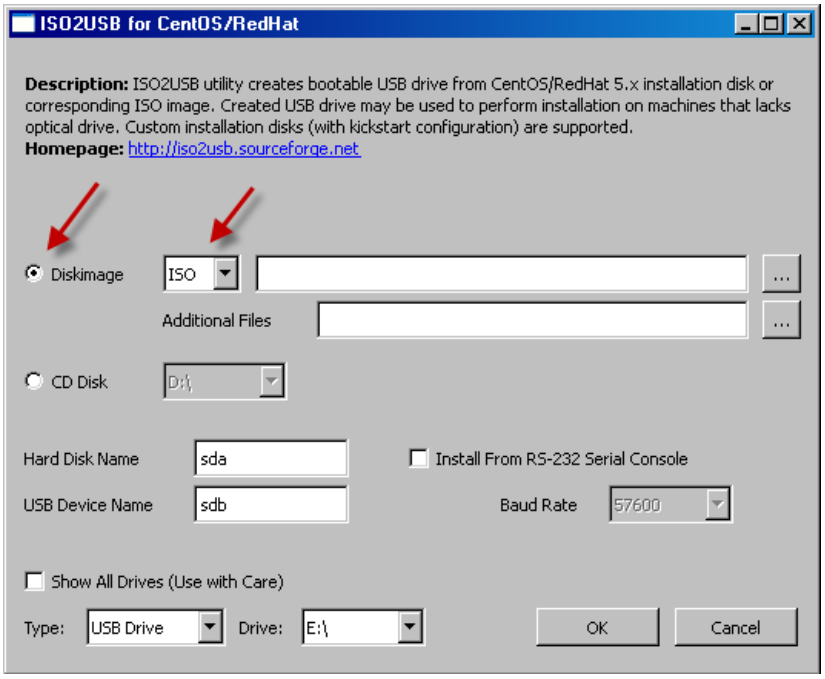
To create a bootable USB drive:

1. Insert a USB thumb drive (ensure that you this is a drive that has no important data on it).

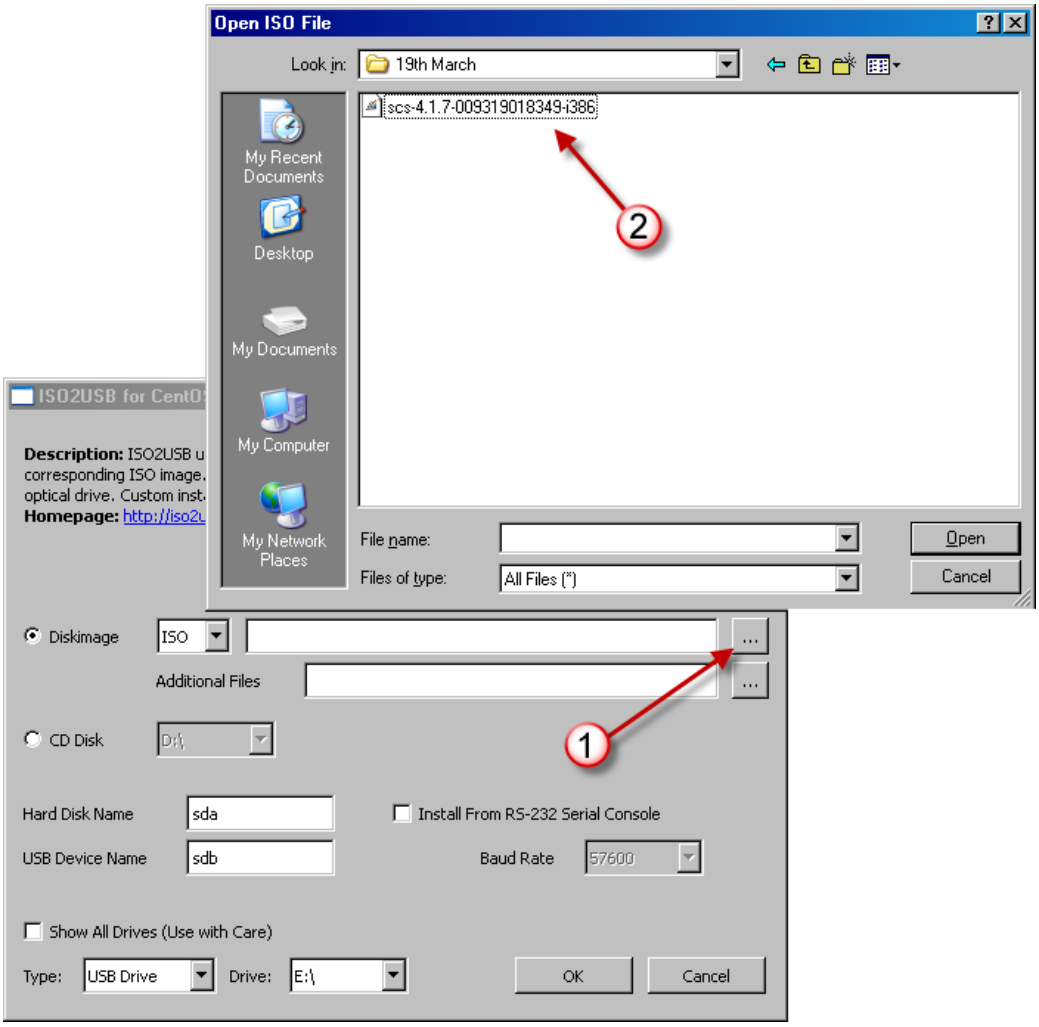
2. Download *ISO2USB*.

3. The package downloads as a ZIP file. Extract the contents and then double-click on **iso2usb.exe** to launch the application.

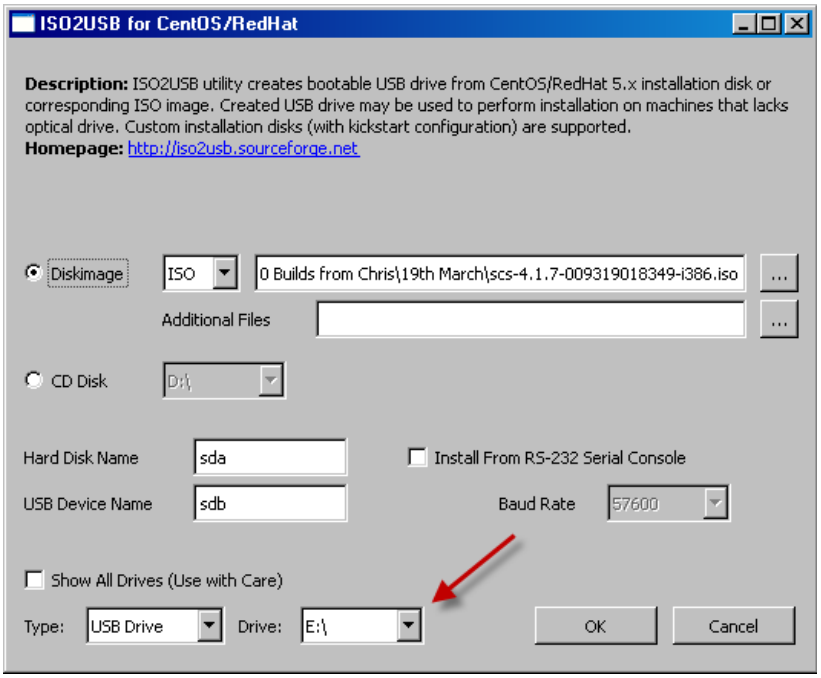
4. Ensure that the **Diskimage** radio button is selected and that **ISO** is selected in the top drop-down menu.



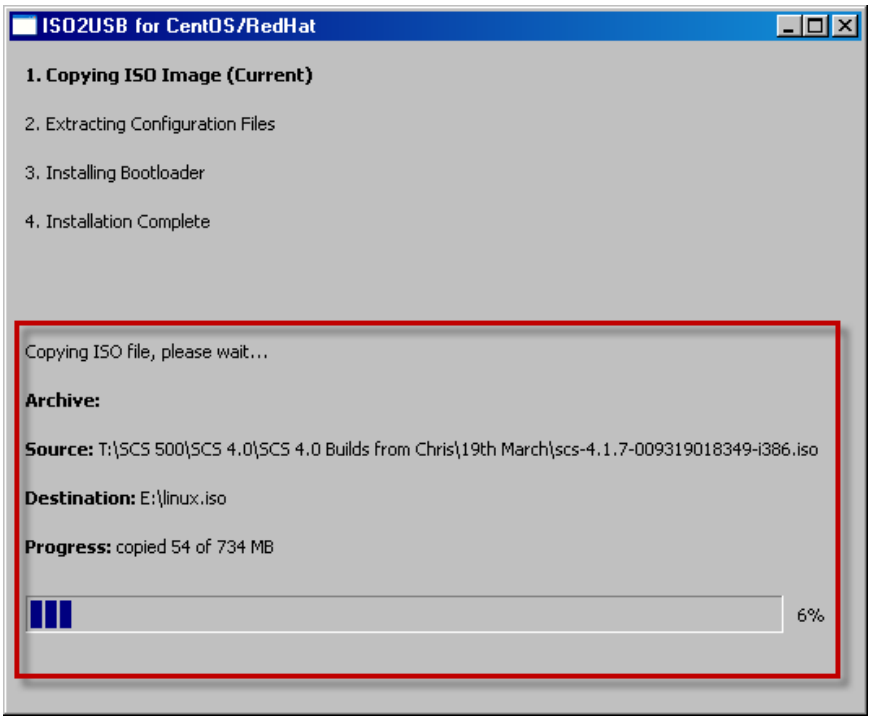
5. Navigate to the location of the SCS ISO image and select it.



6. Select the USB drive from the **Drive** drop-down menu at the bottom of the window and then click **OK**.



7. The image is written to the USB drive.



8. When copying is complete, click the **Exit** button.

You have now created a bootable SCS installation USB drive. Next re-order the boot sequence on the server.

In order to install the SCS software you will need to configure the boot settings so that the server reads the USB drive at power up. This is achieved in the following way:

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **USB Device**.

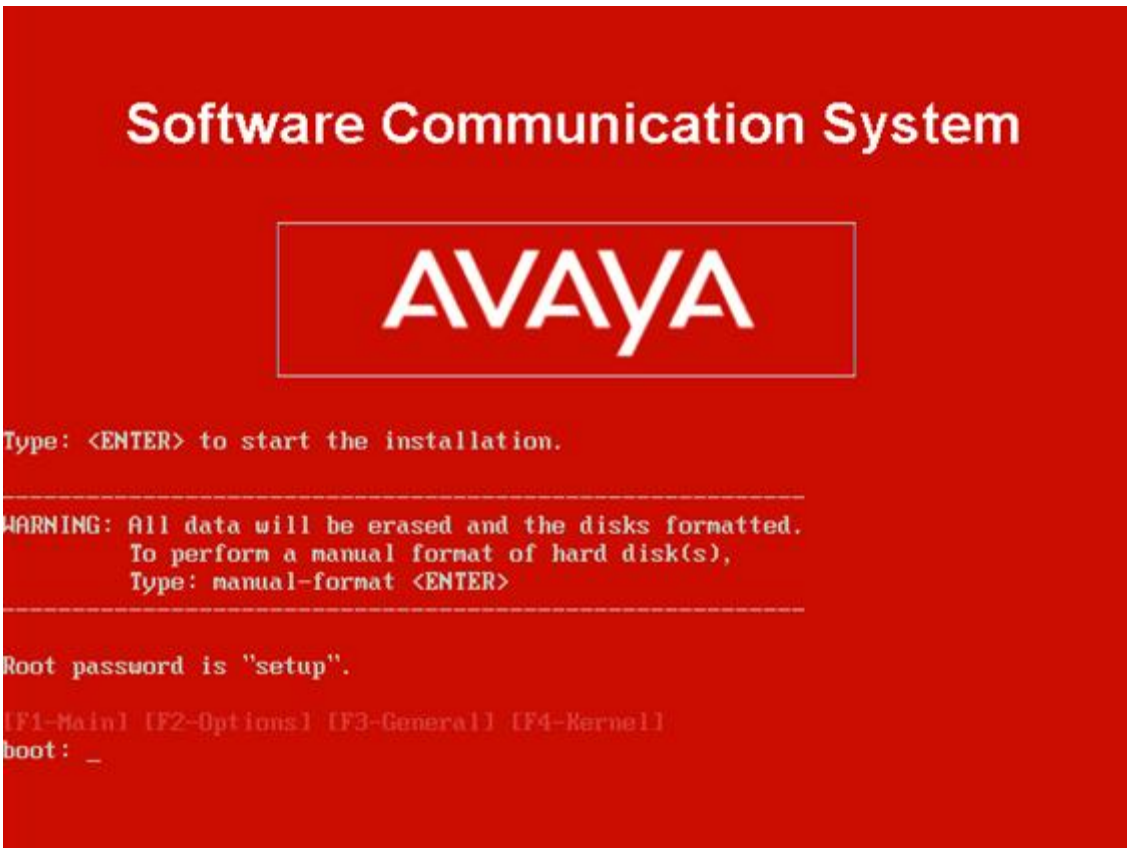
6. Use **U** to move it to the top of the list

    b. On some servers it may be necessary to 'enable' the USB device as a boot option. Press the **Space** bar if **USB Device** does not have a priority number next to it. A '**1**' should appear next to the drive.

7. Press the **Enter** key.
8. Insert the USB thumb drive
9. Press the **ESC** key to exit System Configuration.
10. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
11. Press the **Enter** key.

The server will reboot from the USB drive.

When the red Avaya screen is displayed press **Enter**.



A ‘kickstart’ error will be displayed, this is normal. Simply use the **down** cursor key on your keyboard to highlight the **OK** button and press **Enter** to launch the format utility. When formatting is complete the SCS software will be copied to the server’s hard drive.

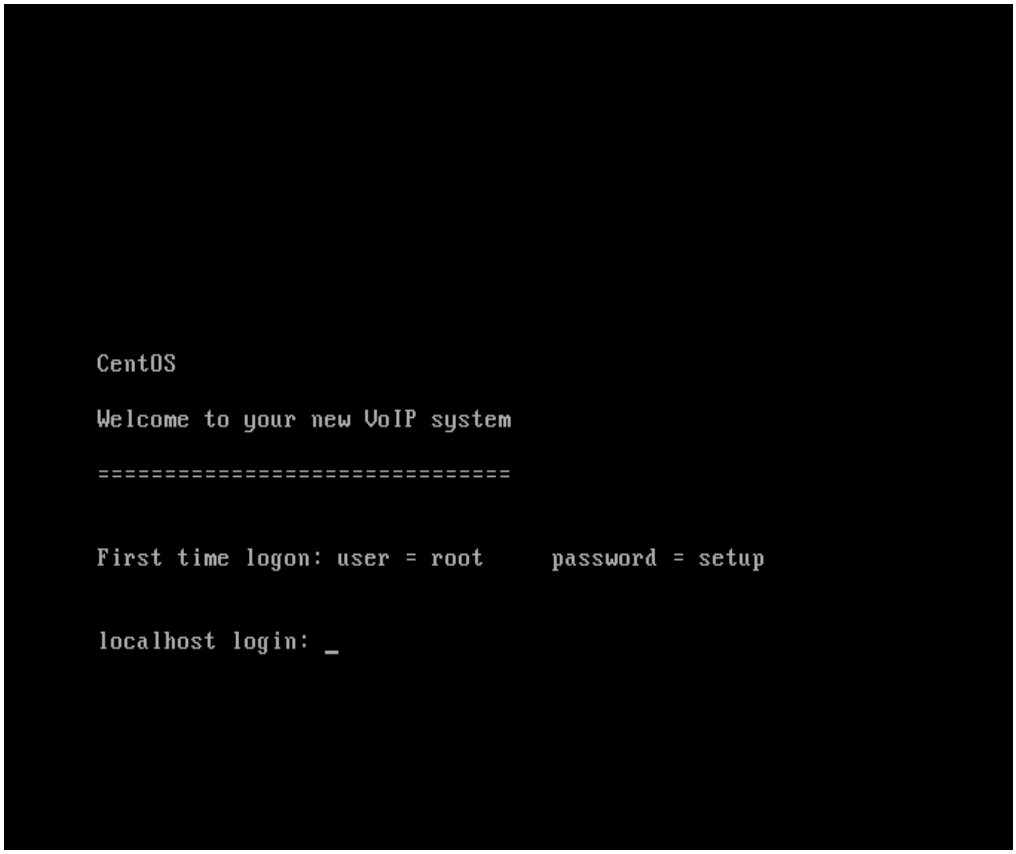
The format and installation process takes approximately 5 minutes, when it is complete the system will announce a reboot – **Ensure that the USB drive is removed from the USB port before the reboot begins otherwise the system will reboot from the thumb drive again**. If you are unable to remove the USB thumb device before the system reboots, wait for the red Avaya

screen to appear, remove the thumb drive and then press **CTRL-ALT-DEL** to reboot the server.

The system will boot to a login screen.
Once installation is complete you will be presented with a login screen.

1. To begin the setup process, enter the following username and password to access the configuration utility:

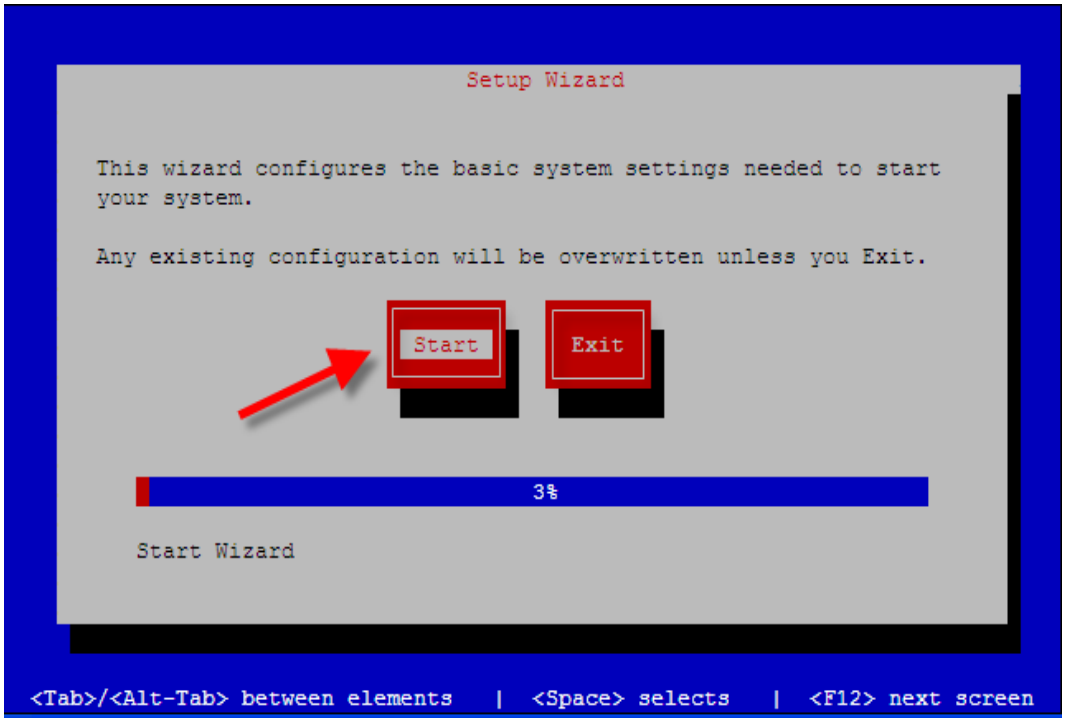
   Localhost Login: `root`
   Password: `setup`



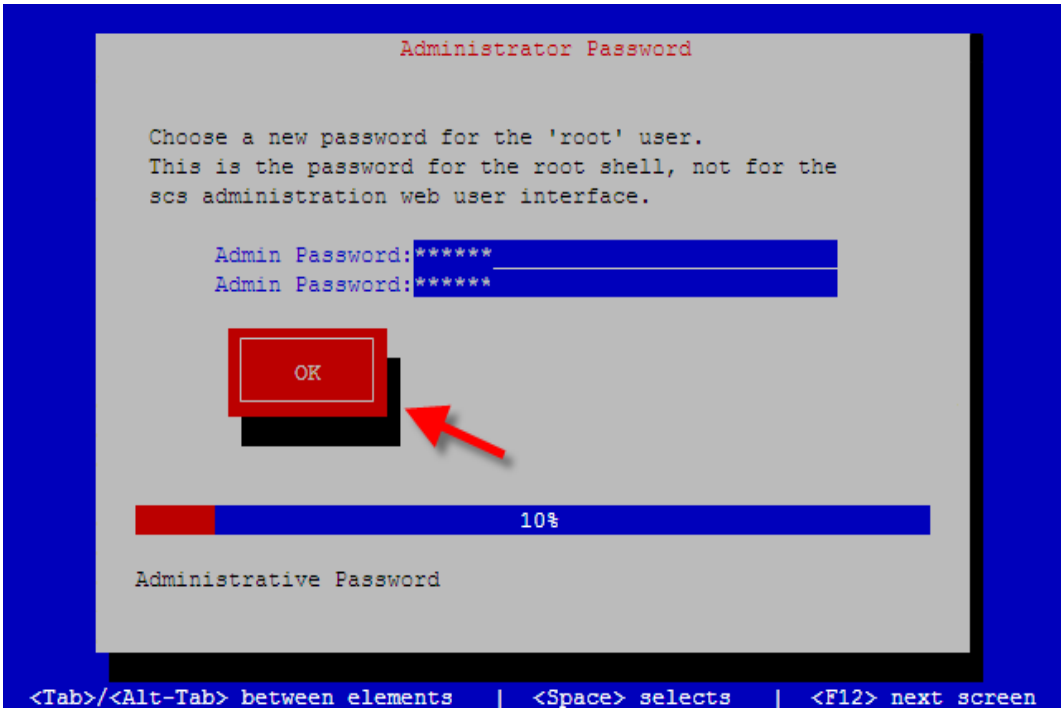
   If at any time during the setup process you make an error, reboot the server and log in using the same username and password. At the command prompt type **sipxecs-setup-system** and press **Enter** to reload the configuration utility from the start.

   Note: The SCS domain cannot be changed by running sipxecs-setup-system. The only way to reconfigure the domain is to access the Domain facility from the administrator GUI.

2. When the configuration utility has finished loading, highlight the **Start** button and press **Enter**.



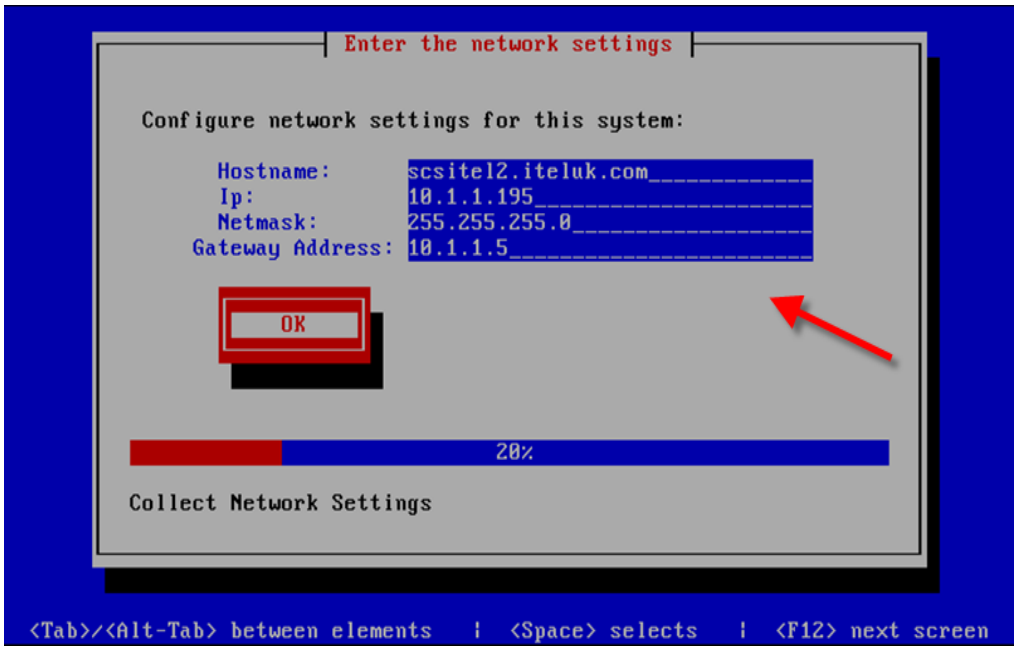
3. Enter the **Admin Password** twice. This is the password that engineers and administrators will enter to gain access to the SCS server locally via the Linux operating system (where you are now). Highlight the **OK** button and press **Enter** when you are ready to continue.



4. Enter the following LAN settings (enter these settings exactly as they were configured on the old system, otherwise the archive restore will fail):

c. **Hostname** – This is the fully qualified domain name (FQDN) of the SCS server as defined in the DNS records.
d. **IP** – The IP address that has been assigned for use with the SCS. Again, this must be consistent with the address defined in the DNS settings.
e. **Netmask** – The network's subnet mask.
f. **Gateway Address** – The address of the default router providing access to the Internet.

If you are unsure of any of these settings, see the network administrator.

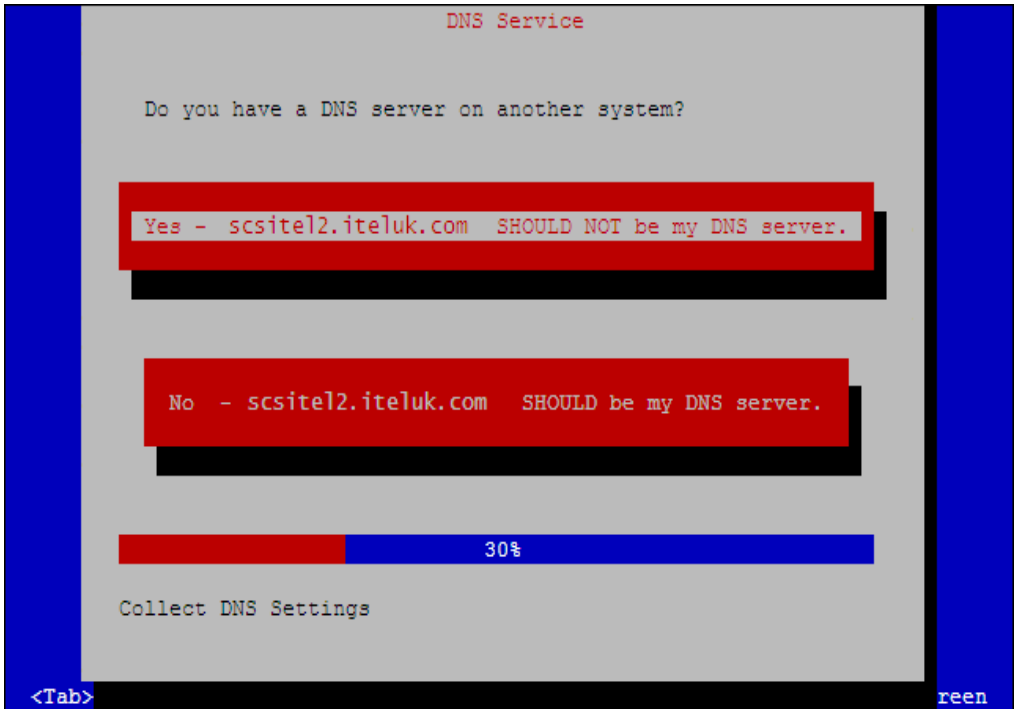


5. The installation wizard will now query whether or not you have DNS configured on the network. The SCS can be configured to function as a DNS server on the network if you do not have DNS or are unable to configure the records required by the SCS.. To enable the SCS onboard DNS, select **No xxx.xxx.xxx should be my DNS server**.

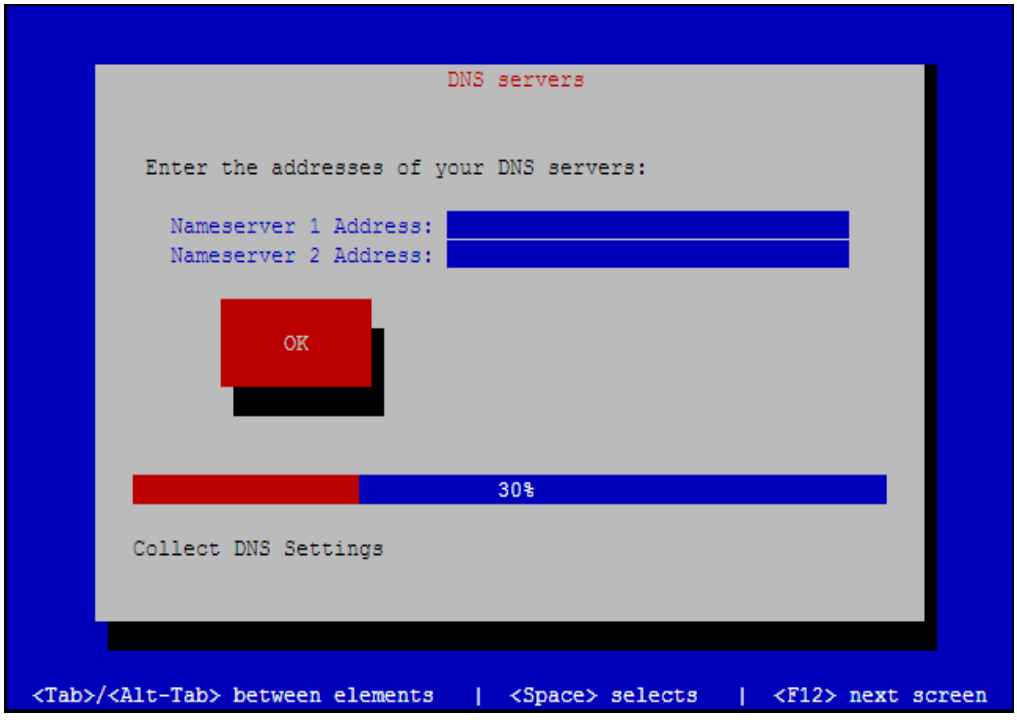
Note: If the DNS service is enabled on the first server it will replicate on the secondary server automatically.

Note: The onboard DNS will create all necessary records required by the SCS in order for it to function correctly.

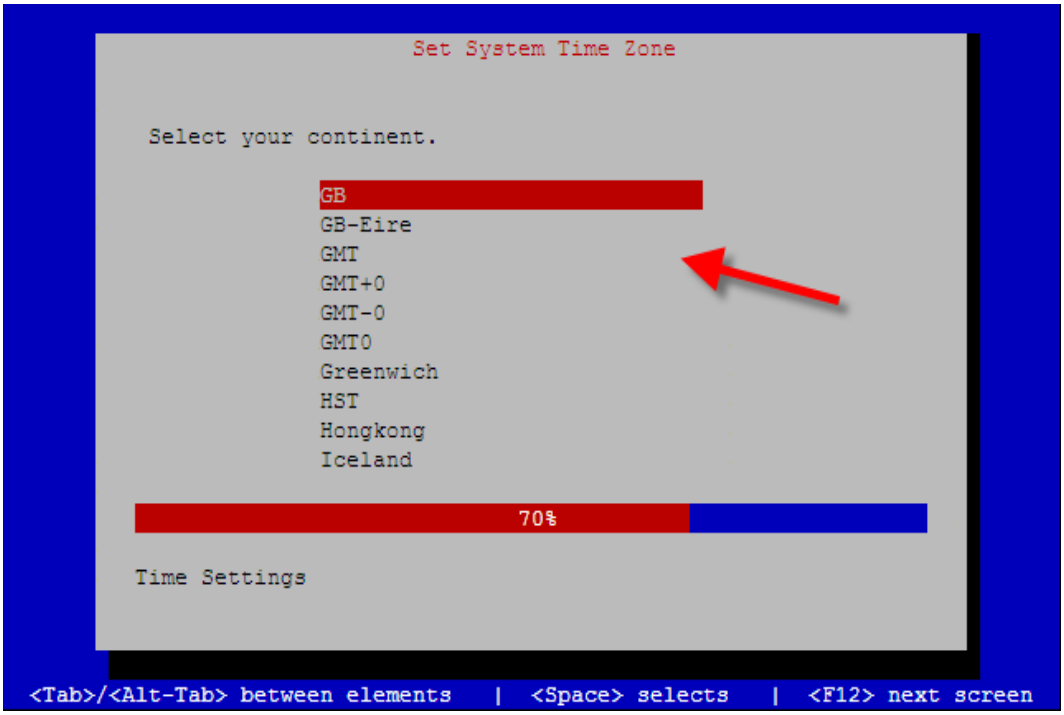
Note: If you elect to enable the SCS's onboard DNS the next screen will offer you the opportunity to define upstream DNS servers if you wish. If the network utilizes Intranet DNS or DNS from an IP service provider then these server addresses can be entered on the next screen. Note that this is an optional configuration step and the fields can be left blank if required, however without these addresses, name and address resolution may prove difficult since the SCS will not be able to resolve *all* DNS queries.



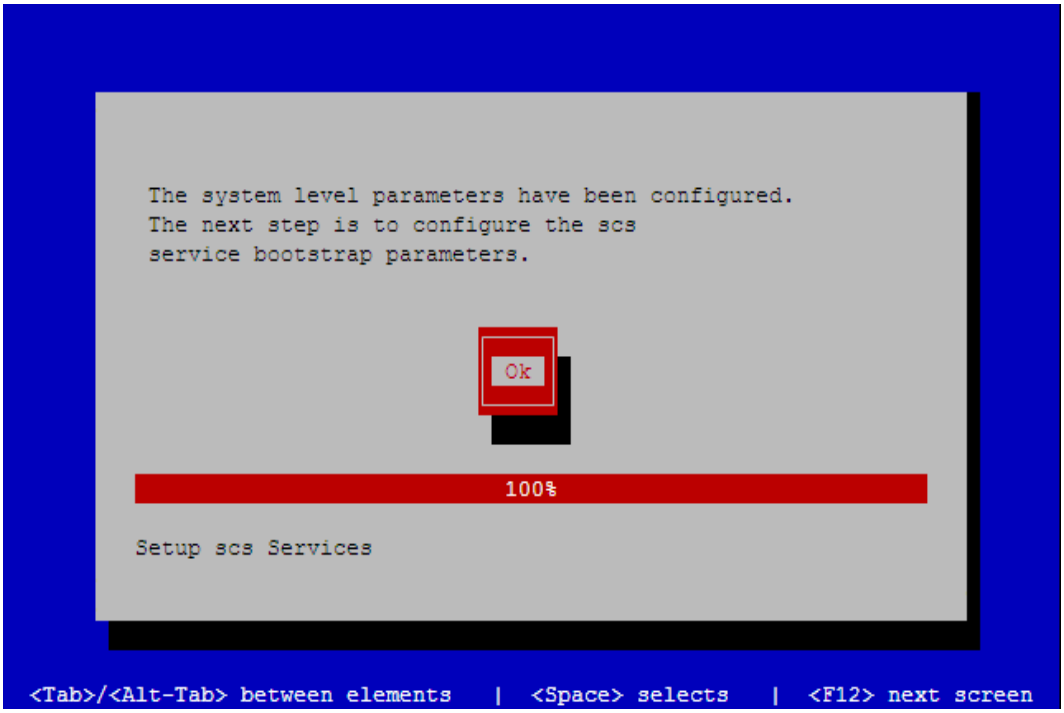
If you already have DNS configured for the SCS select **Yes xxx.xxx.xxx should not be my DNS server**. Note that in this instance the next screen will ask you to configure the address of a primary and secondary DNS server.



6. Select a region or country to set the time zone in which the SCS is situated – if you pick a region, such as ‘Europe’, you will be prompted to then define an area within that region, for example, ‘London’.



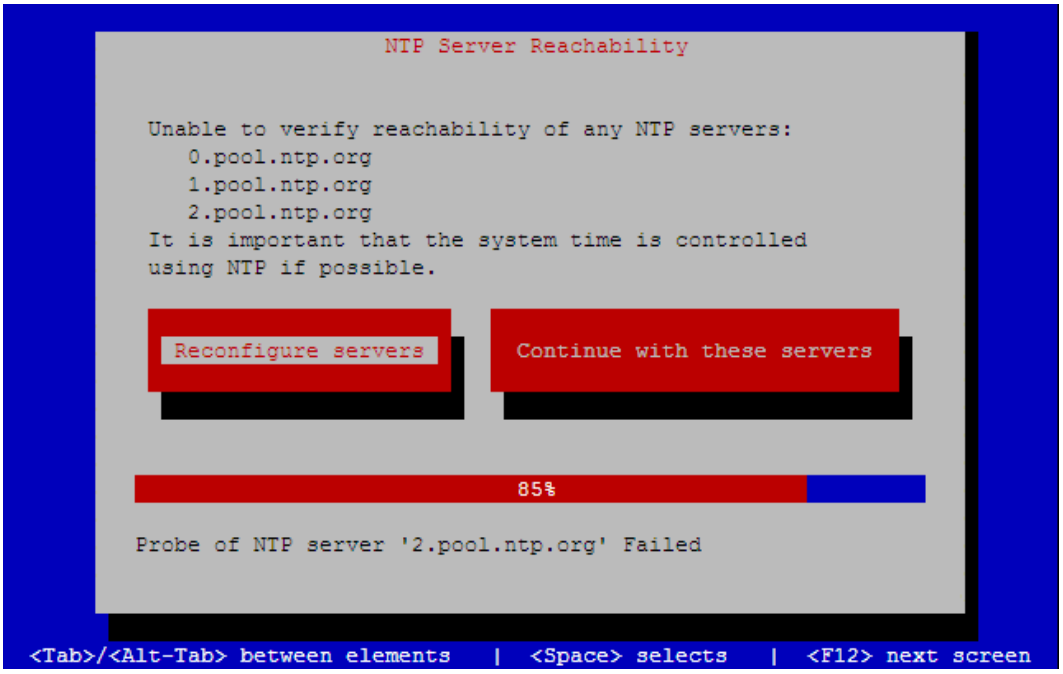
7. The system will now search for NTP servers in order to set system time. By default the SCS is programmed to attempt a connection to a series of Internet-based time servers. If it cannot connect to any of these servers you will be asked to either: 1) move on with the current time server configuration, in which case you will have to set the time manually - see Step 7b; 2) configure the address of a different time server. If the SCS successfully gathers NTP data the following message will be displayed:



Note: The NTP server search can take a while. Do not power off or disconnect the SCS during this process, even if it seems that nothing is happening.

Press **Enter** and continue to Step 8 if you see this message.

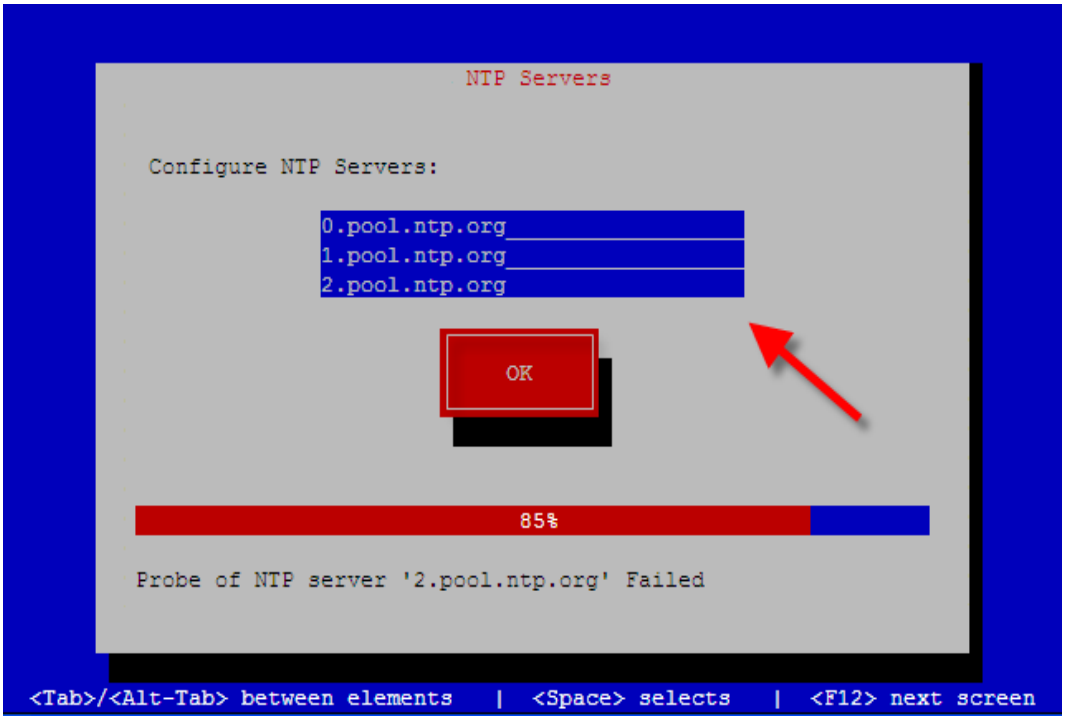
If you see the message below regarding NTP servers continue to Step 7a.



a. You now have the choice of configuring a different set of NTP servers or continuing with the default settings and configuring the time manually on the next screen.

   i. To set new NTP servers, highlight **Reconfigure servers** and press the **Enter** key.

   ii. Enter the new NTP addresses and then highlight the **OK** button and press **Enter**.



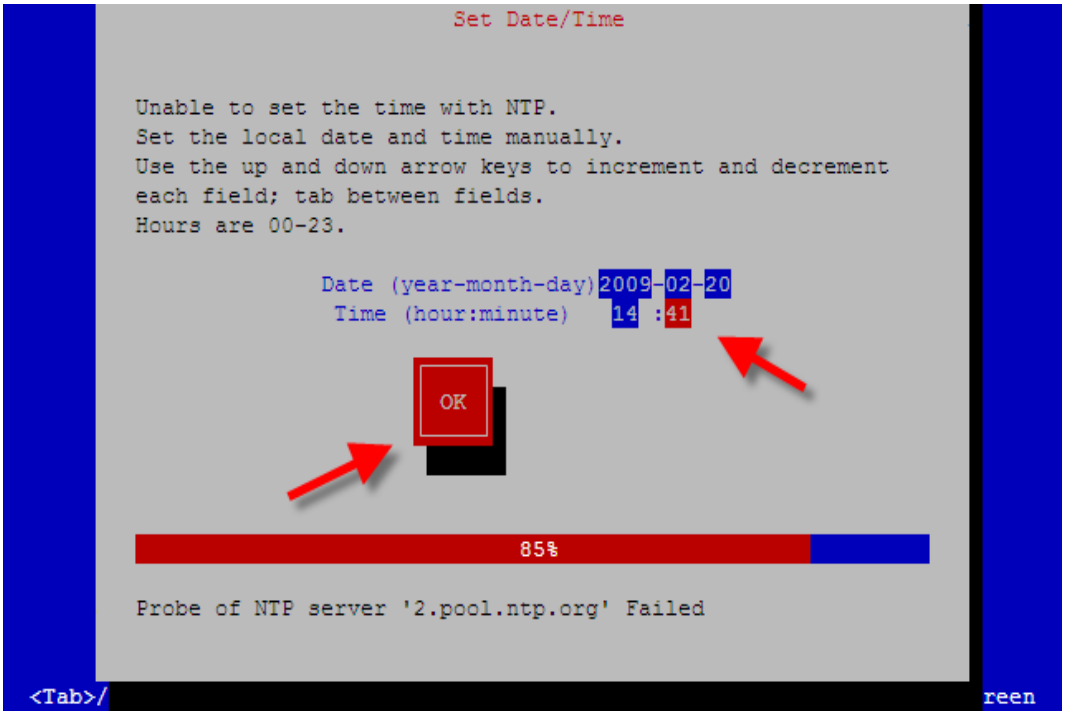
iii. The SCS will attempt to connect to the defined NTP servers.

iv. When a connection is successful press **Enter** to clear the confirmation screen and then continue to Step 8.

b. Instead of configuring alternative NTP servers you can set the time manually.

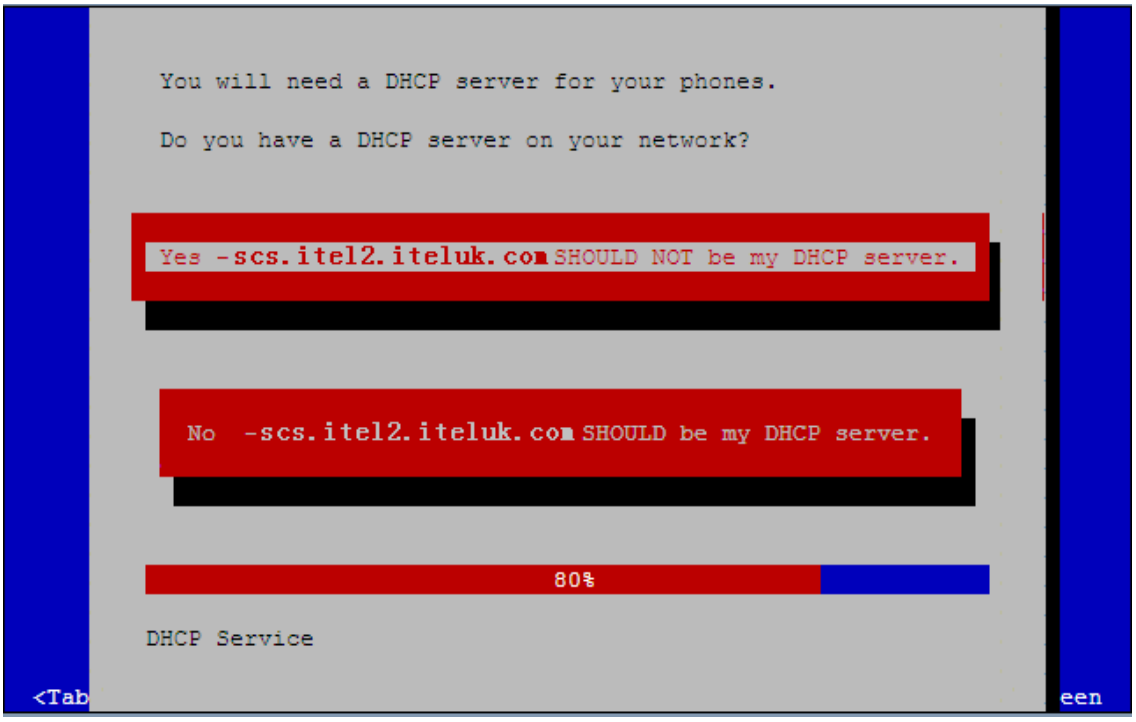
i. Highlight **Continue with these servers** and press **Enter**.

ii. To set the time, use the **left** and **right** cursor keys to move between the fields and the **up** and **down** cursor keys to adjust each value. The time should be set in 24-hour format. Highlight the **OK** button and press **Enter** to continue.



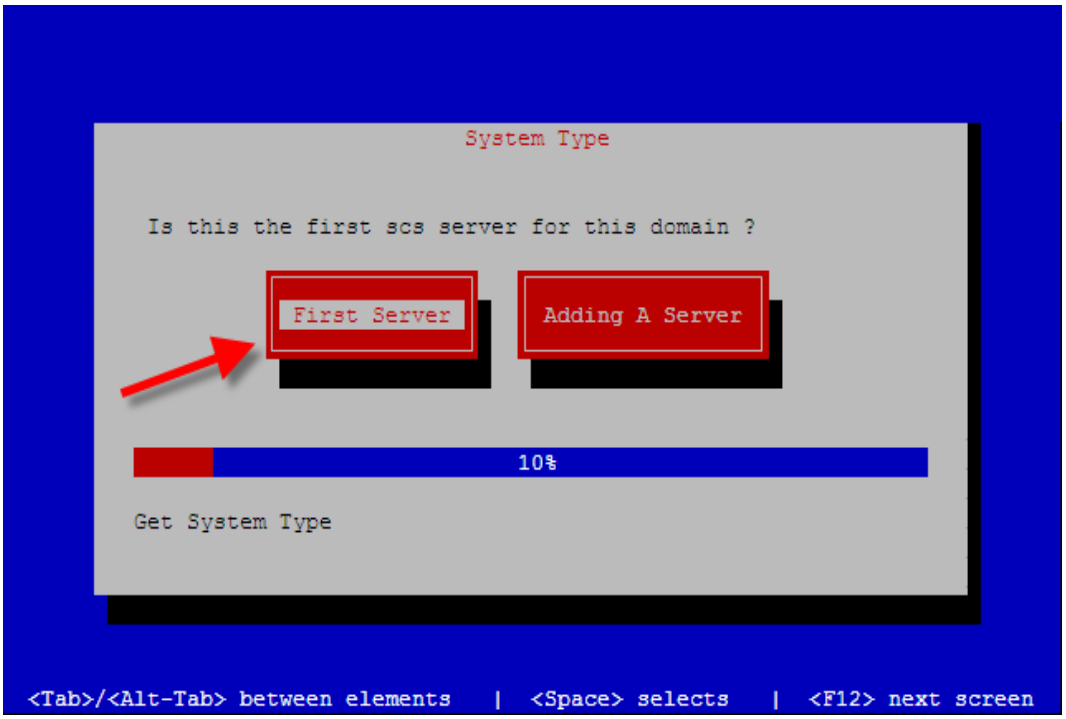
iii. Continue to Step 8.

8. The SCS can provide a DHCP service in order to provide devices joining the network with IP addresses. To enable the DHCP service select **No**.



Note: If a DHCP service is already active on the network **do not** enable the onboard DHCP service since this will cause a conflict.

9. You now need to configure some settings that will define this server as your primary SIP server. First, define the server as your 'First Server'. Highlight **First Server** and press the **Enter** key.

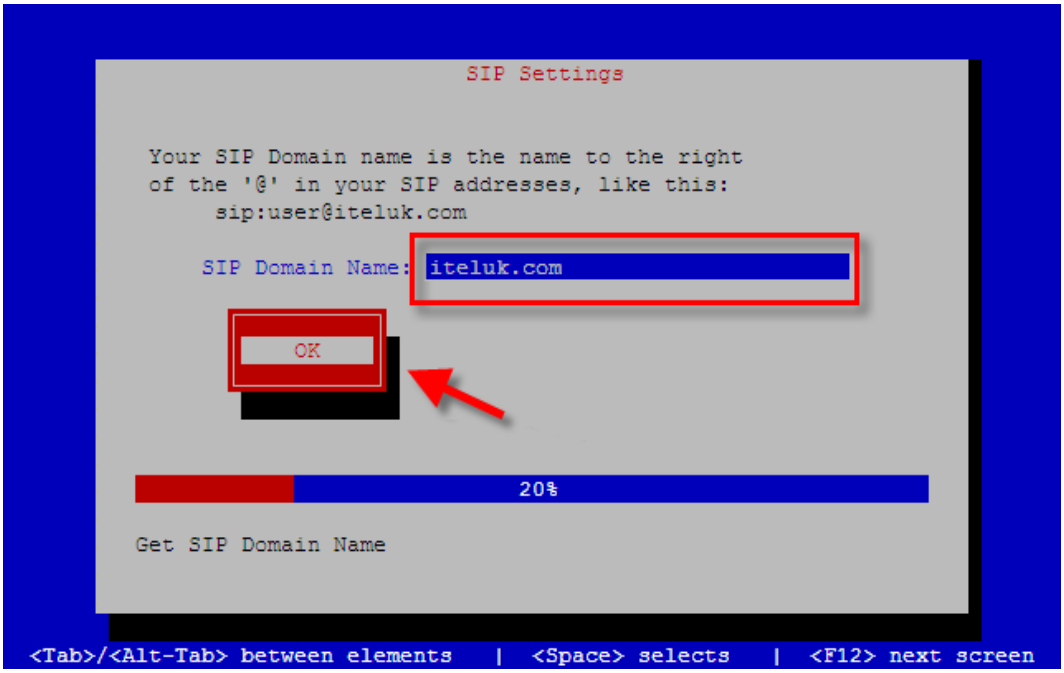


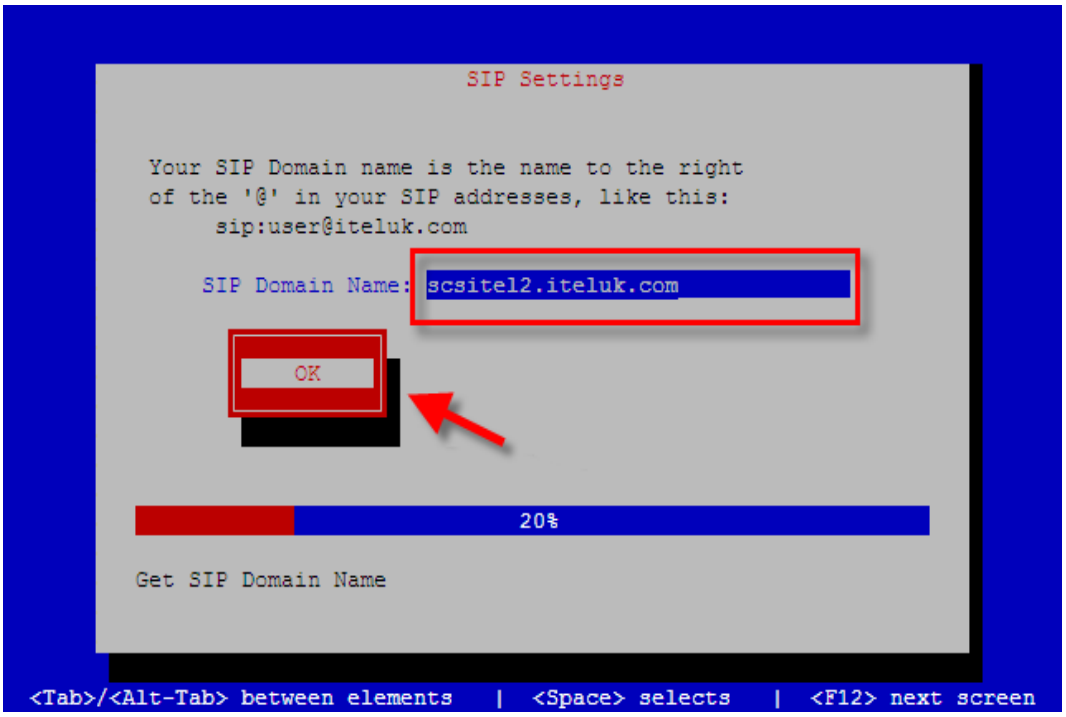
Next set the SIP Domain. Knowledge of your network configuration is vital at this stage. Next set the SIP Domain. Knowledge of your network configuration is vital at this stage. Because you are dealing with an HA configuration, all required DNS SRV records should already be in place, the SIP domain should simply be entered as the domain name: e.g, *scsdomain.com*. In an HA scenario the SIP domain is **never** entered as a fully qualified domain name (FQDN). By default the wizard will enter the domain name in the correct format.

In the example illustrated below the SIP domain has already been entered as *iteluk.com* by the wizard.

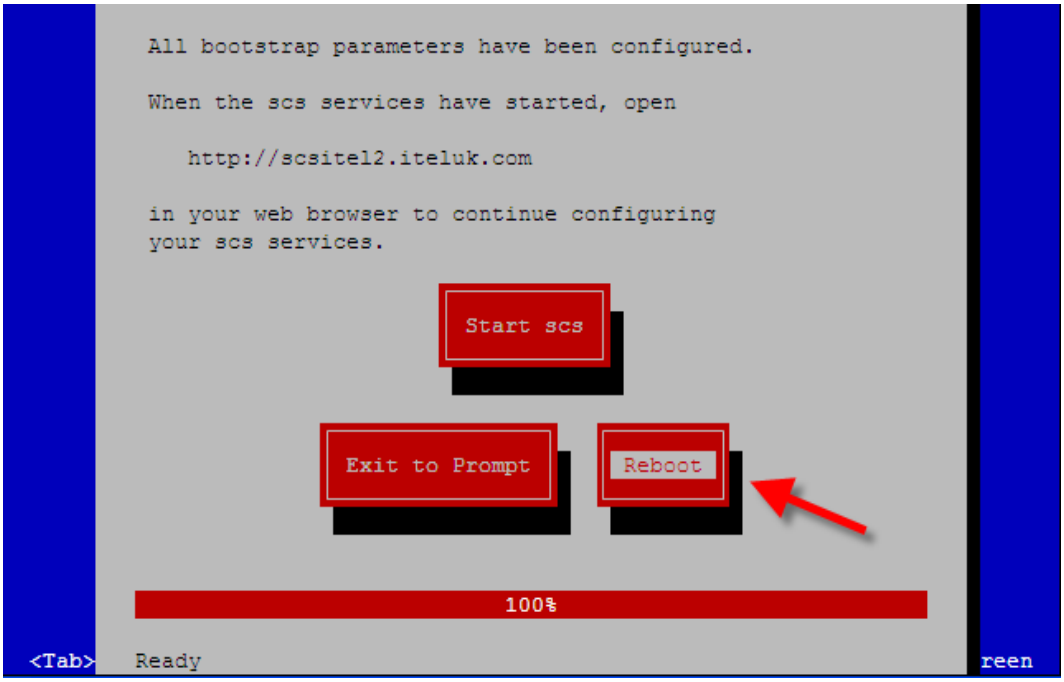
Note: If you elected to activate the SCS's own onboard DNS, SRV records will be created automatically you should therefore leave the SIP Domain entry as the default entry.

Highlight the **OK** button and press the **Enter** key when you are ready to continue.

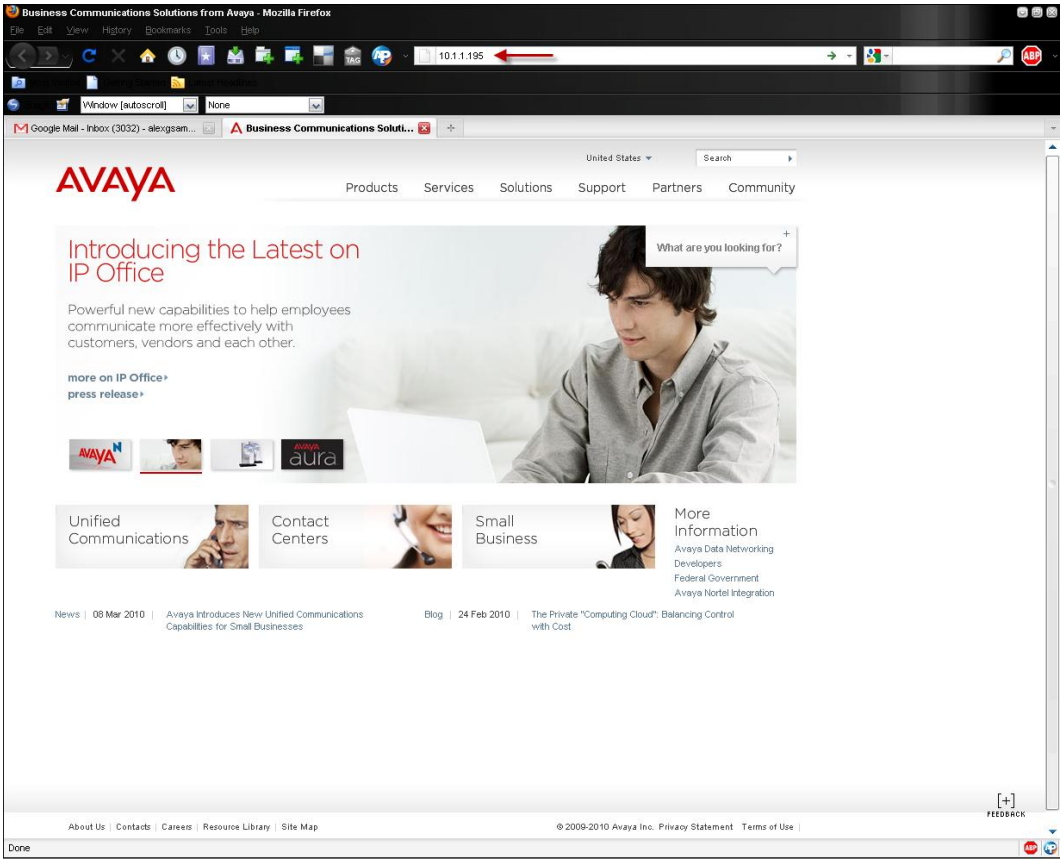




10. Configuration of the SCS server is now complete. Highlight the **Reboot** button and press the **Enter** key to restart the server.



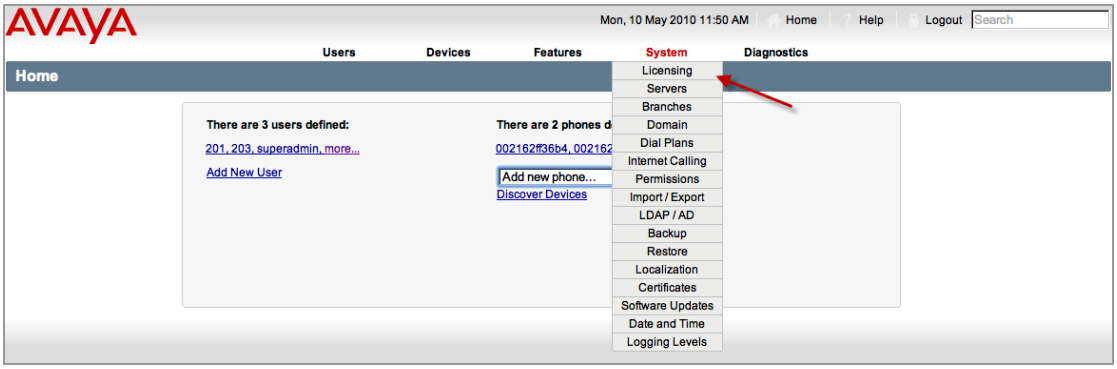
When the server has restarted, administration of the system can be carried out via the web-browser interface, which can be accessed from a remote workstation/laptop by navigating to the server's address or host and domain name in a web browser. See the SCS 'System Configuration' guide for guidance on next steps.



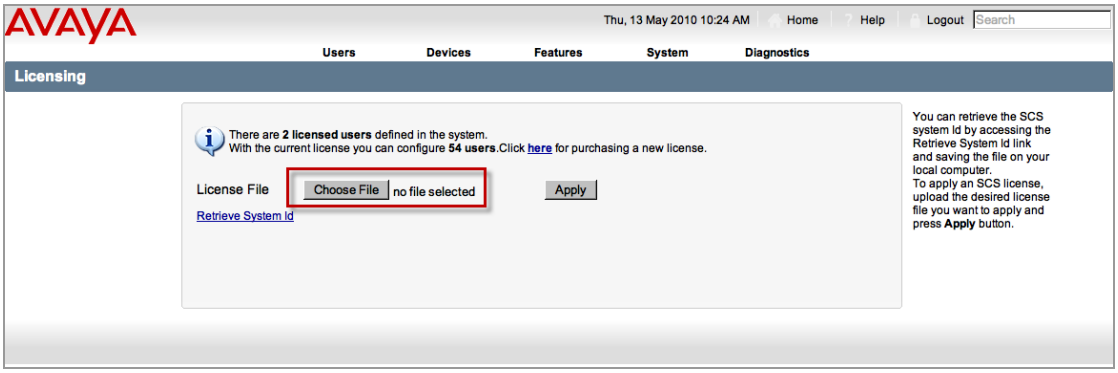
Licensing the System

Now that the Master server is installed and configured you will need to licence it before you can commence creating user and device profiles.

1. Place the mouse pointer over the **System** menu and select **Licensing**.



2. To apply your license file, click the **Choose file / Browse** button and browse to the location of the file. When you have selected a file, click the **Apply** button.



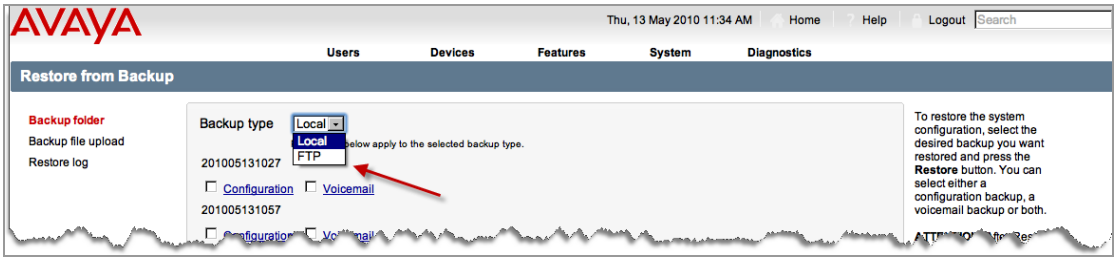
3. The license file will be applied to the SCS system, enabling the configuration of users based on the number of users purchased.

Once the system is licensed you can restore the configuration archive.

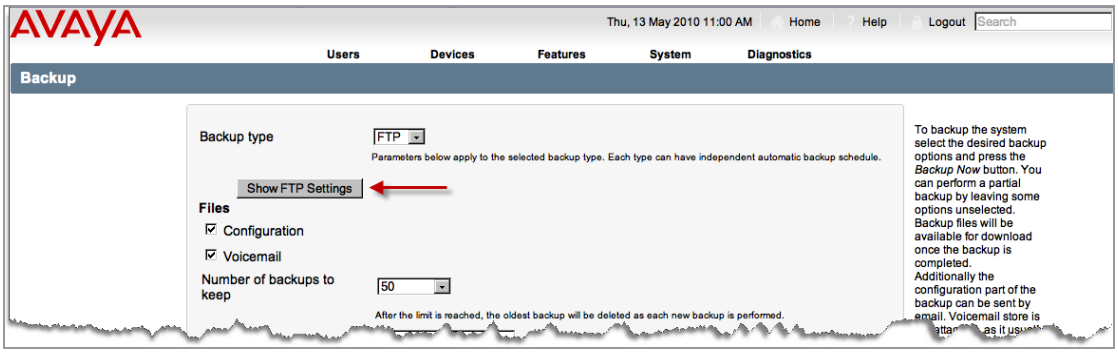
Restoring Backup Archives

1. By default, when you open the restore window you have the option of restoring from the local archive store on the SCS or your chosen FTP server. Since you have rebuilt the system a local restore is out of the question, but you might still wish to restore from an FTP location. Use the drop-down menu to select **FTP**.

   To restore from another source, click on the **Backup file upload** menu option on the left-hand side and follow the instruction found in the following section, ‘Restore by File Upload’.

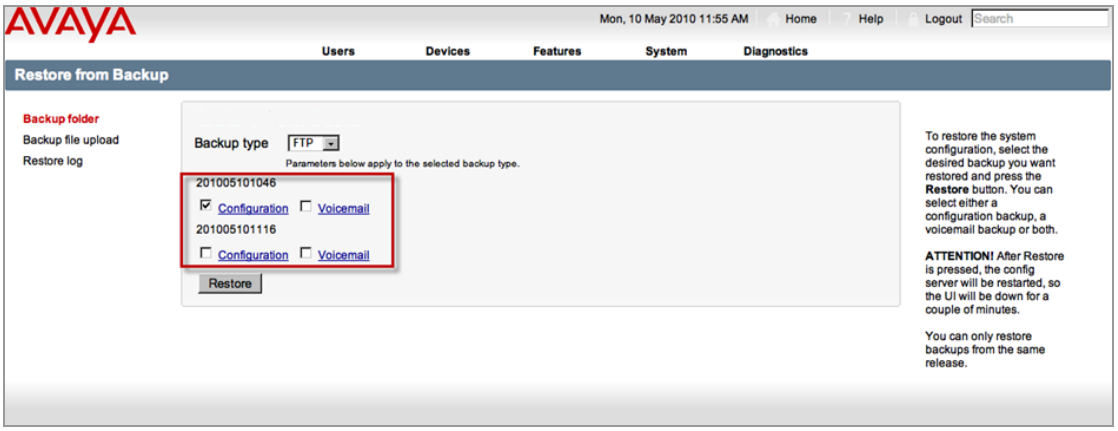


2. Click on **Show FTP Settings** to configure server name, username and password values, and then click **Apply**.



Note: Any of the backup files listed on this page can be saved to another location by clicking on the relevant link, e.g., **Configuration** or **Voicemail**.

3. Select the archive you would like to restore by ticking the corresponding check-box.



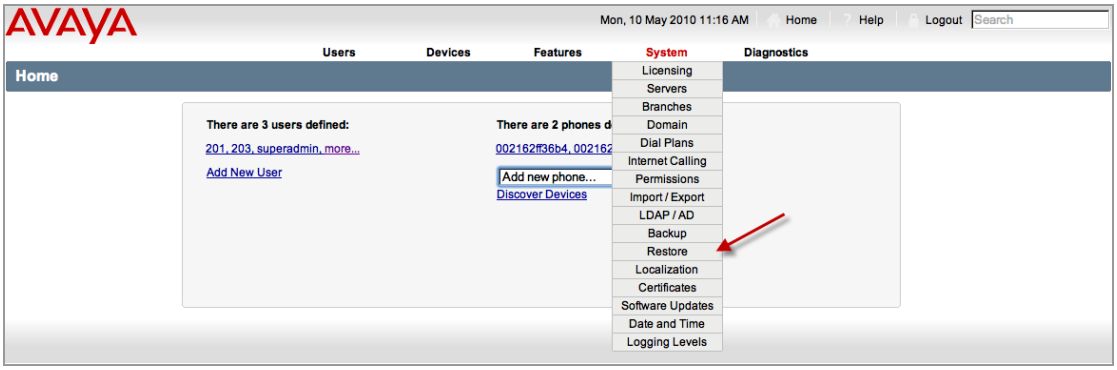
4. Click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

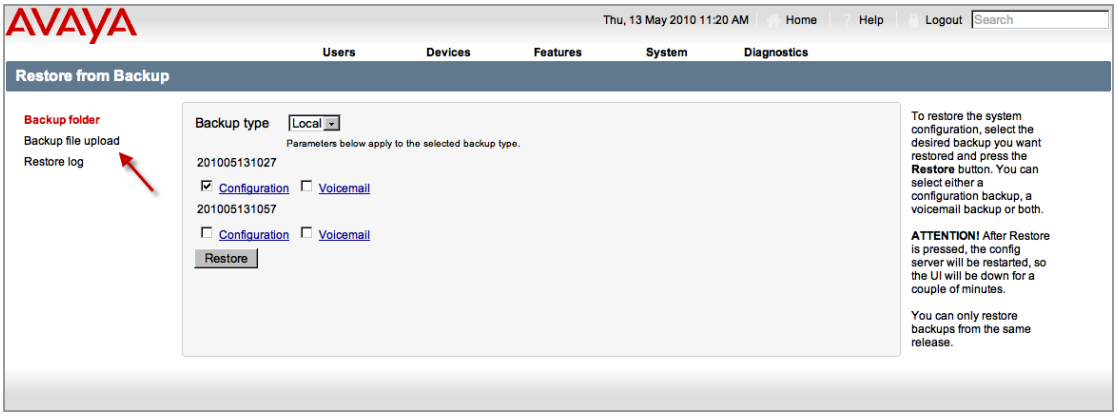
Restoring by File Upload

In the absence of an FTP server, it is still possible to save backup archives to a secondary location for safe keeping. To restore archives from this secondary location follow these steps:

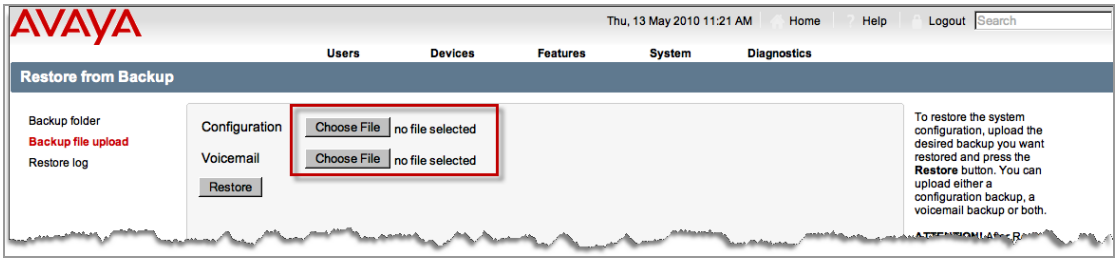
1. Open the **System** menu and select **Restore**.



2. Click on **Backup file upload**.



3. To restore a Configuration file, click on the corresponding **Choose file / Browse** button, to restore a Voicemail file, click on the corresponding **Choose file / Browse** button.



Note: the interface will display an error message if you attempt to enter a voicemail file in the **Configuration** text box and vice versa.

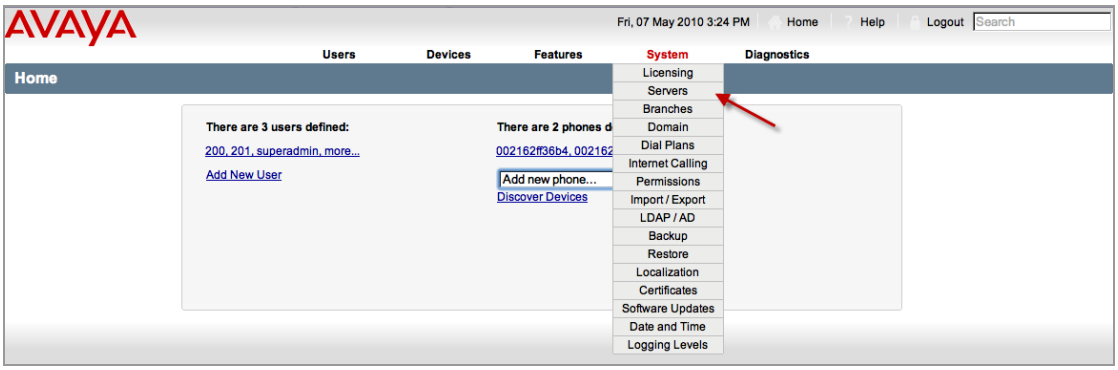
4. When you are ready to continue, click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

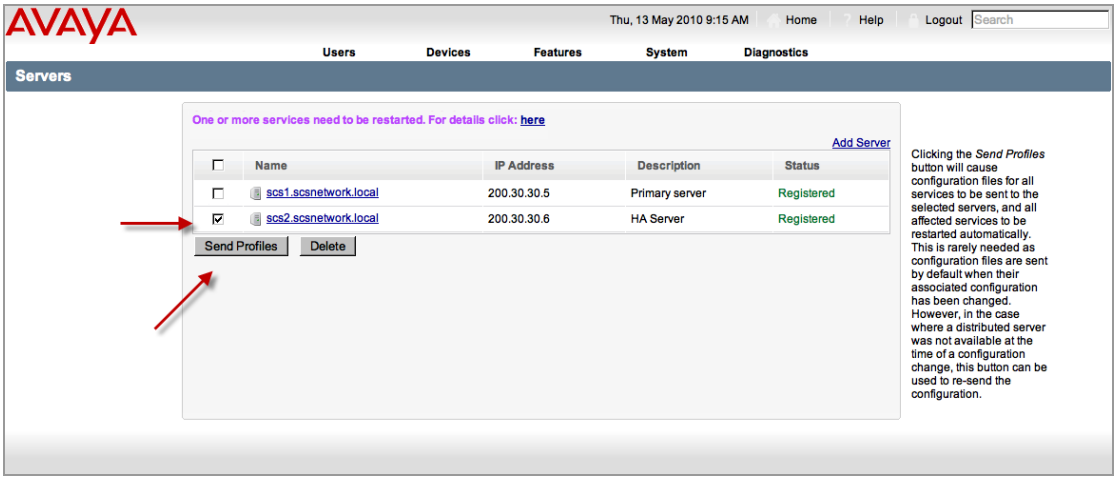
Sending Server Profiles

If the secondary server configuration has changed since the backup was taken – for example if a major configuration change occurred on the master server and was then replicated on the secondary prior to master failure - then it will be necessary to 'resend' the secondary server profile to the secondary server in order to bring its configuration in line with the newly restored master server.

1. Navigate to the servers page by opening the **System** menu and clicking on **Servers**.

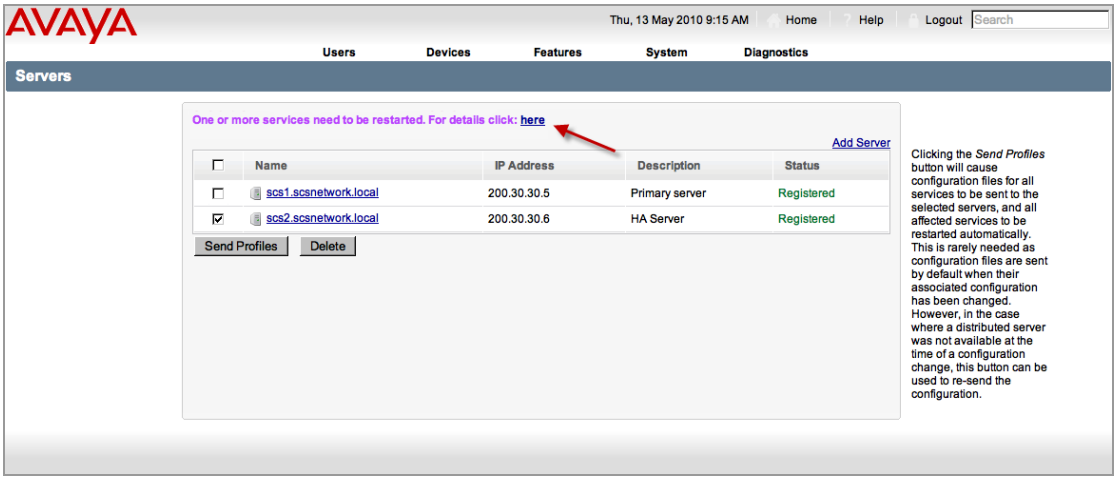


2. The server list is displayed, select the secondary server by ticking its check-box and then click **Send Profiles**.



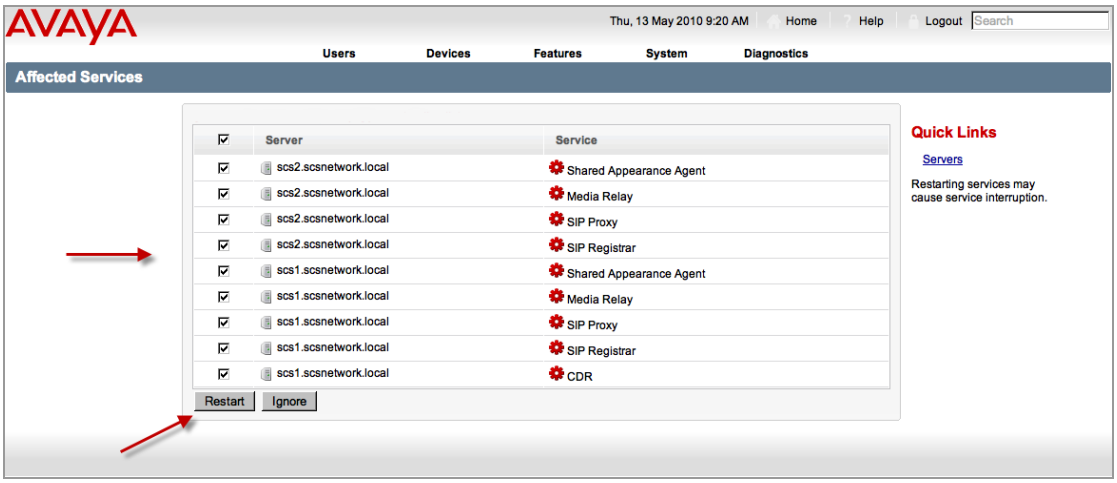
Restart all required services:

1. Click on the **here** link at the top of the screen.



2. Select all available check-boxes and then click the **Restart** button

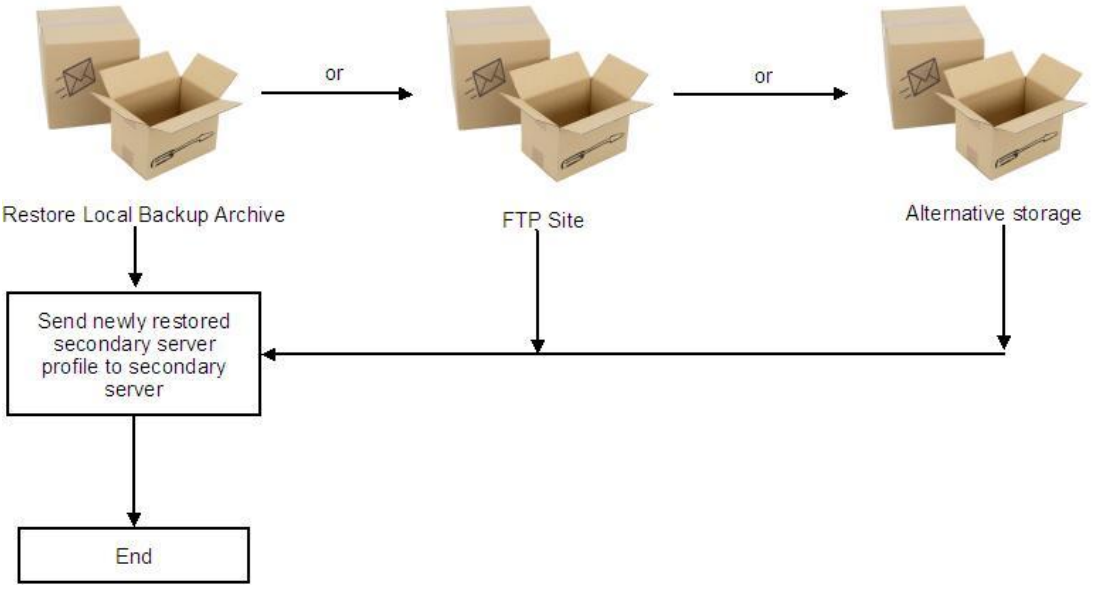
.



Redundant SCS server configuration is now complete.

The master server and secondary server are now restored and operational.

Scenario 3: Rolling System Configuration Back with a Backup Archive



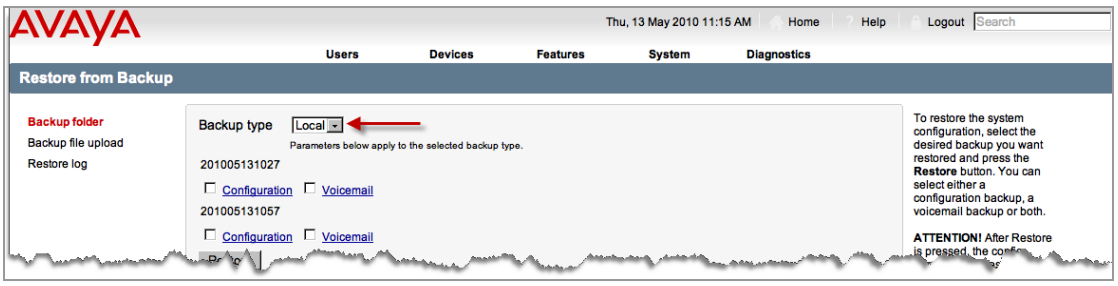
Sometimes it might be the case that you need to perform a 'roll back' to take the system back to a previous configuration. This is an easy enough procedure to perform using the Restore utility – particularly if your have an up-to-date locally stored archive, although the same result can be achieved using backup archives stored on an FTP server or a file upload from an alternative location. However, you must **remember** to send the secondary server profile in order to bring the secondary/distributed server back in line with the master.

Restoring Backup Archives

Restoring from the Local Archive or FTP

1. By default, when you open the restore window you have the option of restoring from the local archive store on the SCS or your chosen FTP server. Use the drop-down menu to select **Local** or **FTP**.

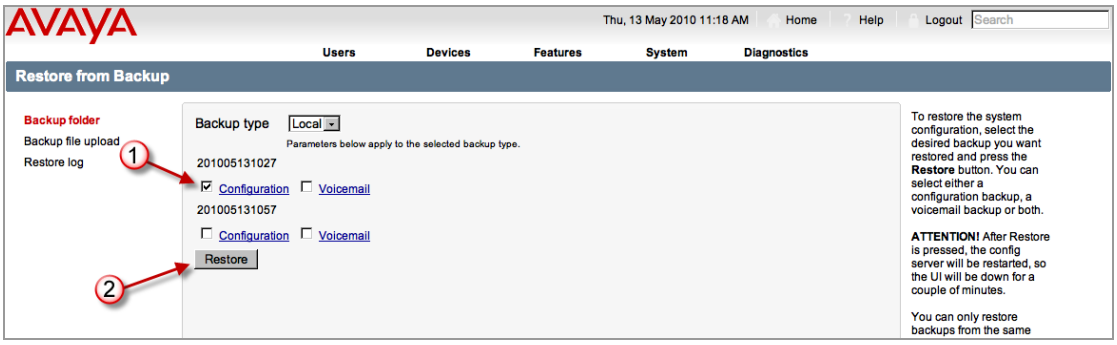
   To restore from another source, click on the **Backup file upload** menu option on the left-hand side and follow the instructions found in the following section, 'Restore by File Upload'.



2. The screen is populated by a list of configuration dates and associated archives.

   If you selected FTP in step 1 you may have to configure FTP settings in order for your files to appear. In this instance, click on **Show FTP Settings** to configure server name, username and password values, and then click **Apply**.

3. Select the archive you would like to restore by ticking the corresponding check-box.



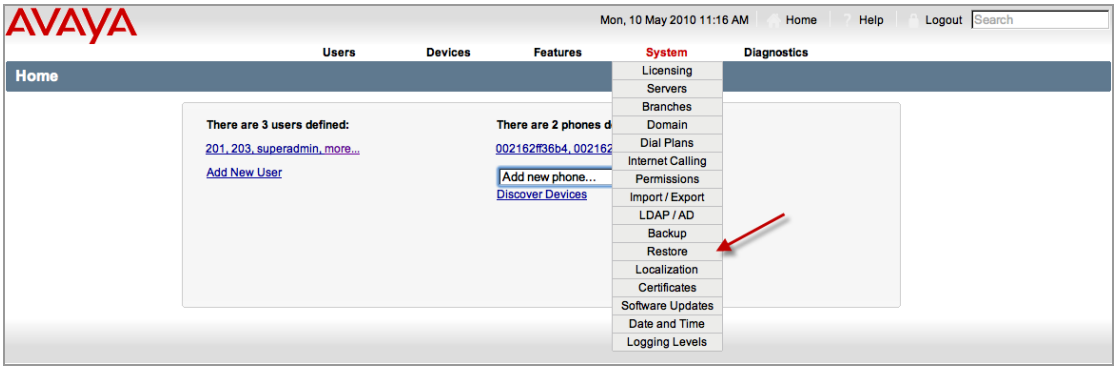
4. Click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

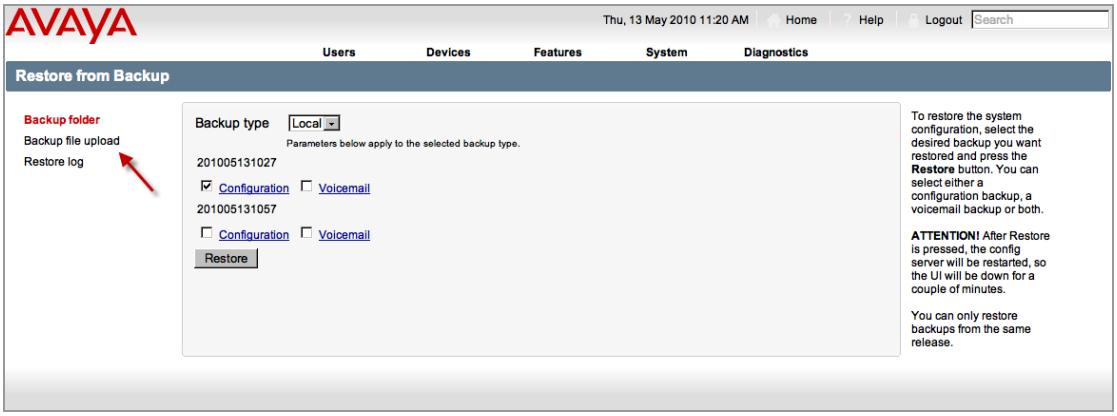
Restoring by File Upload from a Secondary Location

In the absence of an FTP server, it is still possible to save backup archives to a secondary location for safe keeping. To restore archives from this secondary location follow these steps:

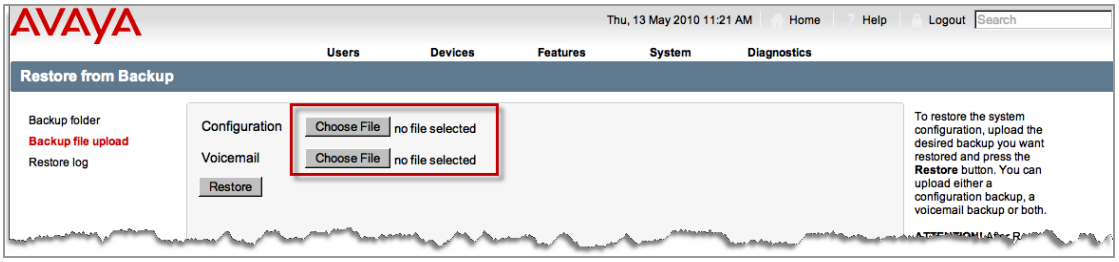
1. Open the **System** menu and select **Restore**.



2. Click on **Backup file upload**.



3. To restore a Configuration file, click on the corresponding **Choose file / Browse** button, to restore a Voicemail file, click on the corresponding **Choose file / Browse** button.



Note: the interface will display an error message if you attempt to enter a voicemail file in the **Configuration** text box and vice versa.

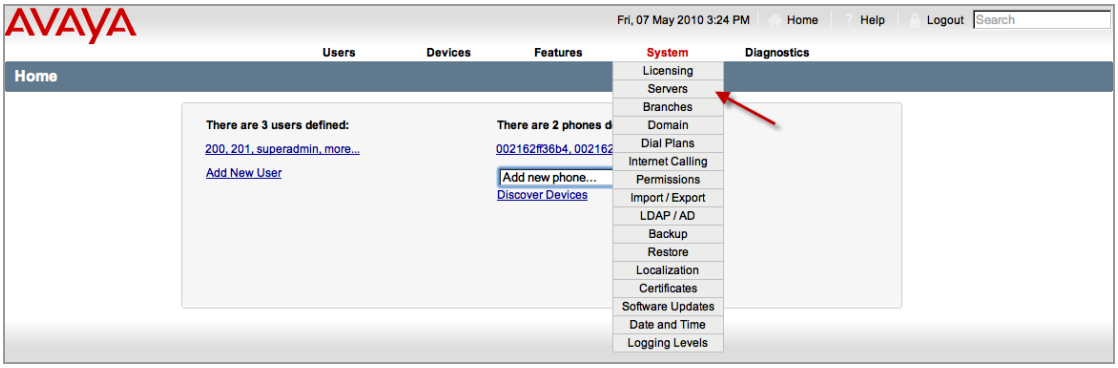
4. When you are ready to continue, click the **Restore** button.

5. The server will reboot during file restoration. During this time, the web interface will be unavailable.

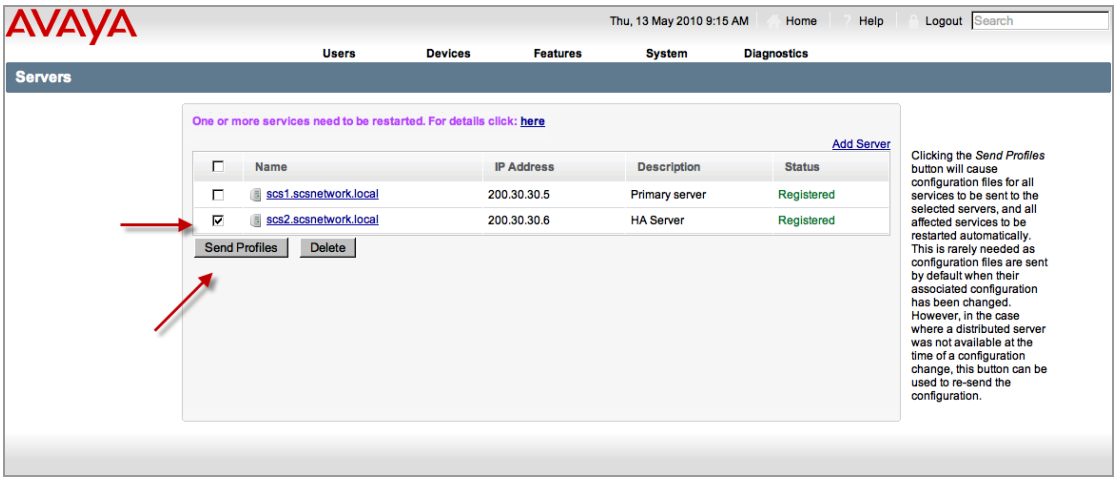
Sending the Secondary Server Profile

Because the Backup archive you just restored contains a different configuration to the secondary server you need to 'update' the secondary server with the secondary server profile that now exists in the master server's Servers page as a consequence of the Restore process. This will bring the two servers into alignment once again.

1. Navigate to the servers page by opening the **System** menu and clicking on **Servers**.

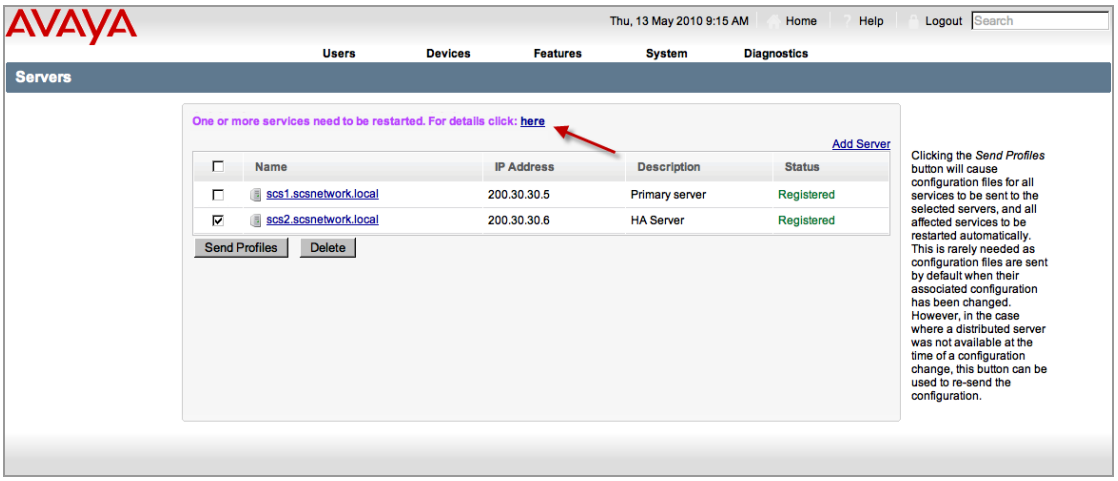


2. The server list is displayed, select the secondary server by ticking its check-box and then click **Send Profiles**.



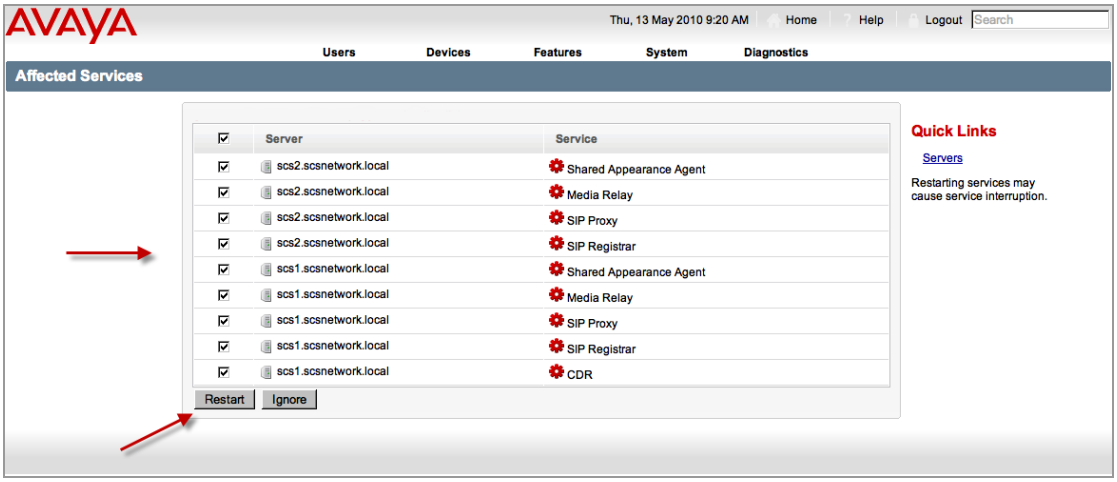
Restart all required services:

1. Click on the **here** link at the top of the screen.



2. Select all available check-boxes and then click the **Restart** button

.



Redundant SCS server configuration is now complete.

The master server and secondary server are now restored and operational.

Scenario 4: Rebuild the Secondary Server



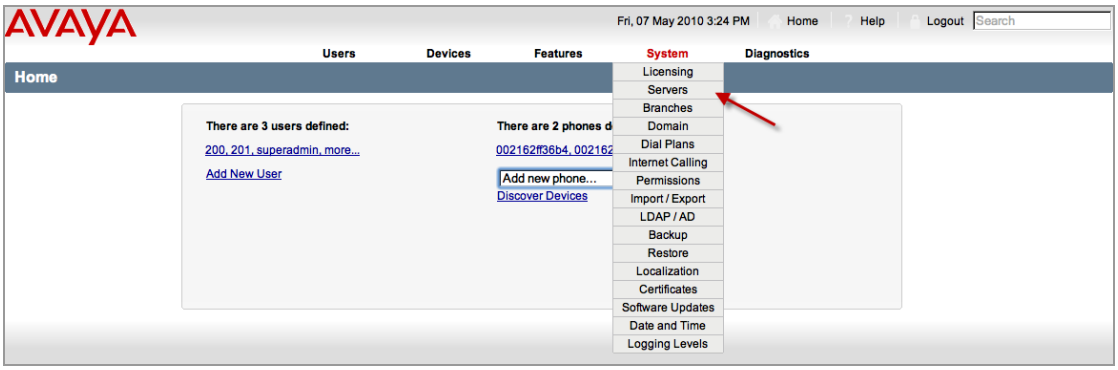
In the event that the secondary server fails all functions will continue to operate, you will however lose fault tolerance capability. It is therefore recommended that you recover the secondary server as quickly as possible. This can be done in the following way:

- Create an install disk/USB thumb drive by downloading the SCS software from the Nortel website.
- Configure the secondary server's boot sequence to ensure that it is capable of booting from the install source.
- Install the SCS software and configure the secondary server.
- Send the secondary server profile from the master to the secondary server.

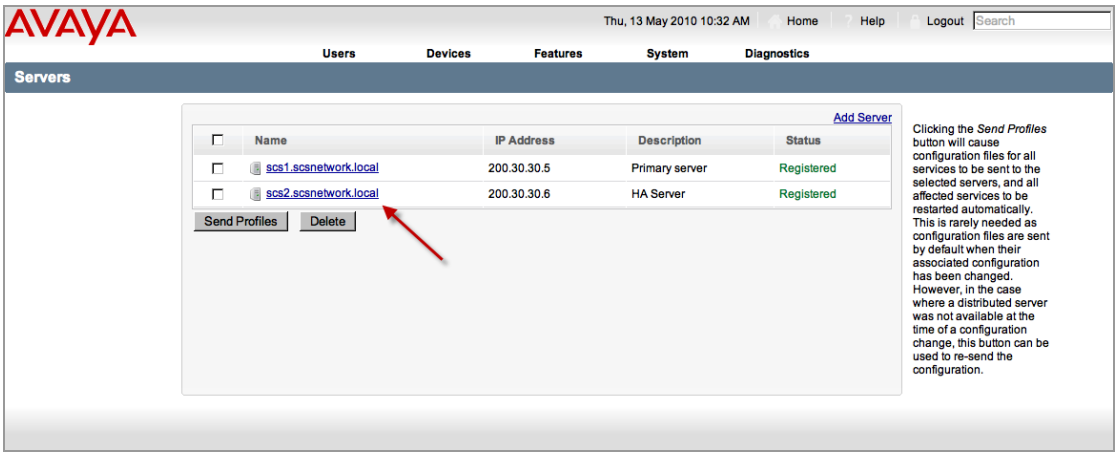
Gathering Secondary Server Profile Information

Before continuing, ensure that you have noted down the hostname, IP address and password found in the secondary server profile, accessed by navigating to the **Servers** page in the master server administrative interface.

1. Open the **System** menu and click on **Servers**.

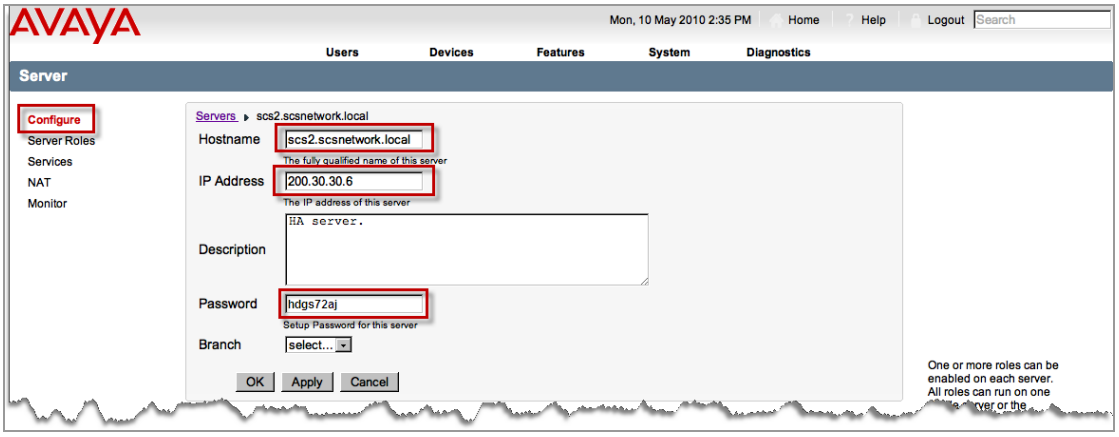


2. Click on the secondary server link.



3. Displayed on the screen you will see the IP address, hostname, and password details of the secondary server. Note these details down or

print the screen; you will need this information when you come to run the secondary server installation wizard. If you can't see the profile information, click on the **Configure** menu on the left-hand side of the screen.



Creating an SCS Installation Build

Before you can configure your SCS server you will need to download and install the SCS software. You will need:

- Internet access
- Writable DVD/USB thumb drive
- DVD burning software capable of creating a bootable DVD from the ISO image – for example *Infra Recorder*.

Downloading the SCS ISO File

The SCS software is contained in an ISO file, which can be obtained from the Avaya website at http://support.avaya.com. Once downloaded, the ISO file should be burnt to a DVD using a DVD burning package that is capable of creating bootable discs, or written to a bootable USB thumb drive.

Burning the ISO File to DVD

Once you have downloaded the ISO file to a suitable location, you must burn it to a DVD. The DVD will then be used to format the server and install the SCS software. For this reason, it is not enough to simply copy the file to a DVD. The file must be burnt to the DVD and the DVD must be made **bootable** using a disc burning application – such as *Infra Recorder*.

Note: Alternatively, you can copy the SCS installation file to a USB drive and boot from that. See 'Creating a Bootable USB Image'.

In order to install the SCS software you might need to configure the boot settings so that the server reads the CD drive at power up. This is achieved in the following way:

Note: If your server already boots from the CD drive, simply place the installation DVD in the CD tray, close it and reboot the system and proceed to the next section, 'Configuring LAN and SIP Settings'.

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **Onboard or USB CD-ROM Drive**.

6. Use **U** to move it to the top of the list (if the CD-ROM drive is already at the top of the list ignore this step).

7. Press the **Enter** key.

8. Open the CD-ROM tray and insert the SCS installation DVD.

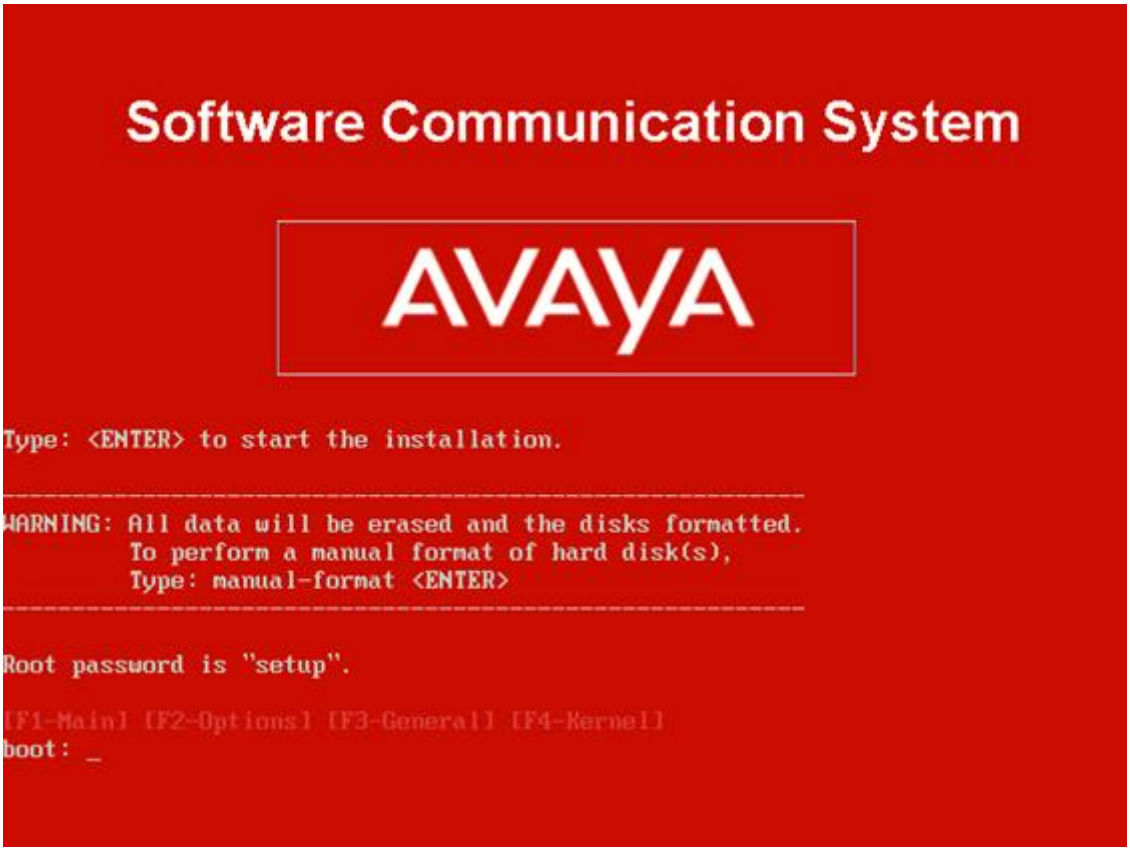
9. Close the tray.

10. Press the **ESC** key to exit System Configuration.

11. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.

12. Press the **Enter** key.

The server will reboot from the DVD and automatically launch the format utility. When the Software Communication System screen is displayed, press the **Enter** key to confirm that you would like to format the hard drive and install the SCS software.



The format and installation process takes approximately 10 minutes, when it is complete the CD tray will eject and the system will reboot to the login screen, from where you can begin the installation process. Continue to 'Configuring the SCS Master Server' for guidance on configuring the server.

Creating a Bootable USB Image

Instead of creating a bootable installation DVD you could instead create a bootable USB image. This will involve:

- Writing the SCS ISO image to a 'bootable' USB thumb drive using an application called *ISO2USB*, which can be obtained at http://iso2usb.sourceforge.net
- Re-ordering the boot sequence of the Dell server.

Note: The USB thumb drive must have a capacity of 1GB or more.

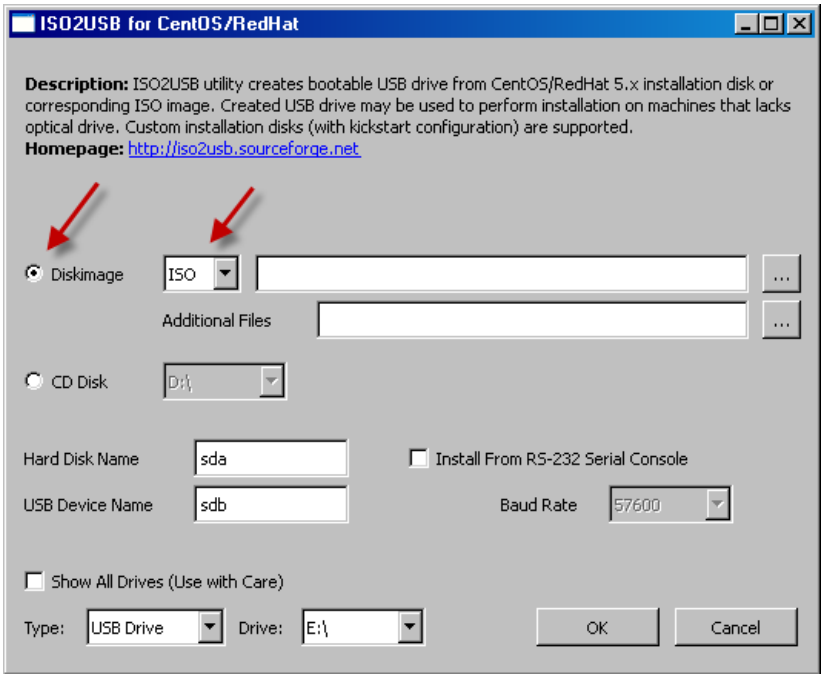
To create a bootable USB drive:

1. Insert a USB thumb drive (ensure that you this is a drive that has no important data on it).

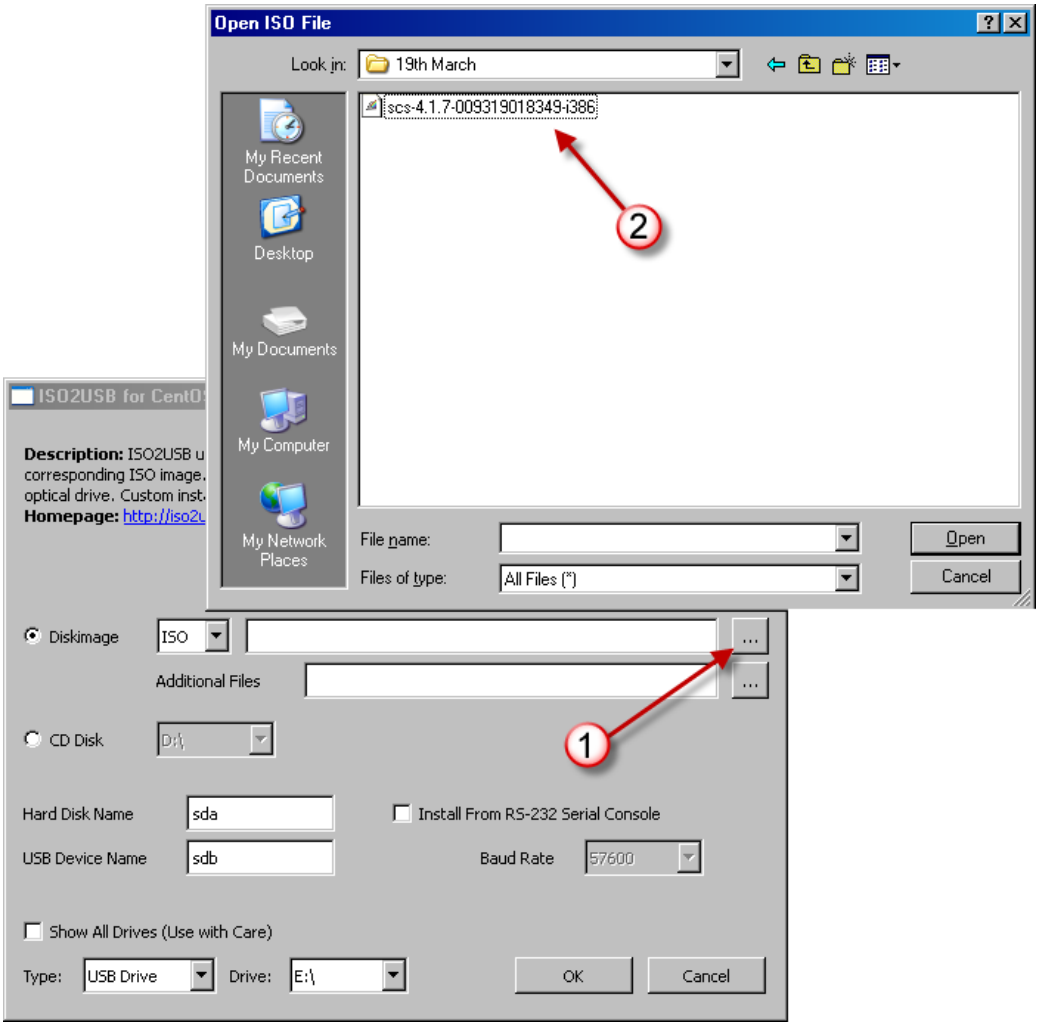
2. Download *ISO2USB*.

3. The package downloads as a ZIP file. Extract the contents and then double-click on **iso2usb.exe** to launch the application.

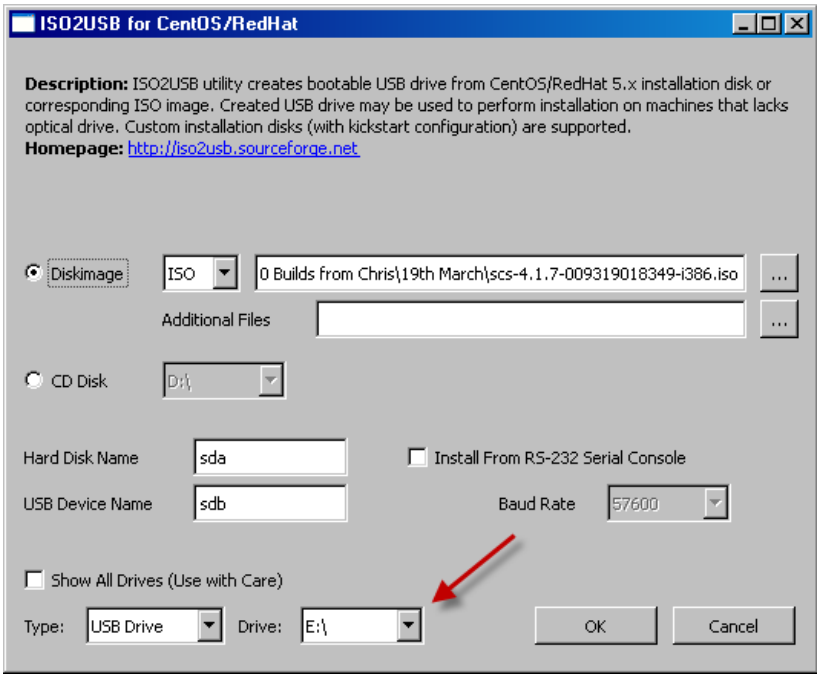
4. Ensure that the **Diskimage** radio button is selected and that **ISO** is selected in the top drop-down menu.



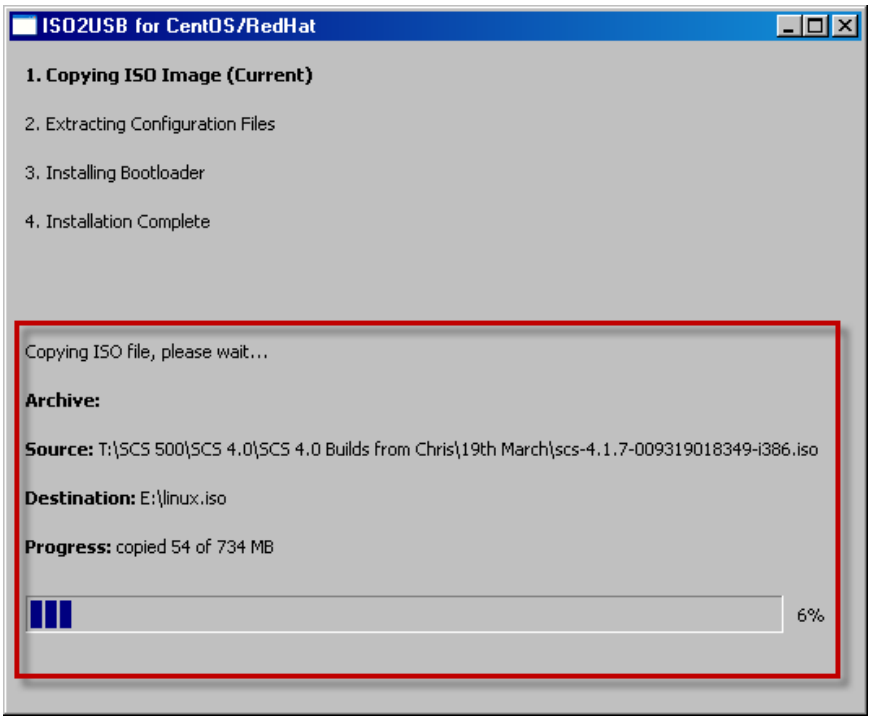
5. Navigate to the location of the SCS ISO image and select it.



6. Select the USB drive from the **Drive** drop-down menu at the bottom of the window and then click **OK**.



7. The image is written to the USB drive.



8. When copying is complete, click the **Exit** button.

You have now created a bootable SCS installation USB drive. Next re-order the boot sequence on the server.

In order to install the SCS software you will need to configure the boot settings so that the server reads the USB drive at power up. This is achieved in the following way:

1. Press the **Power** button to switch the server on.

2. As soon as the blue Dell screen is displayed, press **F2** to enter the System Configuration menu.

3. Using the **Down** cursor key, navigate to the **Boot Sequence** menu on the left-hand side of the screen.

4. Press **Enter** to move the menu highlight to the **Boot Sequence** pane.

5. Using the **Up** and **Down** arrows, move the green highlight strip so that it is resting over **USB Device**.

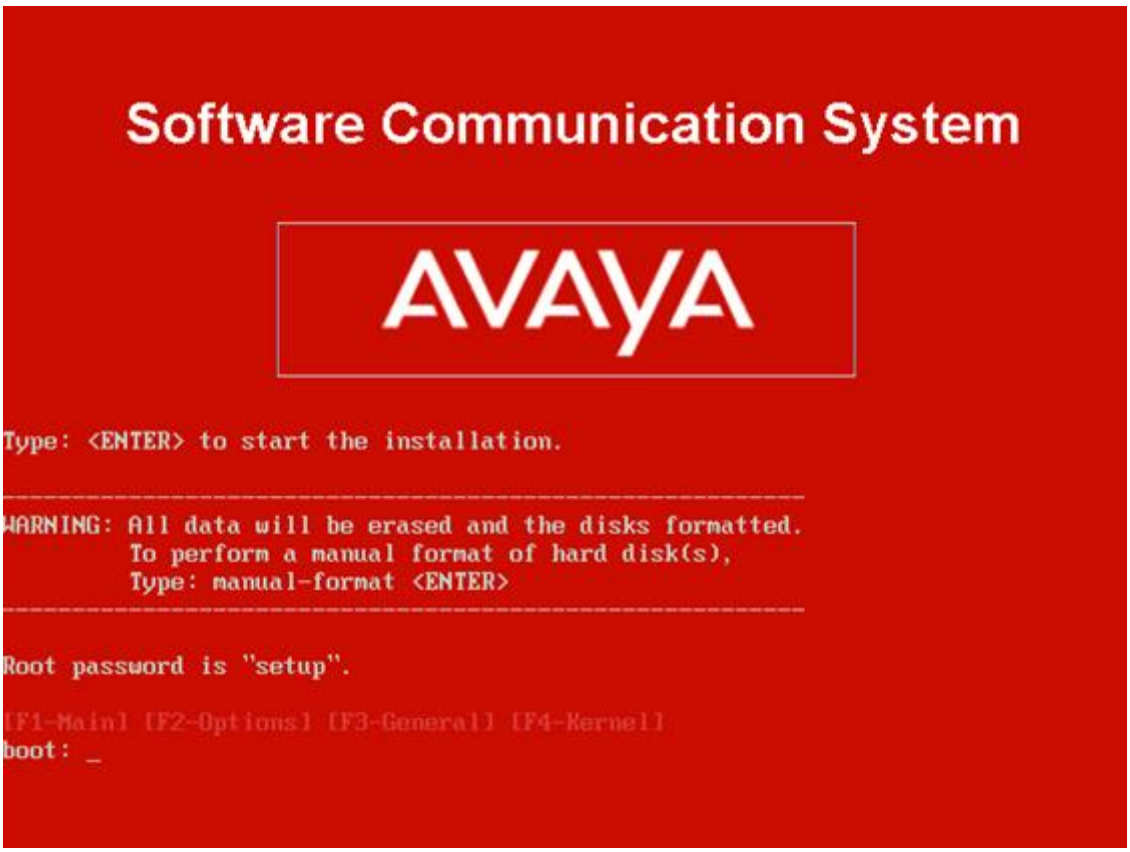
6. Use **U** to move it to the top of the list

    c. On some servers it may be necessary to ‘enable’ the USB device as a boot option. Press the **Space** bar if **USB Device** does not have a priority number next to it. A ‘**1**’ should appear next to the drive.

7. Press the **Enter** key.
8. Insert the USB thumb drive
9. Press the **ESC** key to exit System Configuration.
10. Use the **Left** and **Right** cursor keys to navigate to **Save/Exit**.
11. Press the **Enter** key.

The server will reboot from the USB drive.

When the red Avaya screen is displayed press **Enter**.



A ‘kickstart’ error will be displayed, this is normal. Simply use the **down** cursor key on your keyboard to highlight the **OK** button and press **Enter** to launch the format utility. When formatting is complete the SCS software will be copied to the server’s hard drive.

The format and installation process takes approximately 5 minutes, when it is complete the system will announce a reboot – **Ensure that the USB drive is removed from the USB port before the reboot begins otherwise the system will reboot from the thumb drive again**. If you are unable to remove the USB thumb device before the system reboots, wait for the red Avaya

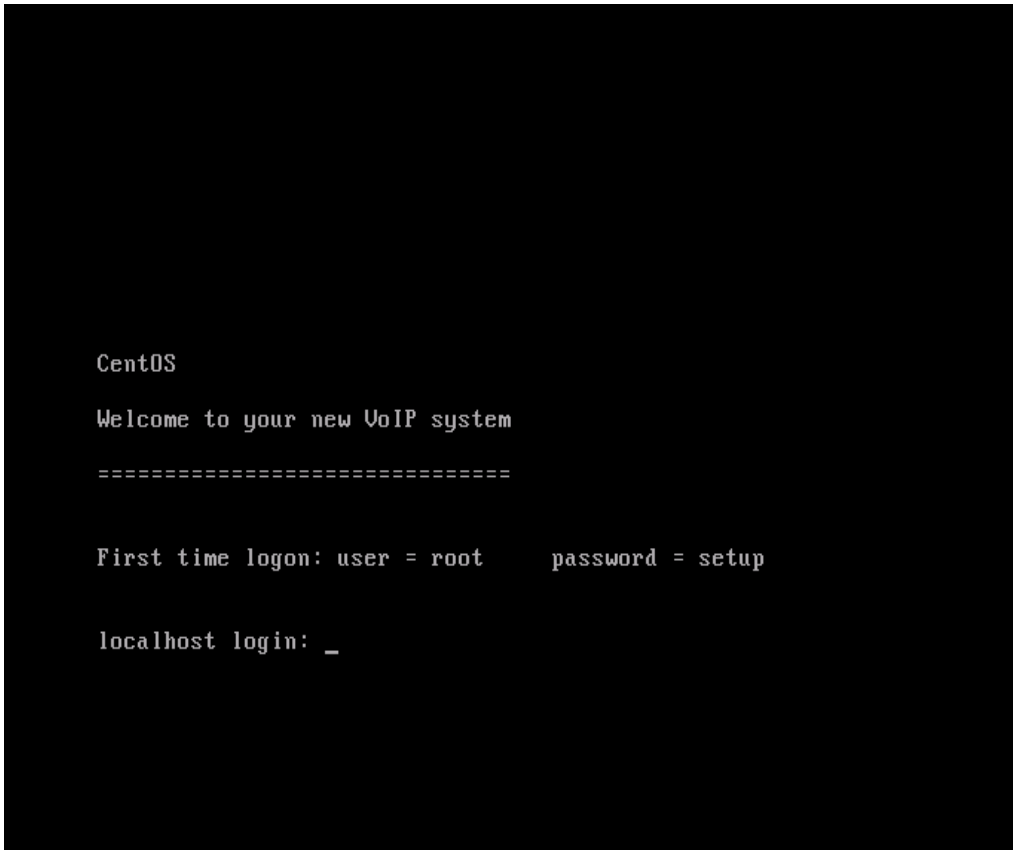
screen to appear, remove the thumb drive and then press **CTRL-ALT-DEL** to reboot the server.

Configuring the Secondary Server

When powered on for the first time, the SCS server boots to the CentOS login screen.

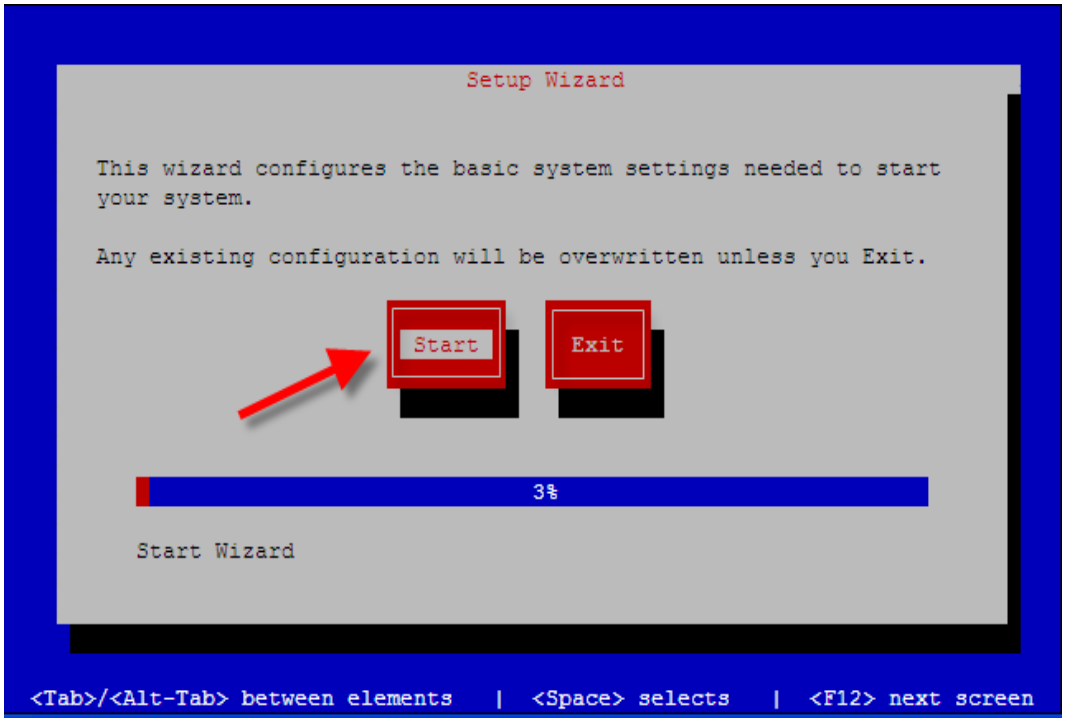
1. To begin the setup process, enter the following username and password to access the configuration utility:

   Localhost Login: `root`
   Password: `setup`

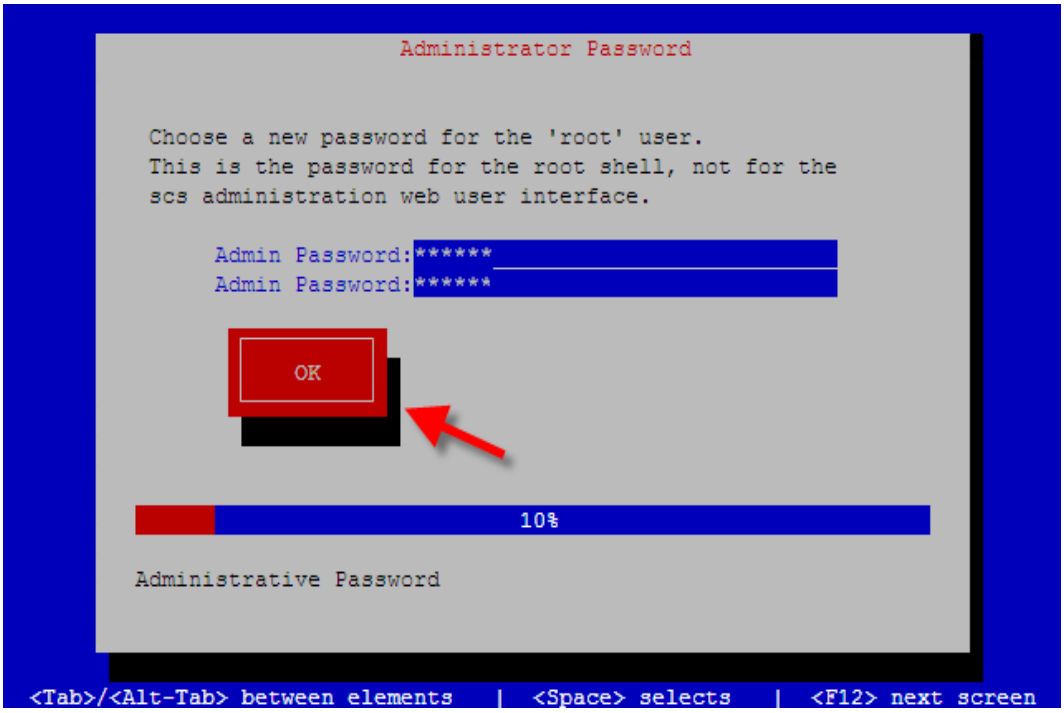
   

   If at any time during the setup process you make an error, reboot the server and log in using the same username and password. At the command prompt type **sipxecs-setup-system** and press **Enter** to reload the configuration utility from the start.

2. When the configuration utility has finished loading, highlight the **Start** button and press **Enter**.



3. Enter the **Admin Password** twice. This is the password that engineers and administrators will enter to gain access to the SCS server locally via the Linux operating system (where you are now). Highlight the **OK** button and press **Enter** when you are ready to continue.

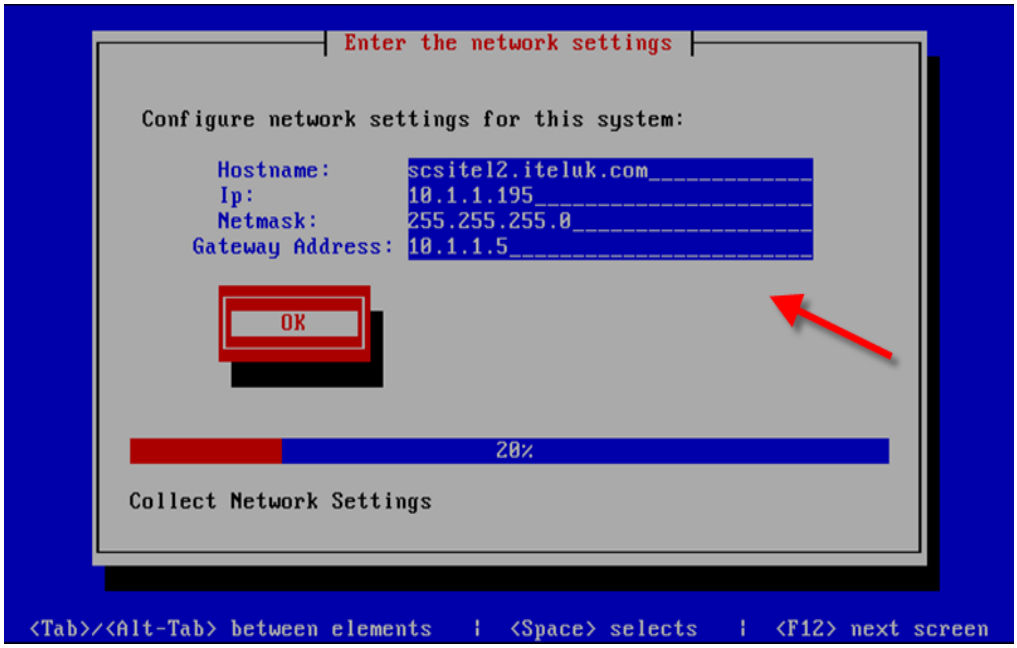


4. Enter the following LAN settings:

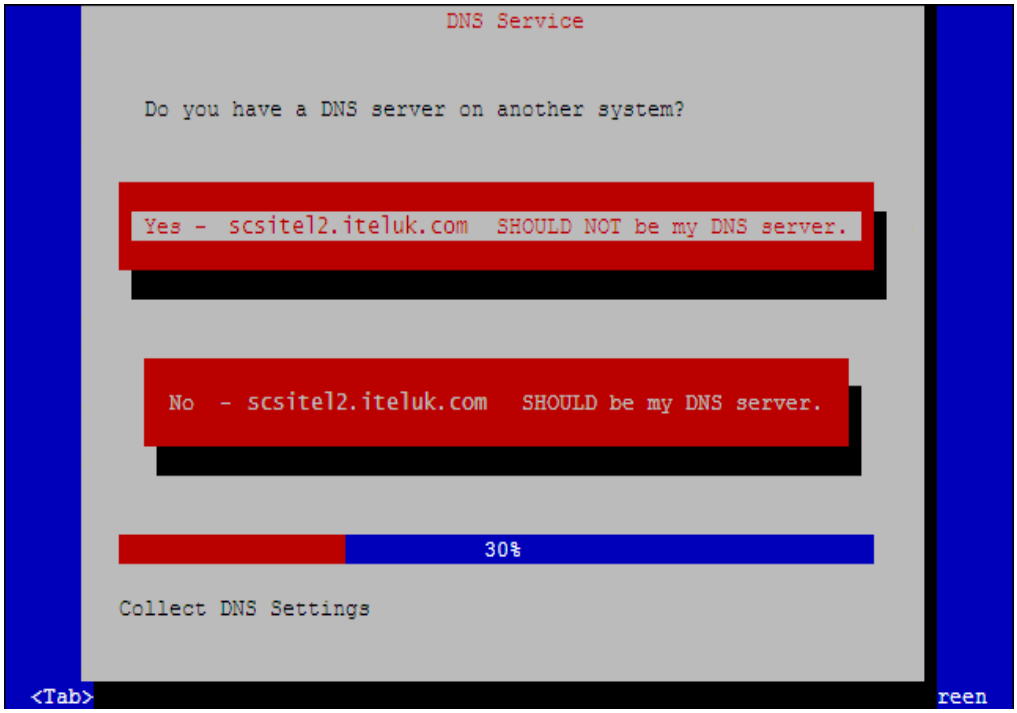
    a. **Hostname** – This is the fully qualified domain name (FQDN) of the SCS server as defined in the DNS records.

b. **IP** – The IP address that has been assigned for use with the secondary SCS. Again, this must be consistent with the address defined in the DNS settings.
c. **Netmask** – The network's subnet mask.
d. **Gateway Address** – The address of the default router providing access to the Internet.

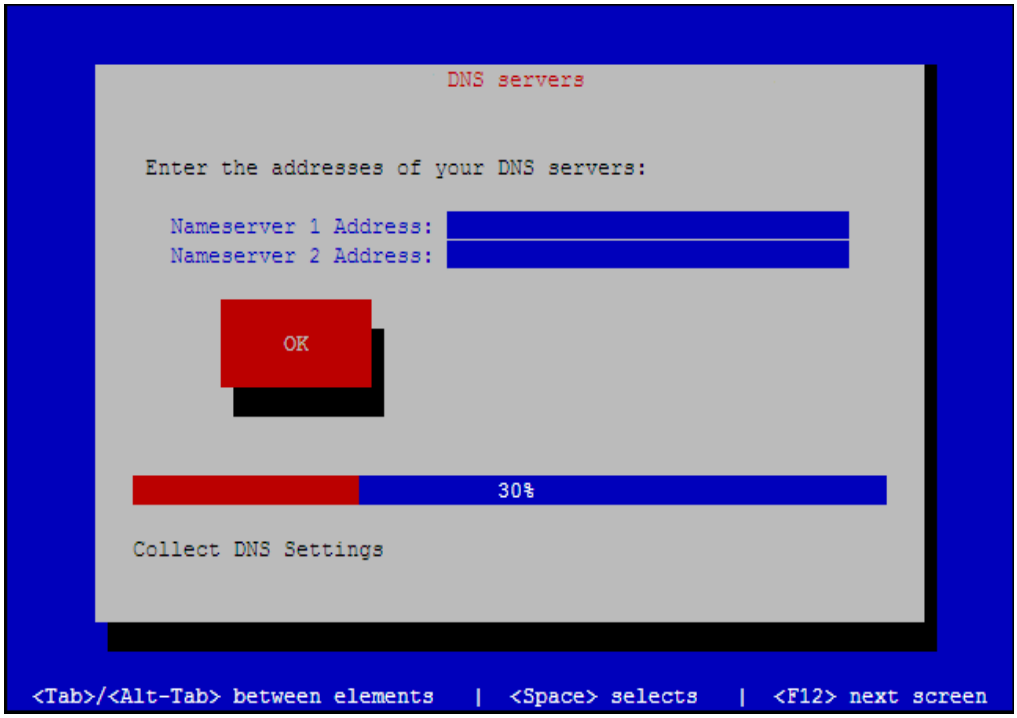
If you are unsure of any of these settings, see the network administrator.



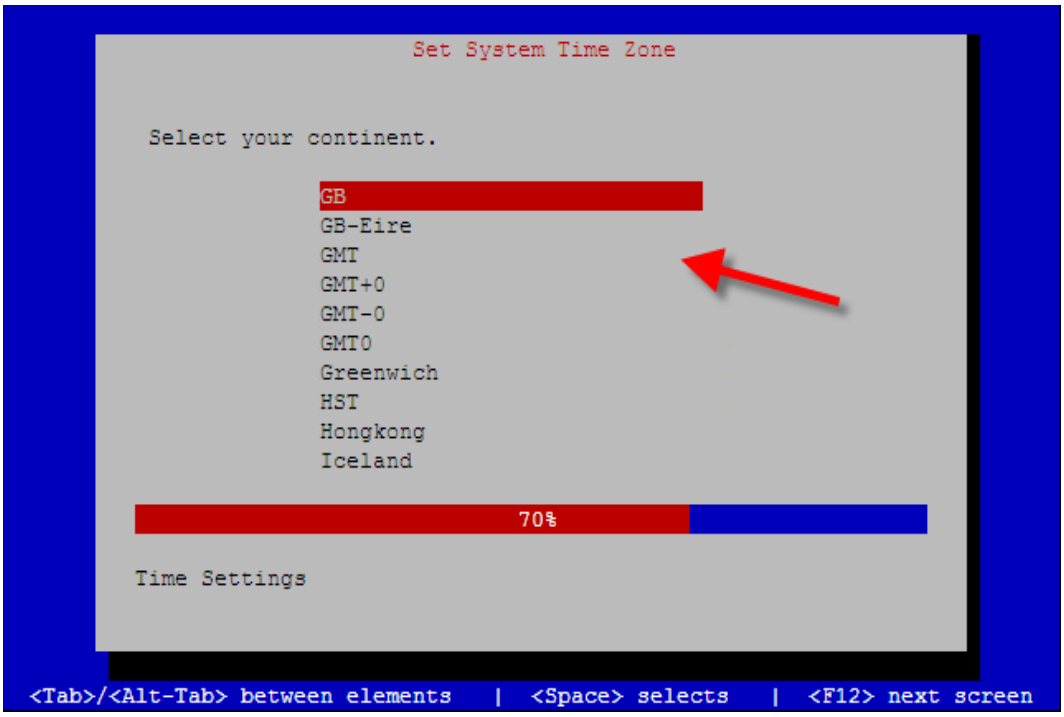
5. The installation wizard will now query whether or not you have DNS configured on the network. When installing a secondary server, this facility can remain disabled because the network will either already have a third party DNS solution or the primary SCS will be configured to provide DNS, in which case the service will automatically be replicated on the secondary server when the two systems synchronise.



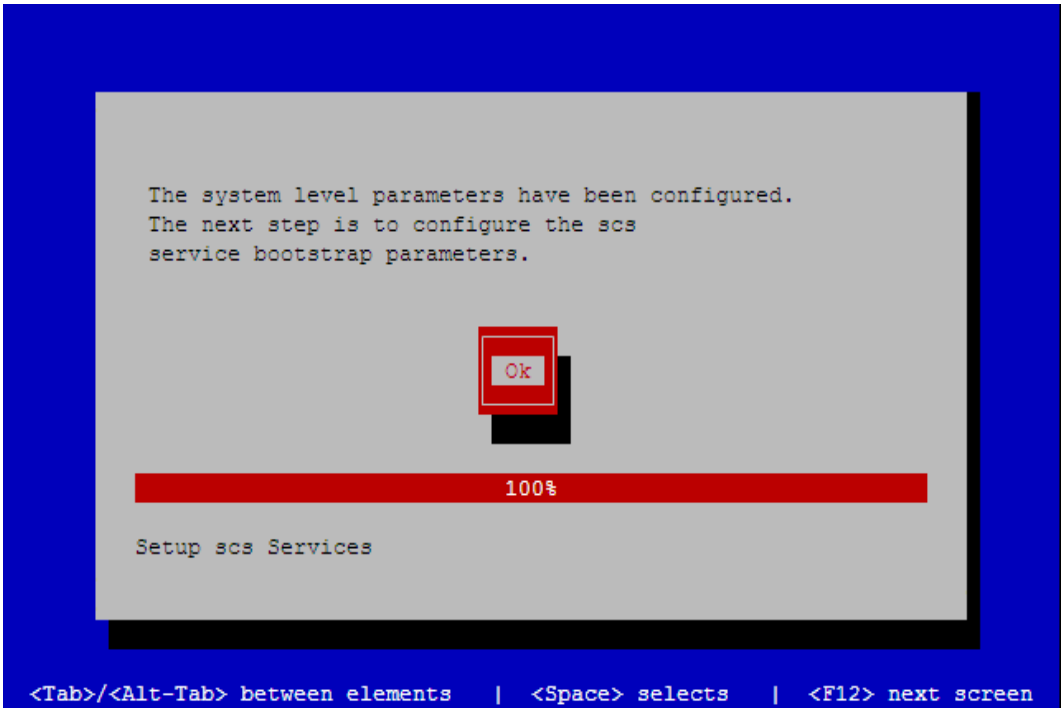
Select **Yes xxx.xxx.xxx should not be my DNS server**. Note that in this instance the next screen will ask you to configure the address of a primary and secondary DNS server. If the primary server was configured as the DNS, enter its IP address as the primary and secondary server - It doesn't matter what is entered on this screen because during synchronisation with the primary server the secondary system will gather DNS configuration information automatically.



6. Select a region or country to set the time zone in which the SCS is situated – if you pick a region, such as ‘Europe’, you will be prompted to then define an area within that region, for example, ‘London’.



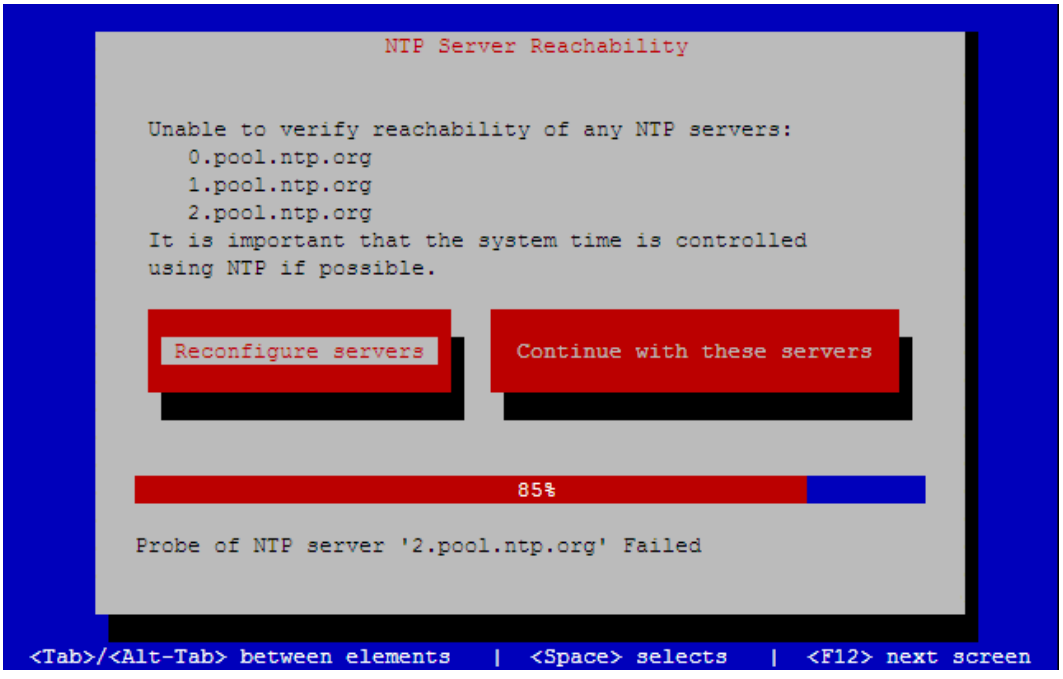
7. The system will now search for NTP servers in order to set system time. By default the SCS is programmed to attempt a connection to a series of Internet-based time servers. If it cannot connect to any of these servers you will be asked to either: 1) move on with the current time server configuration, in which case you will have to set the time manually - see Step 7b; 2) configure the address of a different time server. If the SCS successfully gathers NTP data the following message will be displayed:



Note: The NTP server search can take a while. **Do not** power off or disconnect the SCS during this process, even if it seems that nothing is happening.

Press **Enter** and continue to Step 8 if you see this message.

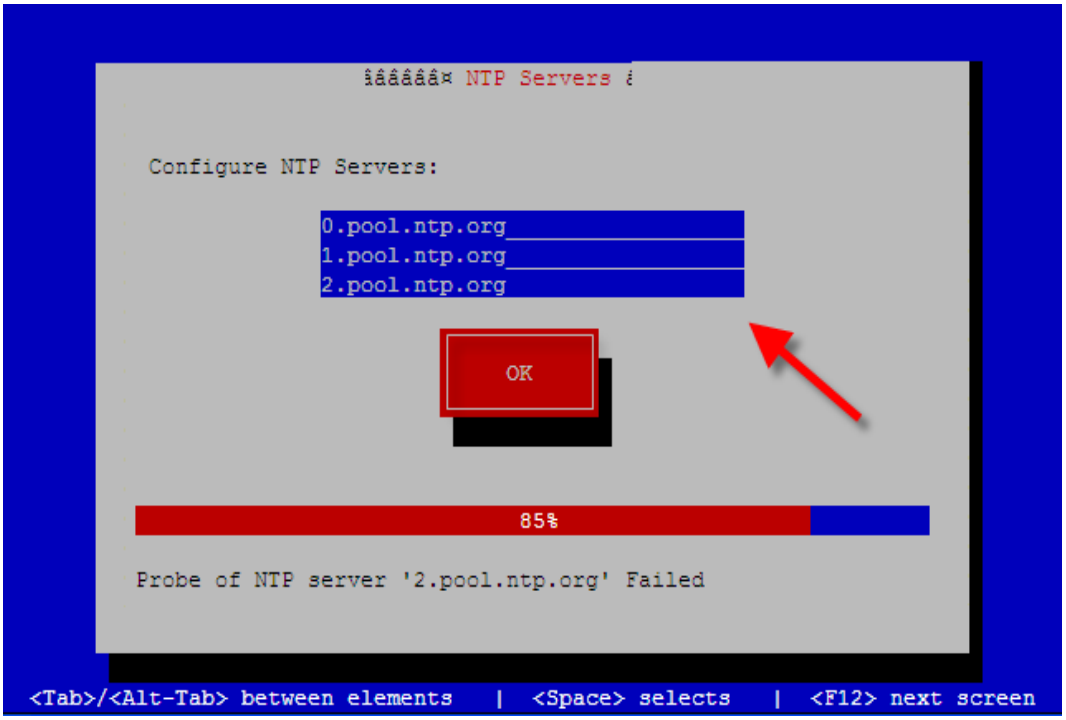
If you see the message below regarding NTP servers continue to Step 7a.



a. You now have the choice of configuring a different set of NTP servers or continuing with the default settings and configuring the time manually on the next screen.

   i. To set new NTP servers, highlight **Reconfigure servers** and press the **Enter** key.

   ii. Enter the new NTP addresses and then highlight the **OK** button and press **Enter**.



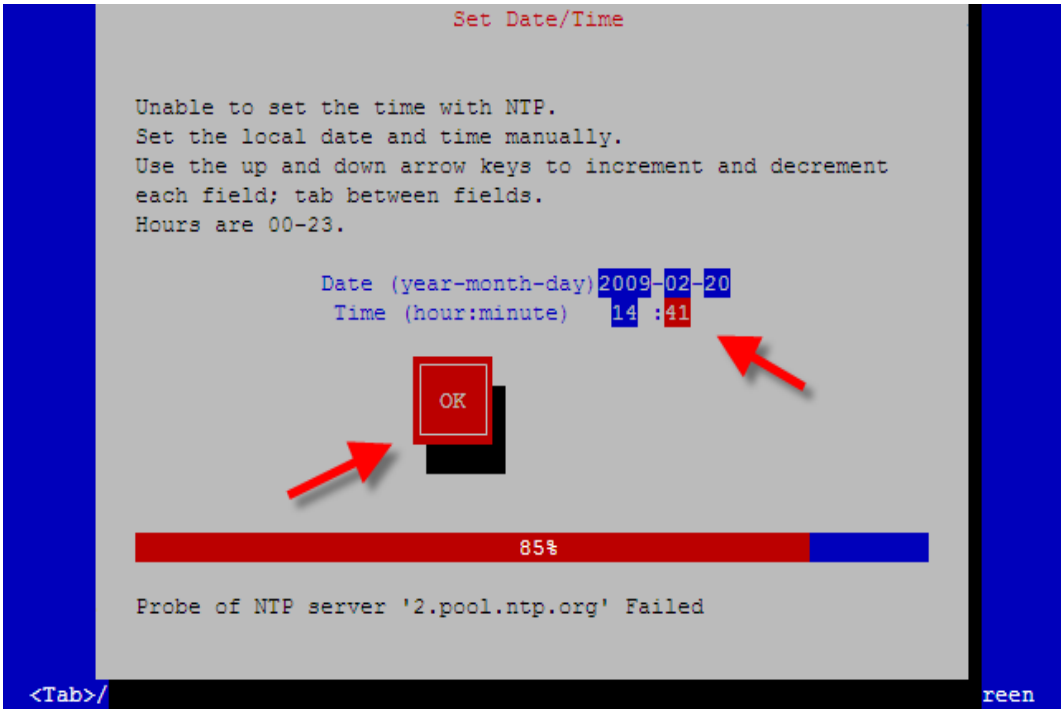
   iii. The SCS will attempt to connect to the defined NTP servers.

   iv. When a connection is successful press **Enter** to clear the confirmation screen and then continue to Step 8.

b. Instead of configuring alternative NTP servers you can set the time manually.

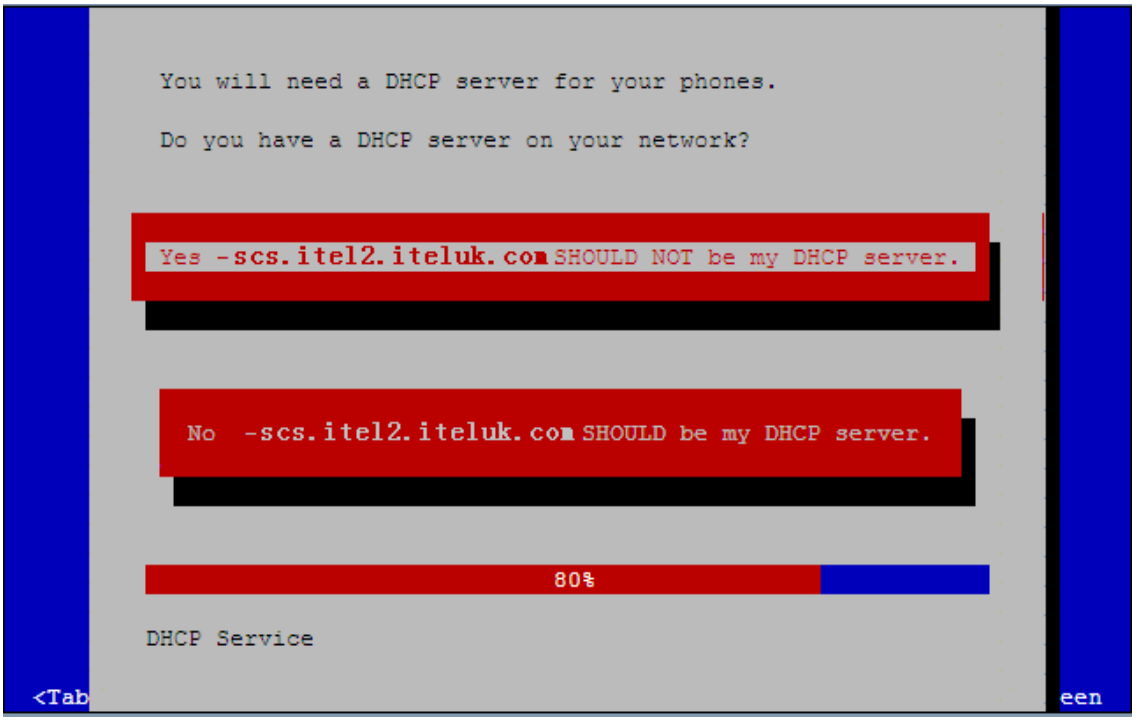
   i. Highlight **Continue with these servers** and press **Enter**.

   ii. To set the time, use the **left** and **right** cursor keys to move between the fields and the **up** and **down** cursor keys to adjust each value. The time should be set in 24-hour format. Highlight the **OK** button and press **Enter** to continue.



iii. Continue to Step 8.

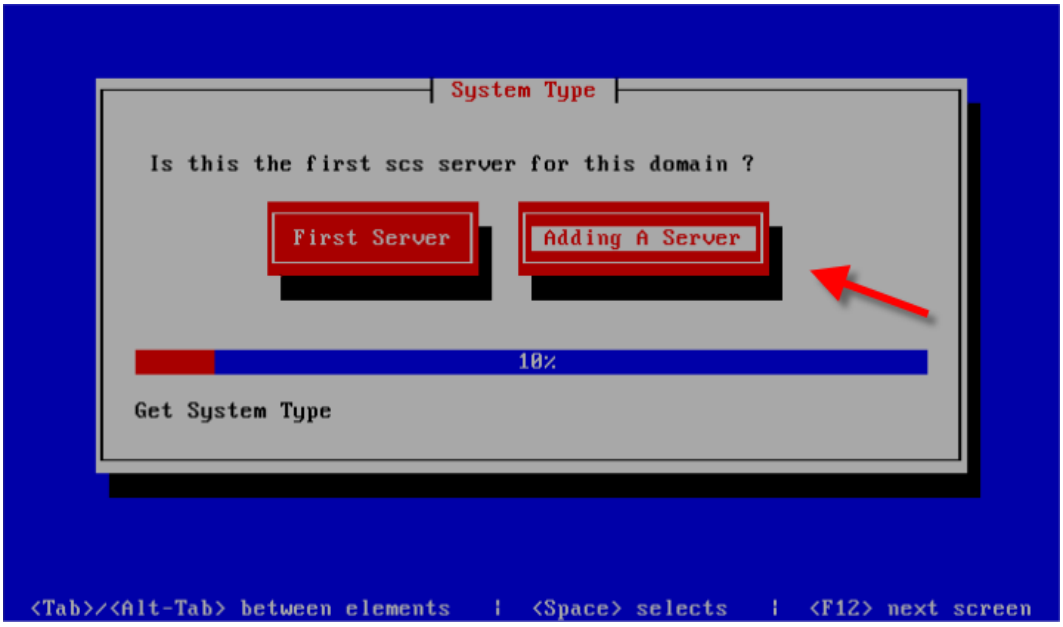
8. The SCS can provide a DHCP service in order to provide devices joining the network with IP addresses. If the network already has a DHCP server, either in the form of a third party DHCP server or the primary SCS's own DHCP service, you should not enable this service. You should therefore select **Yes xxx.xxx.xxx should not be my DHCP server**.



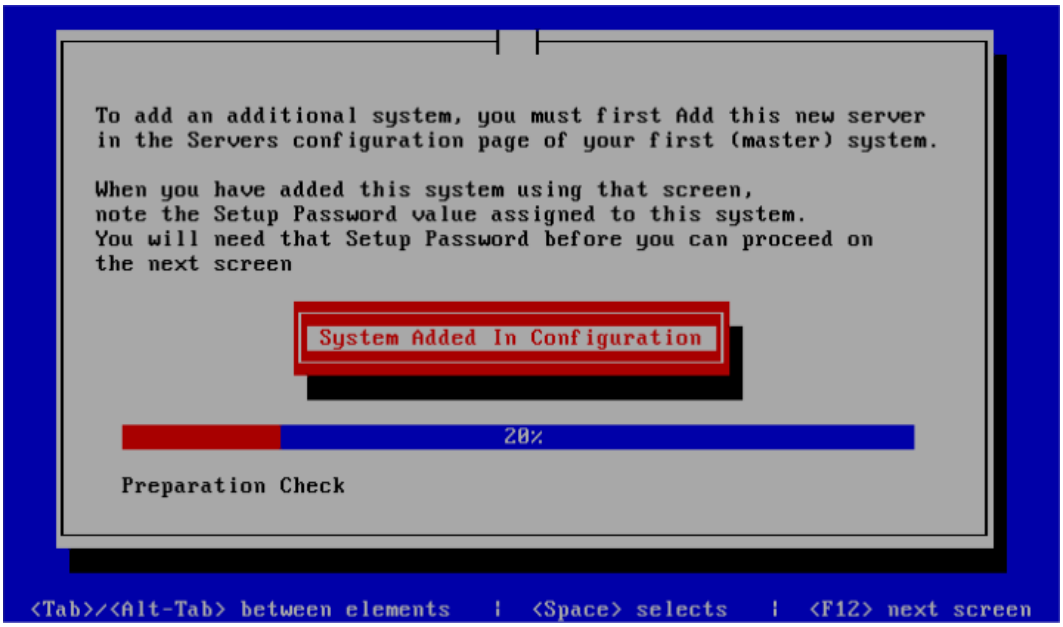
Note: If a DHCP service is already active on the network **do not** enable the

onboard DHCP service since this will cause a conflict.

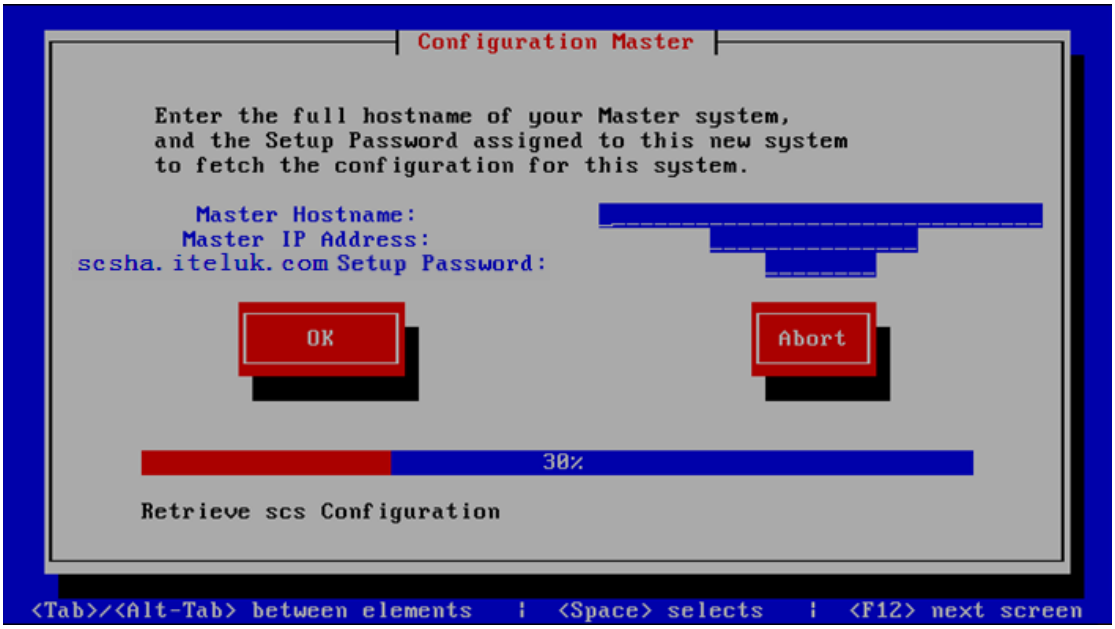
9. You now need to configure some settings that will define this server as your secondary SIP server. First, define the server as an 'added server'. Highlight **Adding a Server** and press the **Enter** key.



10. The next screen acts purely as a reminder, pointing out that before you configure the next settings you must first create a profile in the primary server's GUI. If you have already created the profile press the **Enter** key. If you have not yet created a profile for the secondary server ensure that you do before continuing.

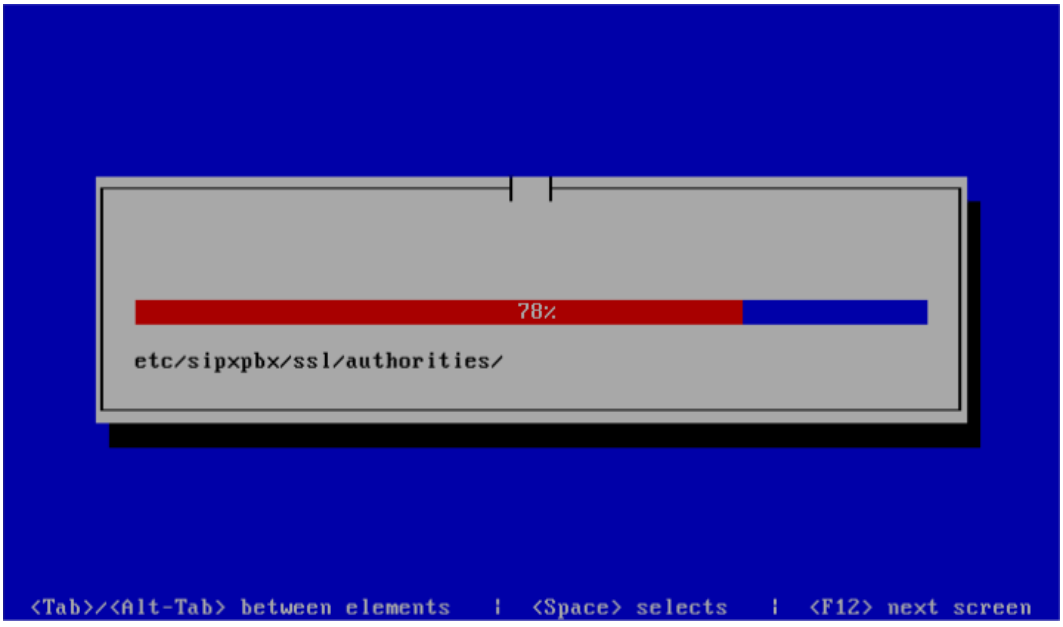


11. Enter the hostname and IP address of the **primary** server, followed by the password for the **secondary** server - created when you configured the secondary's profile earlier.



Highlight the **OK** button and press **Enter** when you are ready to continue.

12. Wait a few moments while the server downloads settings and synchronises with the master server.

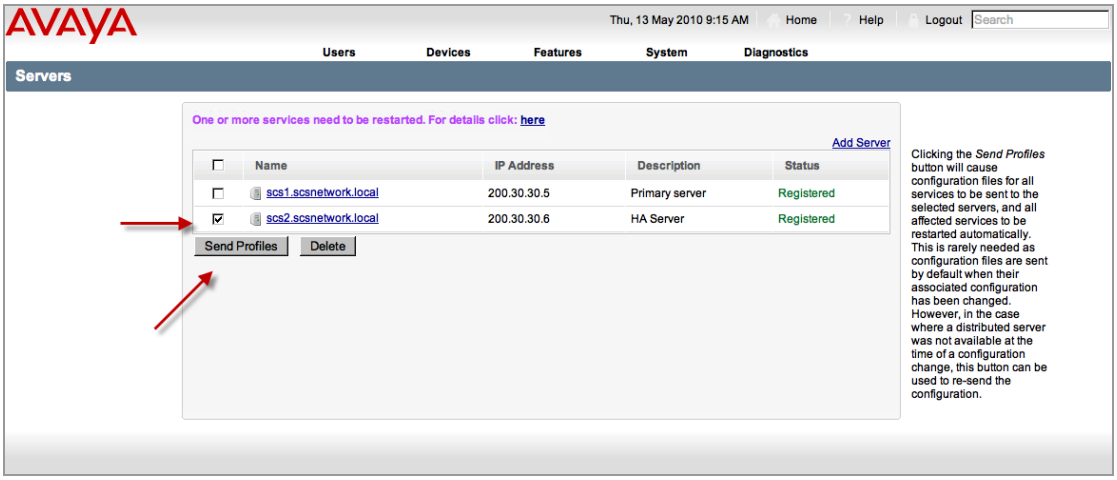


13. Finally, when configuration is complete, highlight the **Reboot** button and press the **Enter** key.

The secondary server is now connected to the network and ready for use. Give it a few moments to reboot and then return to the primary server's GUI to send the profile that you created earlier to the secondary sever.

Sending the Secondary Server Profile

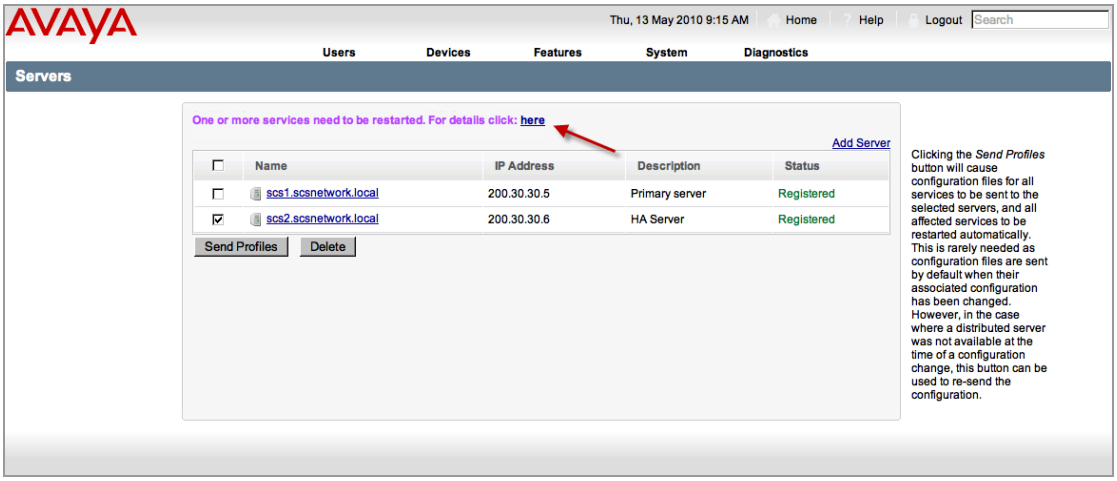
1. From within the **Servers** screen, tick the secondary server's check-box.



2. Click **Send Profiles**.

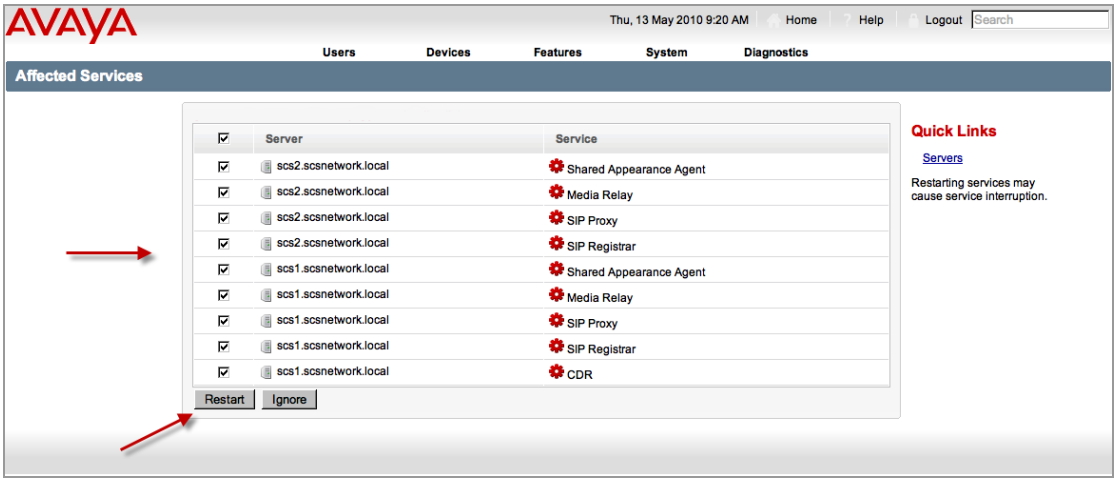
Restart all required services:

3. Click on the **here** link at the top of the screen.



4. Select all available check-boxes and then click the **Restart** button

.



Redundant SCS server configuration is now complete.

Avaya Documentation Links

- SCS 4.0 Backup and Restore Task Based Guide
- SCS 4.0 Programming Record
- SCS 4.0 Configuring the SCS Server with High Availability Task Based Guide
- SCS 4.0 Troubleshooting Task Based Guide