Advanced Simulation Technology inc.
500 A Huntmar Park Drive
Herndon, Virginia 20170 U.S.A.
Tel. (703)471-2104 • Fax. (703)471-2108
www.asti-usa.com

ASTi
Secure Telestra 3.0
Installation and User Guide

Document: DOC-01-TELS-SEC-3

Advanced Simulation Technology inc. 500 A Huntmar Drive, Herndon, Virginia, 20170 USA
Revision B.1 (June, 2008)

Product Name: Secure Telestra

ASTi ASTi Secure Telestra 3.0 Installation and User Guide

ASTi

500 A Huntmar Park Drive

Herndon, VA 20170

Table of Contents

1.0. Overview

ASTi has created a secure version of the Telestra platform to help customers meet the Information Assurance (IA) requirements for systems attached to a secure network. Driven by the Department of Defense Directive (DODD) 8500.1, trainers and equipment are now required to follow a strict sets of rules handed down from DISA, NSA and alike. ASTi ensures that our suite of products will adhere to current security requirements forced upon today's trainers. For more detailed information see the Information Assurance Support Environment (IASE) web site.

ASTi offers a certifiable secure version of Telestra software. In the secure software version the majority of the security risks identified by DISA are eliminated by ASTi, but some customer action is required to resolve vulnerabilities that may exist at the installation site.

1.1. DISA and SRR

The Defense Information Systems Agency (DISA) develops and provides security configuration guidance for IA and IA-enabled IT products. The guidelines are outlined in DISA's Security Technical Implementation Guides (STIGS), which identify existing and potential vulnerabilities on a system. STIGS exist for a variety of operating systems and applications. Additionally, there are Security Readiness Review (SRR) scripts that automate the process of validating a system configuration against the STIG requirements. Every Secure Telestra software version is tested against the latest versions of the following STIGS.

- UNIX STIG with UNIX SRR scripts
- Web Server STIG with UNIX Web SRR script

For more information on the STIGS see http://iase.disa.mil/stigs/stig/index.html

For more information on the SRR scripts see http://iase.disa.mil/stigs/SRR/index.html

Within each STIG there are four vulnerability code definitions from category I –high vulnerability to category IV –low vulnerability.

- **Category I** - Vulnerabilities that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.
- **Category II** - Vulnerabilities that provide information that have a high potential of giving access to an intruder.
- **Category III** - Vulnerabilities that provide information that potentially could lead to compromise.
- **Category IV** - Vulnerabilities that provide information that will lead to the possibility of degraded security.

ASTi's goal for the Secure Telestra is to eliminate all CAT I's and CAT II's and to minimize CAT III and IV vulnerabilities. ASTi has also incorporated the UNIX SRR scripts into the production testing process so that the Secure Telestra is constantly updated with the most valid security enhancements.[1]

[1] As the DISA STIG CAT I and II vulnerabilities change in future STIG releases it is impossible to predict future issues. While ASTi will make every reasonable attempt to remove all CAT I and II issues we cannot guarantee removal of all these issues. The CAT I and II issues are constantly changing over time. If removal of an issue is not feasible we will work with the customer to obtain a waiver as required. This will be documented in the accompanying ASTi SRR Report.

1.2. Customer Responsibilities

The vulnerabilities are given unique labels called Potential Discrepancy Items (PDIs). Each PDI is categorized with a short description of the vulnerability. Out of the hundreds of PDIs, ASTi can eliminate the majority of them; however, the customer is responsible for eliminating several PDIs.

For example, certain elements of the STIGS require that the customer:

- Set non-guessable passwords
- Review audit logs
- Maintain specific physical security requirements

As the STIGS and SRR scripts are updated, the PDI list will change. The specific PDI list is provided on a per Telestra security software release tested against the latest STIG/SRR versions.

2.0. Requirements

The following items are required for a Secure Telestra platform:

- Telestra 3.x Software Installation CD-ROM (i.e. 3.30-1)
- Options File CD-ROM
- Telestra 3.x Security Software Installation CD-ROM
- ASTi SRR Report (This is not required for installation, but it is part of the Security Package.)

2.1. Reference Documents

This document supplements the Telestra 3.0 Cold Start and Telestra 3.0 User Guide. This document does not replace these documents.

- Telestra 3.0 Cold Start (DOC-01-TELS-CS-3)
- Telestra 3.0 User Guide (DOC-01-TELS-UG-3)
- Telestra 3.0. and Model Builder Visual Quick Start Guide (DOC-02-TMBV-QSG-1)

3.0. Telestra Cold Start Procedure and Software Installation

Important: The Secure Telestra software does not currently support the upgrade feature. After the Security Software Installation is complete, do not upgrade the base Telestra software this may cause a risk of opening up security holes in the software.

In the Telestra 3.0 Cold Start document (DOC-01-TELS-CS-3) follow the '**Cold Start Procedure**' and '**Installing Linux & Telestra Software**' for installing the base Telestra software using the Telestra 3.x Software Installation CD-ROM.

These steps must be done prior to completing the following section, 4.0 Security Requirements Procedure.

3.1. Telestra Network Connection

First connect the Telestra to a network so you can access the Remote Management System (RMS) pages. RMS is the web-based interface used to manage and interact with Telestra.

1. Connect the Telestra to a network using the ***eth0*** port. ***Eth0*** will try to obtain a network IP address and subnet mask using a DHCP server. If the Telestra cannot contact a DHCP server for eth0, it will assign a meaningless IP address of 0.0.0.0 to that interface.
2. Upon boot-up, the GNU GRUB screen will display three options, Embedded, Development, and Recovery. Select Embedded for normal operation.
3. On the Telestra Welcome screen navigate to the Settings screen by pressing "**Enter**" once the settings button is highlighted.
3. If your network does not have DHCP enabled, you must manually enter a unique IP address and its accompanying subnet mask into their respective fields on the "Setup" screen.
4. Then write down the IP address. You will need this to access the Telestra's RMS pages from a workstation on the network with a local web browser.
5. After setting the IP address for eth0, navigate to a workstation on the network with a local web browser. Type the IP address in the web browser address bar as follows:

   `http://xxx.xxx.xxx.xxx/`

   where "xxx.xxx.xxx.xxx" is the IP address previously assigned to eth0 using the Telestra Configuration Utility.

3.2. Uploading the Options File

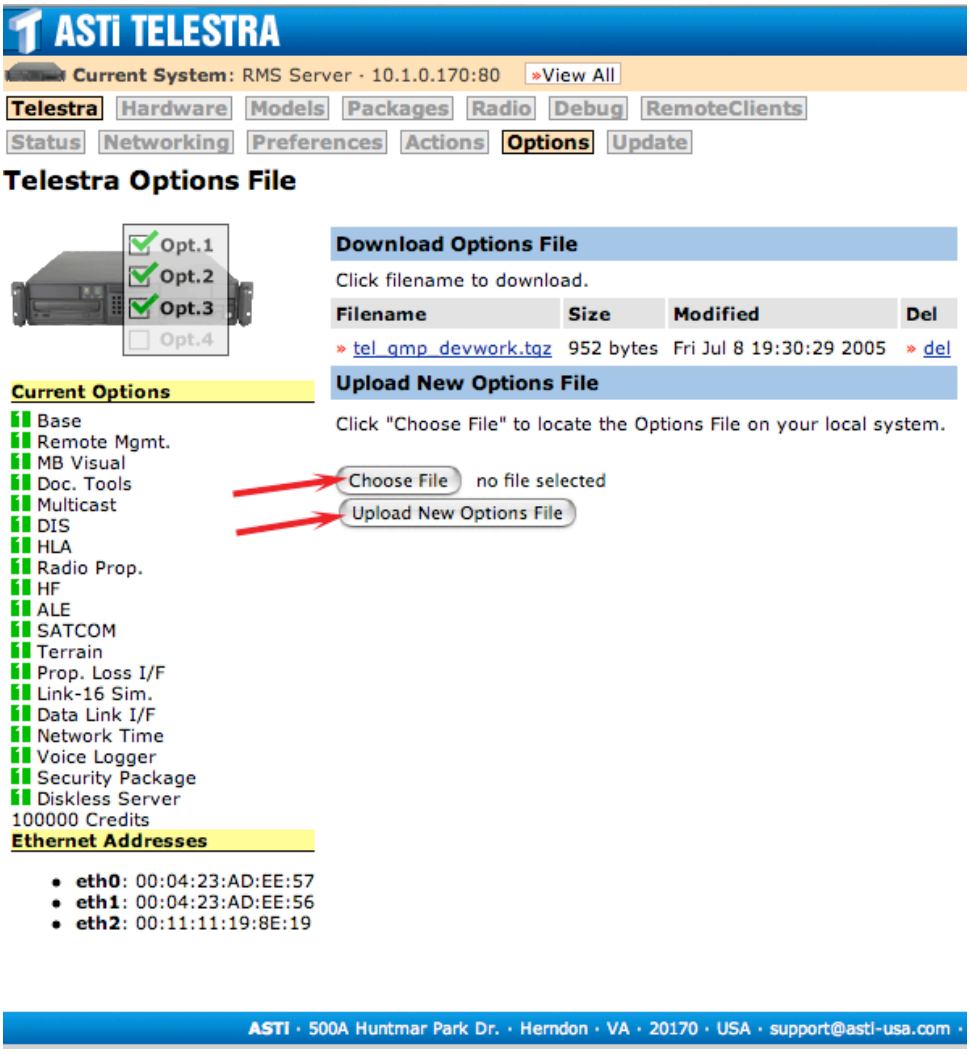
A system must have an Options File to activate full software functionality. For more details about Options Files see “System Options” in the Telestra 3.0 User Guide (DOC-01-TELS-UG-3).

To upload an Options File navigate to RMS through a local web browser on the network and select Telestra >> Options in the top menu bar. Click the “Choose File” button to locate the file on your local workstation, followed by clicking the “Upload New Options File” button.

Please note: Selecting an Options File with the same name as the currently-installed Options File will result in the new file overwriting the existing file.

Click on the filename of the existing Options File to download it to your local workstation for archiving and backup purposes.

Ensure that you upload the proper .tgz file that contains the Options File. If you upload a file that does not contain an Options File, the system will not operate properly.



4.0. Security Requirements Procedure

The following steps are required for the Secure Telestra platform.

4.1. Additional BIOS Settings for the Secure Telestra platform

The following BIOS settings are required in addition to the BIOS settings in the Telestra 3.0 Cold Start (DOC-01-TELS-CS-3). This section is a supplement to the default BIOS settings set in the '**Cold Start Procedure**.'

4.1.1. Secure BIOS Configuration version BF86510A.86A.xxxx.Pxx and NT94510J.86A.xxxx.xxxx.xxxx.xxxx

The following instructions apply only to the BIOS version BF86510A.86A.xxxx.Pxx and NT94510J.86A.xxxx.xxxx.xxxx.xxxx.

1. If you have not already done so, attach a monitor, keyboard, and power cable to the Telestra.
2. Power on the Telestra and press the F2 key as the system starts.
3. Set BIOS password to prevent unauthorized use of the Telestra. Use the arrow keys to move to the Security field.

   a. Select '**Set Supervisor Password**' and enter a password as required.

   b. Select '**Set User Password**' and enter a password as required.

   c. Set '**User Access Level**' to the required level for the Telestra's facility.

4. **For BF86510A.86A.xxxx.Pxx**:

   Change the Boot Order to prevent booting to removable media and network devices. Use the arrow keys to move to the Boot field and select '**Boot Device Priority**.'

   a. Under 1st choose Hard Drive or specific destination device.

   b. Under 2nd choose Disabled. Press ESC when finished.

   For NT94510J.86A.xxxx.xxxx.xxxx.xxxx:

   a. Set '**Boot to Optical Devices**' to Disable.

   b. Set '**Boot to Removable Devices**' to Disable.

   c. Set '**Boot to Network**' to Disable.

   d. Set '**USB Boot**' to Disable.

5. Follow the steps below to disable extra peripherals, including USB, audio, and etc. Use the arrow keys to move to the **Advanced Field** and select '**Peripheral Configuration**.'

   a. Set **Serial Port** to Disabled. (ignore this step for **NT94510J.86A.xxxx.xxxx.xxxx.xxxx**)

   b. Set **Parallel Port** to Disabled.

   c. Set **Audio** to Disabled

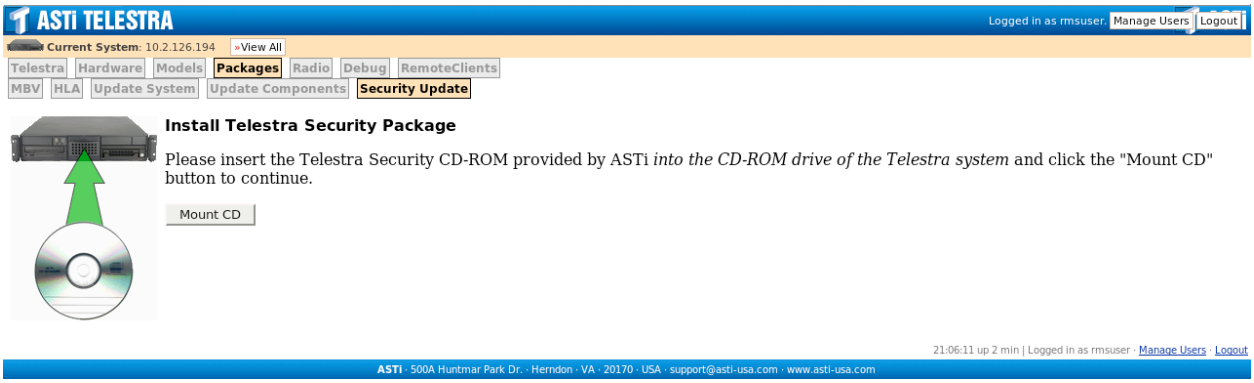
   d. Select '**Floppy Configuration**' and set **Diskette Controller** to Disabled.

   e. Use the arrow keys to move to the Exit field. Select Save Changes and choose Ok.

4.2. Telestra 3.x Security Software Installation

The custom security software package will lock-down the platform and minimize all CAT I, II, III, and IV vulnerabilities. Follow the steps below to install the Telestra 3.x Security Software package.

1. Insert the Telestra 3.x Security Software CD-ROM.
2. Open the RMS browser and select **Packages** -> **Security Update** and click "**Mount CD**."



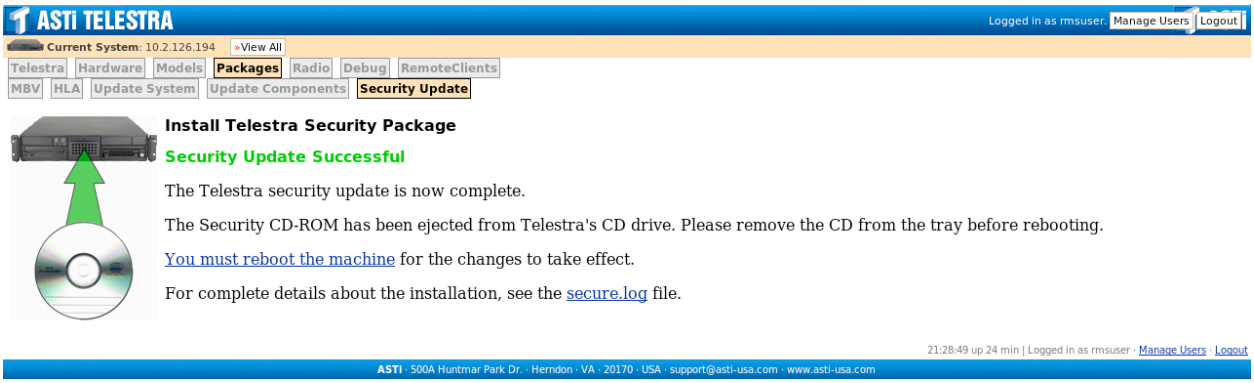
3. The RMS screen shown below will display the Telestra Security package information. To view the security software version select the **README.txt** link.

The text file will display the security software version and the corresponding SRR version provided by DISA.

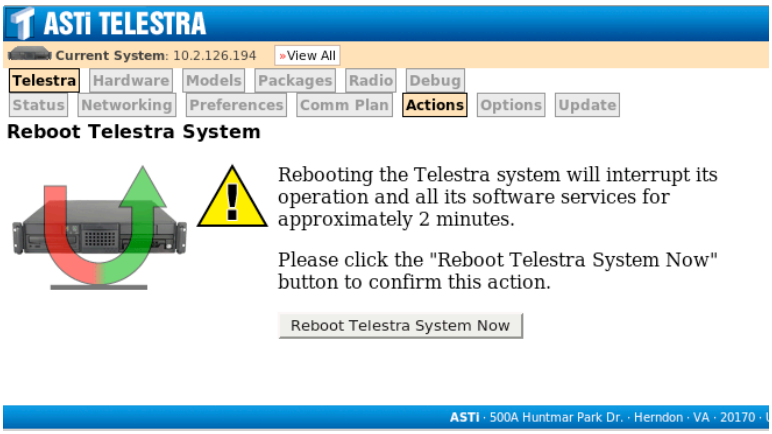
```
Release 1.0
----------------------------
 * Initial release.
 * Supports Unix SRR UNIX_51-15November06
```

4. Select the "**Install Security Update**" button to start the installation.

5. After the installation is complete, the following confirmation screen will display in the RMS browser and the CD will eject from the Telestra's CD drive. Remove the CD from the tray.

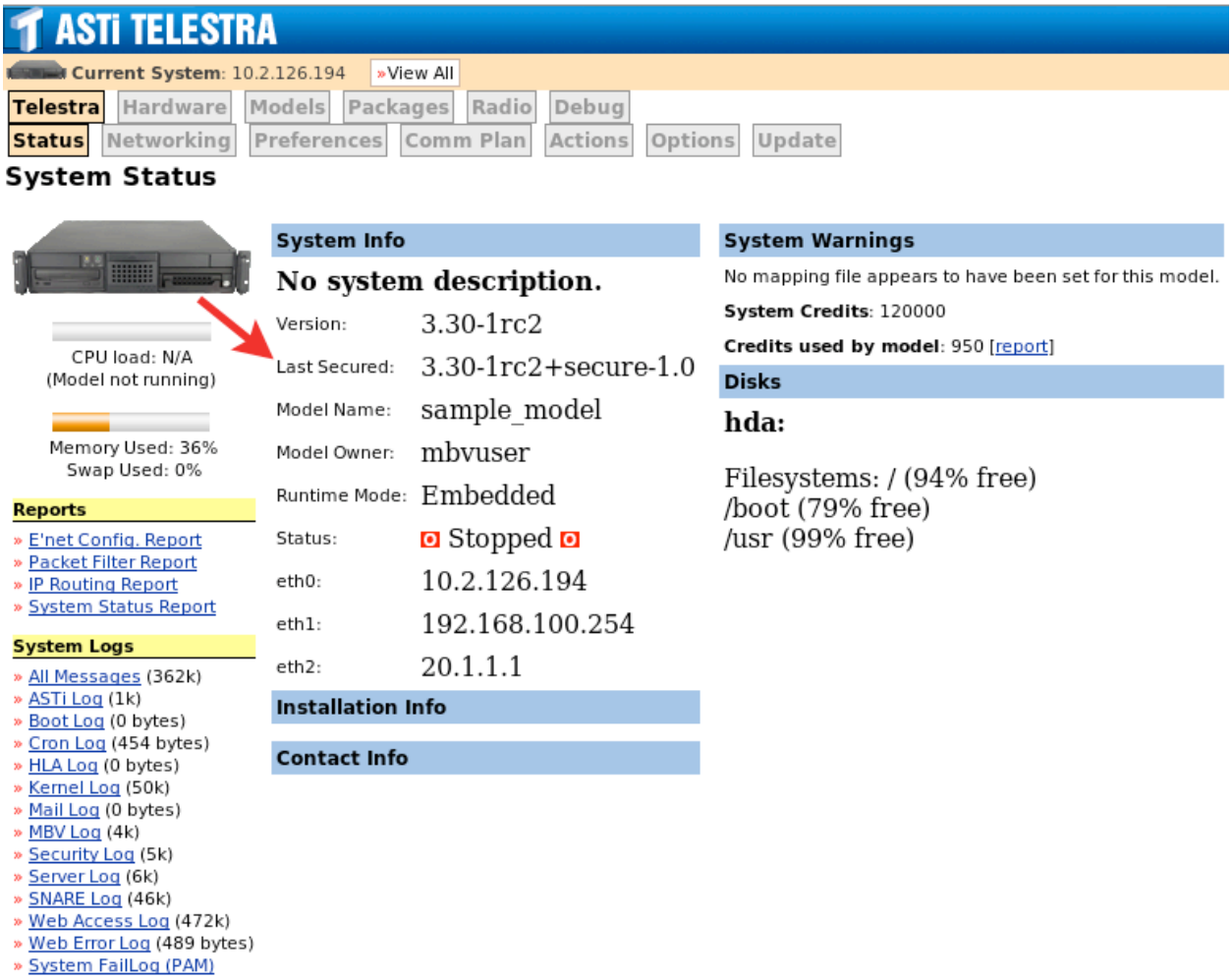


6. Select the reboot link, this will open the **Telestra** -> **Actions** page shown below.



7. Click the "**Reboot Telestra System Now**" button.

8. After the Telestra reboots, you will have a Secure Telestra platform. View the **Telestra** -> **Status** page to verify the secure software version on your system.



4.3. ASTi Customized SRR Report

For each security software release, ASTi runs the DISA SRR scripts and generates a report with required customer actions. This report is provided as a PDF on a CD-ROM. The report can be viewed on any machine that can read PDFs. The CD-ROM is labeled “ASTi Generated SRR Report for Telestra 3.” For a sample SRR report see http://www.asti-usa.com/telestra/srr_report.html.

Appendix A: Telestra Security Software Compatibility Matrix

Telestra Software Version	Security Software Version
3.30-1	TL3-Secure-1.0
3.1-1 through 3.29-1	Not Supported

Appendix B: Troubleshooting

How do I restore an account after I am locked out?

You can re-enable accounts via the GRUB menu by booting into single user mode as root. Follow the steps below to boot into single user mode and restore a locked out account called `<user-name>`.

1. Reboot the Telestra.
2. As soon as you see the GNU GRUB screen, type the letter '`p`'.

   IMPORTANT: You have 10 seconds to do this before it starts booting. If you are too late and it starts booting, immediately press the reset switch and try again.
3. After you type '`p`', you are prompted for a password. Type in your grub password. If you have not changed the password, type the default grub password:

   ```
   abcd1234
   ```
4. After successfully entering the grub password, type the letter '`e`'.
5. Then press the down arrow, type '`e`' again, press `backspace`, then type '`single`', press `enter`, and type '`b`'.
6. The Telestra will boot into single user mode.
7. Enter the root password to login.
8. Type the following command to re-enable the user account you are interested in:

   ```
   faillog -u <username> -r
   ```
9. Type '**reboot**' to reboot the Telestra. The user should be able to login as rmsuser.

All System Account (including the 'root' user) passwords will expire after 60 days.

How do I change my system account password, which has expired (after 60 days)?

If your system account password is expired, and you are trying to login in Development mode via the X, your only indication is a "`Login incorrect`" message.

If your system account password is expired, and you are trying to login on the text console screen, you will see the following:

`You are required to change you password immediately (password aged).`

`Changing password for` <your username>

`(current) UNIX password:` <type your **old** password again (the one you just typed in)>

`New UNIX password:` <see **Unix Password Guidelines** below>

`Retype new UNIX password:`

This password will expire again in two more months.

Unix Password Guidelines

- Must have at least 10 characters.
- Must have at least two (2) numbers.
- Must have at least two (2) special characters, for example, $#-!
- Must have at least two (2) upper case letters.
- Must have at least two (2) lower case letters.
- Cannot spell any common known dictionary words.

How do I change my root password, which has expired (after 60 days)?

If the root system account password is expired, you will find out when you try the '`su`' command, because security requirements prevent the root user from logging in directly. When you supply the correct root password to the '`su`' command, you will see the following:

```
You are required to change your password immediately (password aged).

su: Authentication token is no longer valid; new one required.

Sorry.
```

At this point, to access superuser privilege, you must reboot into single-user mode and login as root in order to update root's password. Follow the procedures below:

1. Use a privileged RMS account (using a web browser on another system) to reboot the Telestra. If you can't do this, hit the reset switch on the front of the Telestra.
2. As soon as you see the GNU GRUB screen, type the letter '`p`'.

   IMPORTANT: You have 10 seconds to do this before it starts booting. If you are too late and it starts booting, immediately press the reset switch and try again.

1. After you type '`p`', you are prompted for a password. Type in your grub password. If you have not changed the password, type the default grub password:

   ```
   abcd1234
   ```

3. After successfully entering the grub password, type the letter '`e`'.
4. Then press the down arrow, type '`e`' again, press `backspace`, then type '`single`', press `enter`, and type '`b`'.
5. The system should then start to boot in single user mode, you will see the following:

   ```
   Give root password for maintenance

   (or type Control-D for normal startup):
   ```

   Enter the old root password, and the prompt should read:

   ```
   root@telestra:~#
   ```

   Now you can change your root password by executing the '`passwd`' command:

   ```
   root@telestra:~# passwd

   New UNIX password: <enter your new password, see Unix Password Guidelines on previous page>

   Retype new UNIX password: <enter it again>

   passwd: password updated successfully
   ```

   Now you can type '`reboot`' and return to normal operation.

How do I change the grub password?

1. To change the grub password, type ‘su’ at the ‘$’ prompt, example:

   `$ su`

2. The prompt will ask for the root password:

   `Password:` <supply root password>

3. Type:

   `# grub`

4. The prompt will display the grub version:

   `GNU GRUB version 0.95 (640K lower / 3072K upper memory)`

   [Minimal BASH-like line editing is supported. For the first word, TAB lists possible command completions. Anywhere else TAB lists the possible completions of a device/filename.]

5. At the ‘`grub>`’ prompt, type ‘`md5crypt`’, example:

   `grub> md5crypt`

6. The prompt will ask for a password:

   `Password:` <type new grub password>

   Then it will display a long string of characters:

   `Encrypted: $1$tLTIQ$Jzsm.WJERuWbK4iAIwdZA0`

7. Write down the long string of characters after "`Encrypted:`". This is the encrypted password which you must put into the `/boot/grub/menu.lst` file.

8. Type:

   `grub>  quit`

9. As the root/superuser edit the `/boot/grub/menu.lst` file and find the line:

   `password --md5` <old long string of characters>

10. Replace the <old long string of characters> with the <new long string of characters> obtained from the `md5crypt` grub command.

11. Save the file and reboot.

12. Test the new password by typing '`p`' at the grub menu.

    If you are unable to edit (using '`e`' after supplying the correct grub password), then you probably either copied the md5crypt string incorrectly or supplied a different password (perhaps a typo?) to the md5crypt grub command. Try again until you are able to successfully use the 'e' grub command.

