VOSS Insights
Dashboard and Arbitrator Maintenance and Upgrade Guide

Release 23.2

Jul 31, 2023

Legal Information

DOCUMENT ID: 20230731125019

Contents

1. Upgrade

1.1.   Pre Checks

1. Verify your access to the UI, then verify the application version via the profile menu (your username), for example, **admin** (top right).
2. Verify available storage of the disk of the server, via system/stats dashboards.

1.2.   Backup VM Before Upgrade

If the application is a Virtual Machine (VM), then a pre-upgrade snapshot is recommended.

1.3.   Backup Dashboards before upgrades

1. Log in to the UI as admin.
2. Click on your profile name (top right). As super user, this is **admin**.
3. From the drop-down, select **Import/Export Wizard**.
4. Click the **Export** tab.
5. Select all the dashboards.
6. Click the **Export .lxtr** blue button on the top right.
7. Click the **Download** button, then save to your local computer or a secure network location.

1.4.   Backup Arbitrator Before Upgrade

1. Log in to the UI as admin.
2. Select the System Configuration icon (spanner), then select the **Import & Export** icon (down arrow).
3. Drag the following items from the **Configuration Items** pane to the **Export** pane:
    - Asset Entries
    - Asset Groups

- Controls
- Policy Modules
- Probe Groups
- Response Procedures
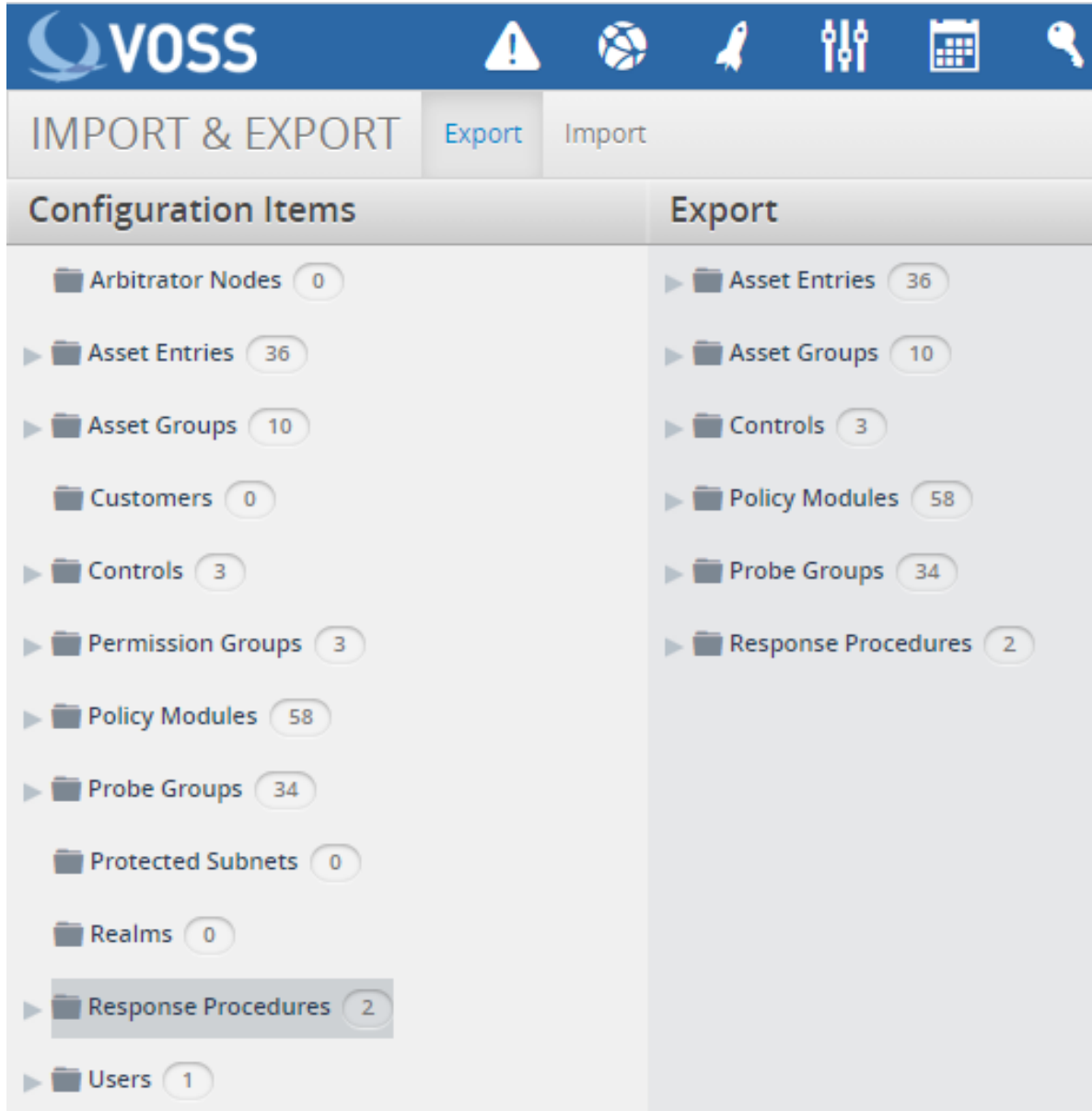
4. Click **Export**
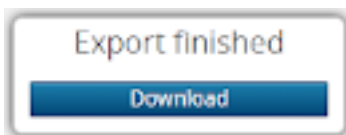
5. Click **Download**, then save to your local computer or a secure network location.

1.4.1.   Admin Menu Backup (Arbitrator or Dashboard)
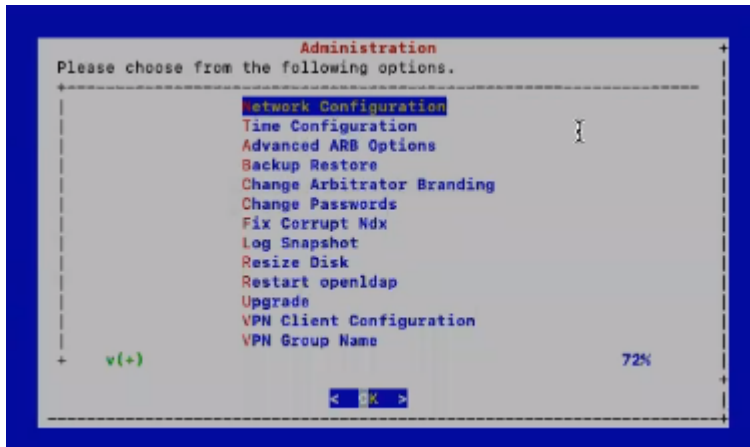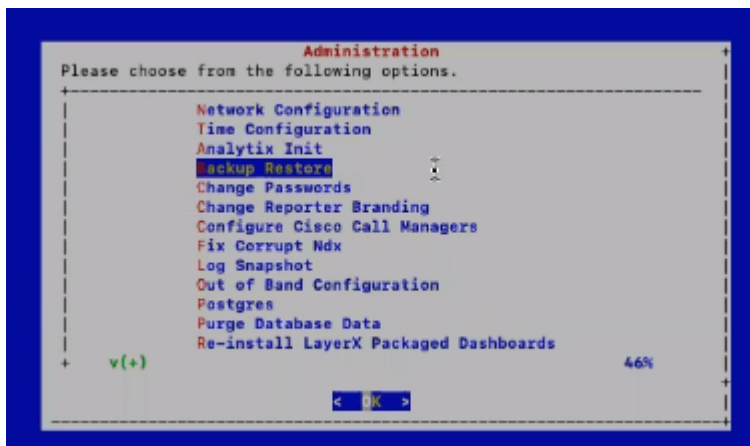
1. Log in to server using *Putty* via the admin account.

2. From the admin account **Administration** menu:

Arbitrator

or Dashboard

choose **Backup Restore**, and then choose **Create a backup**.
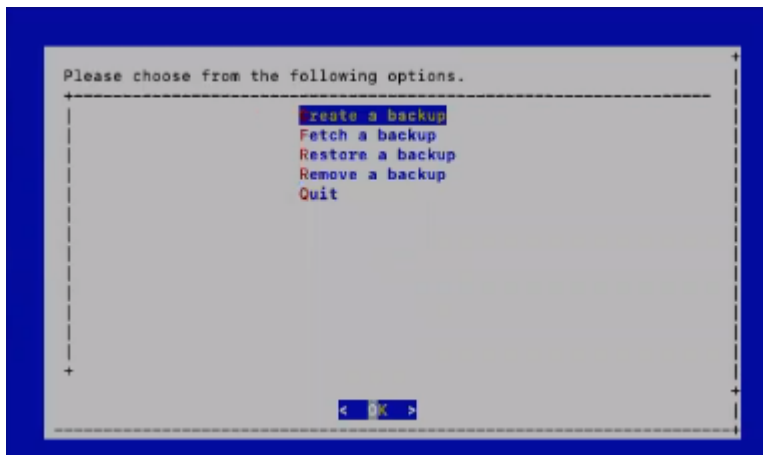
This backup creates a backup `tar.bz2` file in the `lxt_archive/` directory.

If needed, then the **Administration** menu can be used to restore a selected backup.

***
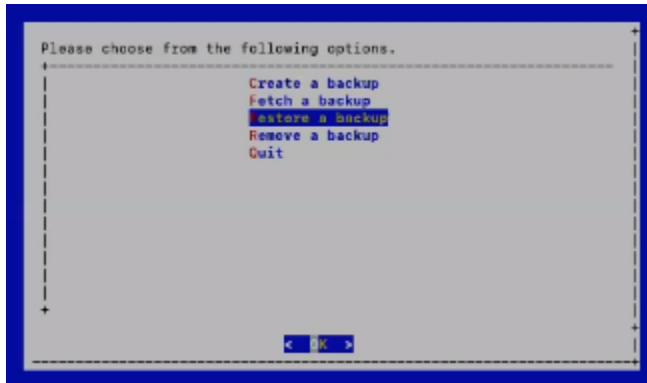
Note: If any themes were present on the system, these are also backed up and will also be available from the restore list.

***

1.5. Upgrade Timings

- Arbitrator = Approx 20-30 Mins
- Dashboard = Approx 20-60 Mins

1.6. Upgrade Method of Procedure (MOP)

1. Using *Winscp* and the drop account, copy the file (example file for the arbitrator `insights-arbitrator-<from>-<to>.lxsp`) to the `lxt_upgrade` directory.

2. Log in to server using *Putty* via the admin account.

3. Select **Upgrade** from the admin menu.
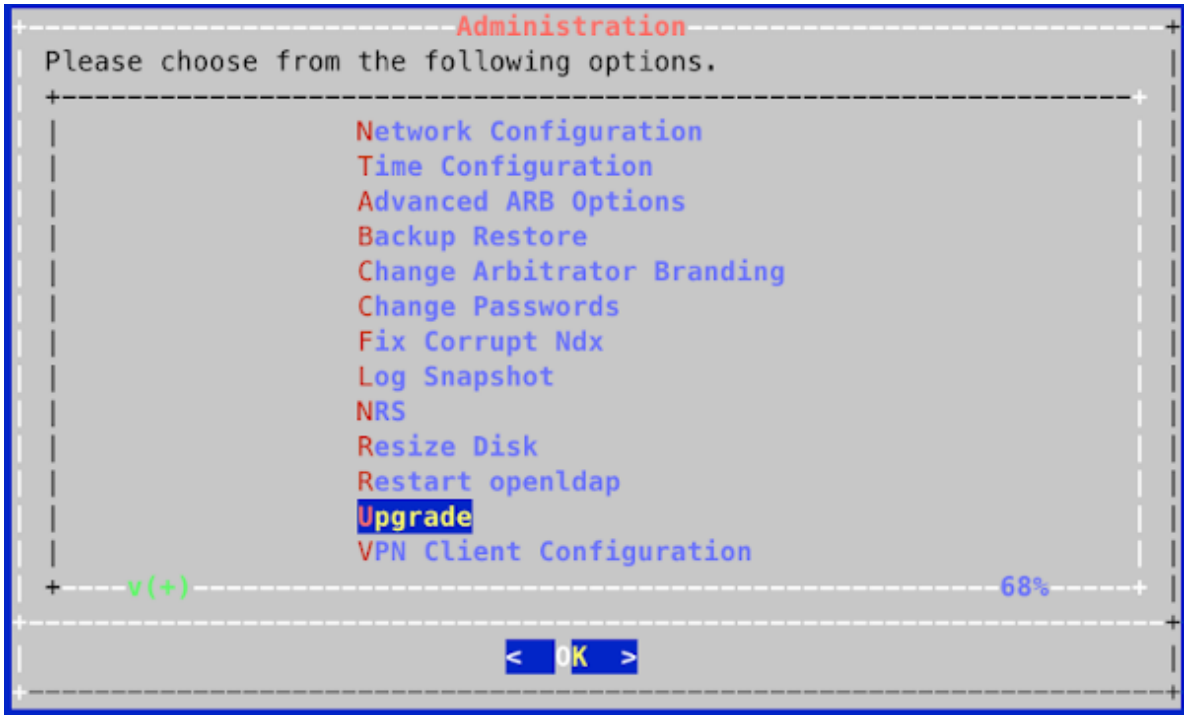
4. Select the **Check and Upgrade** option.
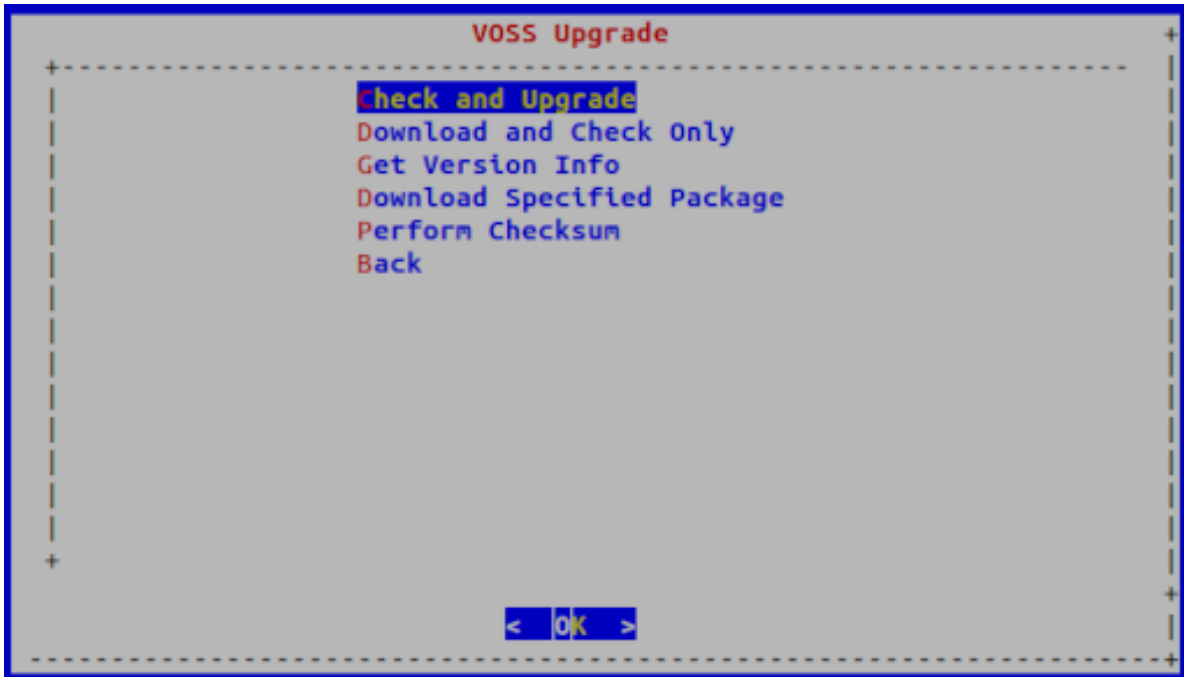
1.7.   Patch Install Steps

1. Using *Winscp* and the drop account, copy the file (example file for the arbitrator `insights-arbitrator-<from>-<to>.lxsp`) to the `lxt_upgrade` directory.

2. Log on to the server using *Putty* and the admin user credentials

3. Navigate down to **Upgrade**
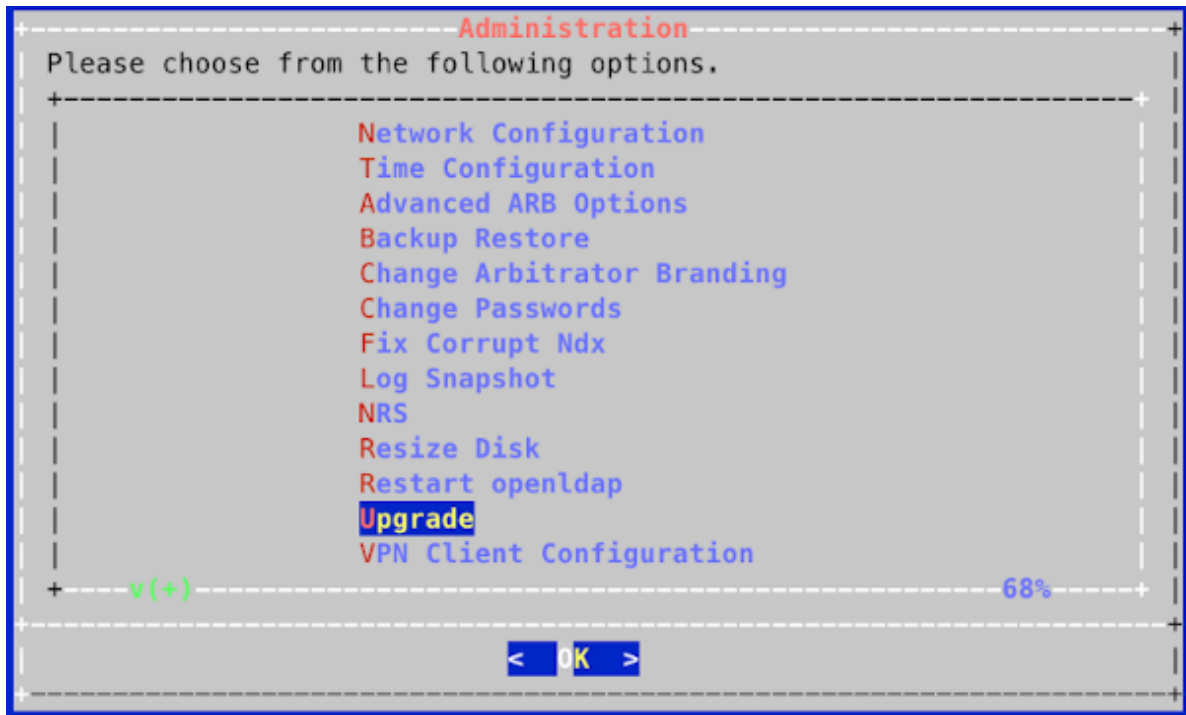
4. Select **Check and Upgrade**:
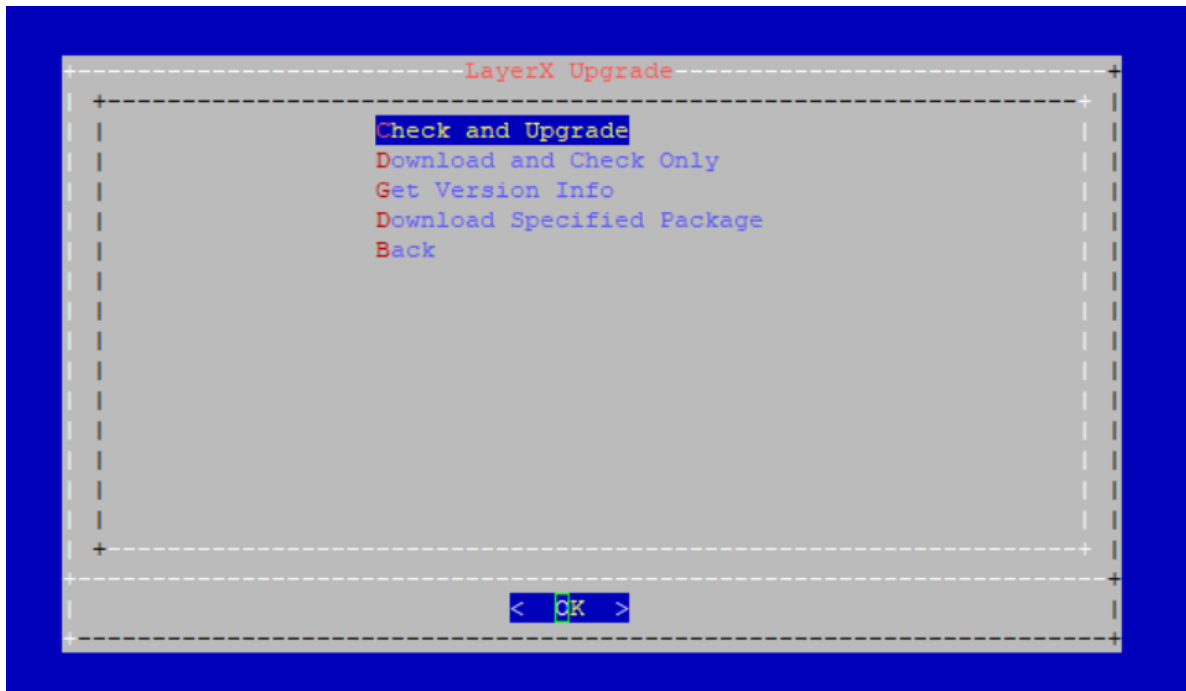
(Optional) Select **Perform Checksum** and enter the downloaded filename. This step will verify the downloaded file against its `.sha256` file.

5. After the upgrade is complete, reboot the server and log in again to verify.

1.8.   Post Checks

Check the system's version by selecting the **About** menu in the UI, for example:
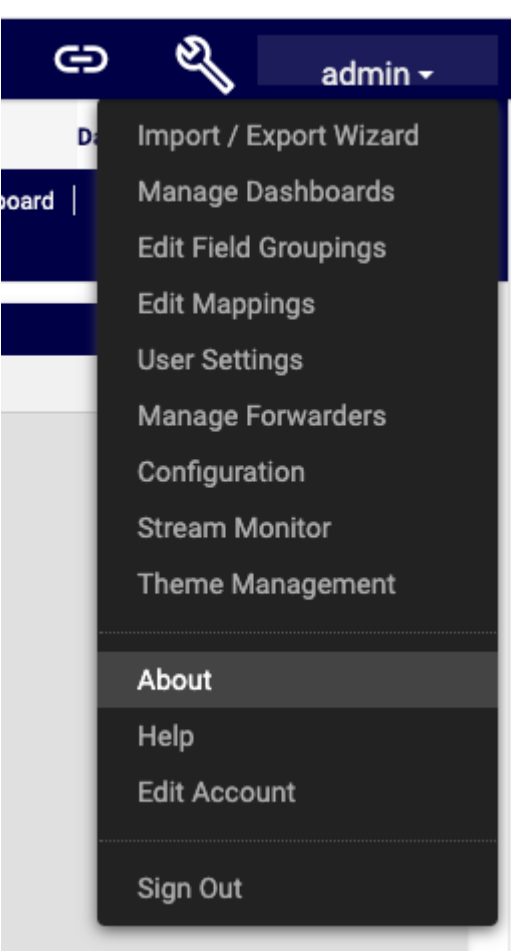
or

Note: If the version does not appear to be updated, then clear your browser's cache and reconnect.

2.   Add or Update Certificates

Users can now update SSL Certificates and SSL keys from the Admin console menu.

```
---------------------------Network Configuration---------------------------+
 What would you like to configure?                                         |
 +-------------------------------------------------------------------------+
 |                      Interface Settings                                 |
 |                      DNS Settings                                       |
 |                      Hostname                                           |
 |                      Apache Certs                                       |
 |                      Apache Config                                      |
 |                      SSH Config                                         |
 |                      SSHD Config                                        |
 |                      Quit                                               |
 |                                                                         |
 |                                                                         |
 +-------------------------------------------------------------------------+
                                                                           |
                          <  OK  >                                         |
 --------------------------------------------------------------------------
```
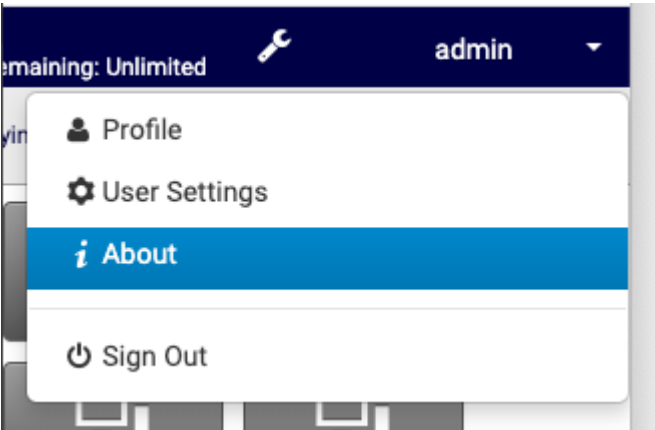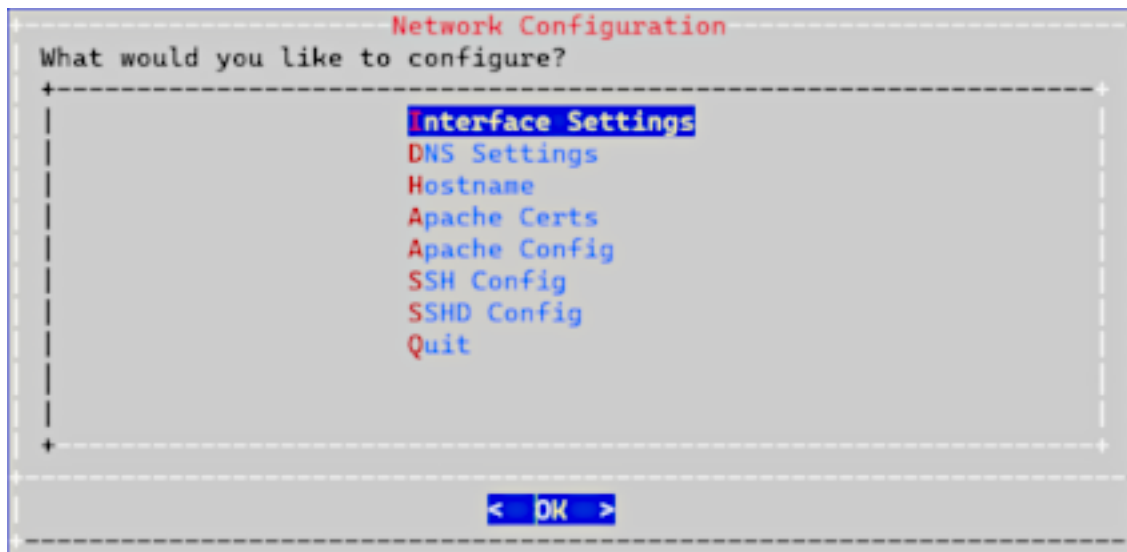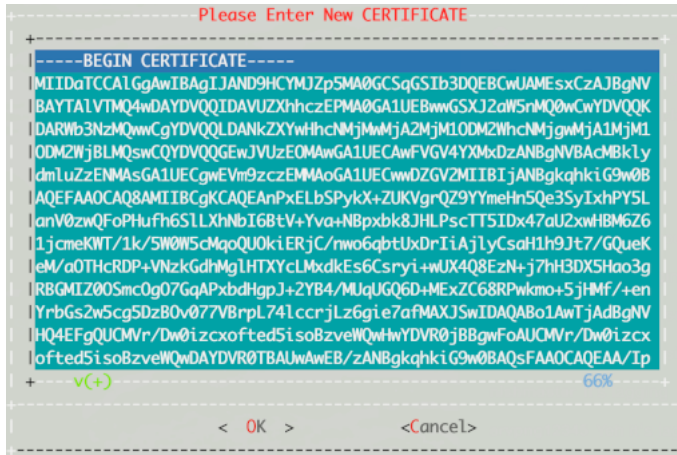
2.1.   Add Certificates

To add your own certificate, you will need both the certificate and private key.

1. SSH to the system using admin account

2. Select **Network Configuration**

3. Select **Apache Certs**

4. Select **Insert Cert**

5. Paste in customer certificate

   A certificate has the following header and footer

   ```
   --BEGIN CERTIFICATE--
   --END CERTIFICATE--
   ```

6. Select **Insert Private Key**

7. Paste in customer private key

   A private key has the following header and footer

   ```
   --BEGIN PRIVATE KEY--
   --END PRIVATE KEY--
   ```


8. Select **Display Cert Details** to view certificate details.

9. Select **Back** and exit the menu.

10. Refresh the browser. The system should be using the new certificate.

2.2. Update Certificates

If you want to generate a new unsigned certificate or to reset a certificate and private key:

1. SSH to the system using admin account

2. Select **Network Configuration**

3. Select **Apache Certs**

4. Select **Generate New Unsigned Cert**

5. When prompted, fill in the information requested.

```
Generating a 2048 bit RSA private key
.................................................................
..............+++
writing new private key to '/etc/apache2/server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

6. Select **Back** and exit the menu.

7. Refresh browser. The system should be using the new unsigned certificate.

12