VOSS Insights
Dashboard and Arbitrator Maintenance and Upgrade Guide

Release 24.2

November 22, 2024

Legal Information

DOCUMENT ID: 20241122150530

Contents

1. What's New

1.1. Dashboard and Arbitrator Maintenance and Upgrade Guide: Release 24.2

- EKB-21341: DS9 database password management. See: *Upgrade and Maintenance*

  Added a new topic in the Maintenance and Upgrade Guide on DS9 password management.
- EKB-22054: Backup Arbitrator and Dashboard. See: *Upgrade and Maintenance*

  Added note on upgrade time change in release 24.2.

2. Upgrade and Maintenance

This topic covers the upgrade of Dashboard, Arbitrator and DS-9, as well as maintenance tasks such as *DS9 Database Password Management*.

2.1. 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.

2.2. Backup VM Before Upgrade

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

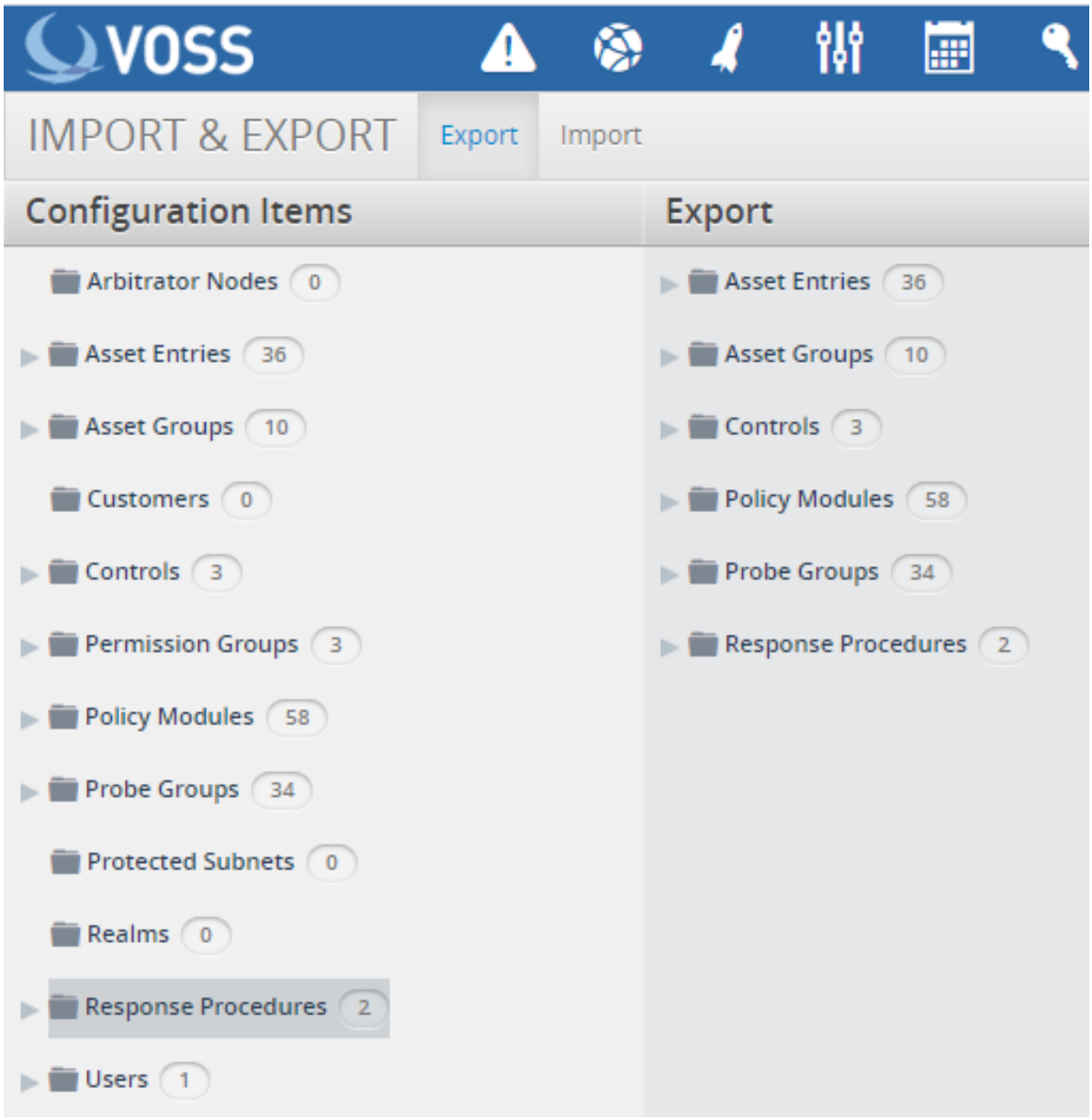
2.3. Backup Dashboards Before Upgrade

This procedure backs up dashboards before you start the upgrade.

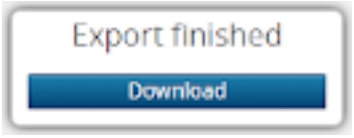
1. Log in to the Dashboard user interface as admin (superuser).
2. Click on the **System Configuration** icon (Cog), then select **Import/Export Wizard**.
3. On the **Export** tab, select all the dashboards.
4. Select all the dashboards.
5. Click the **Export .lxtr** button on the top right.
6. Click **Download**.
7. Save the file to your local computer or to a secure network location.

2.4. Backup Arbitrator Before Upgrade

1. Log in to the Arbitrator user interface as admin.
2. Click on the **System Configuration** icon (Cog), then select **Import**/**Export**.
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

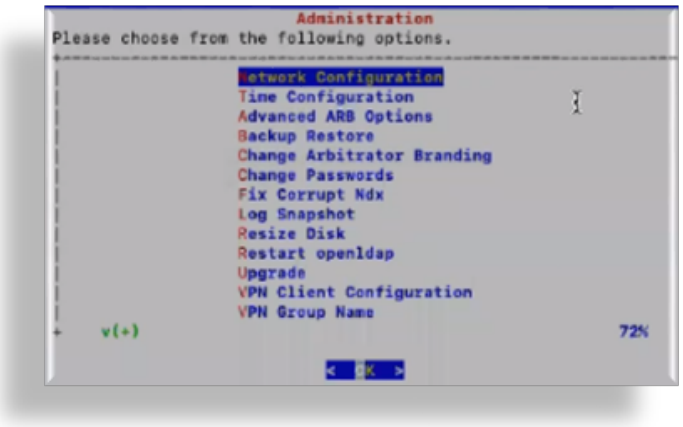


4. Click **Export**
5. Click **Download**, then save to your local computer or a secure network location.

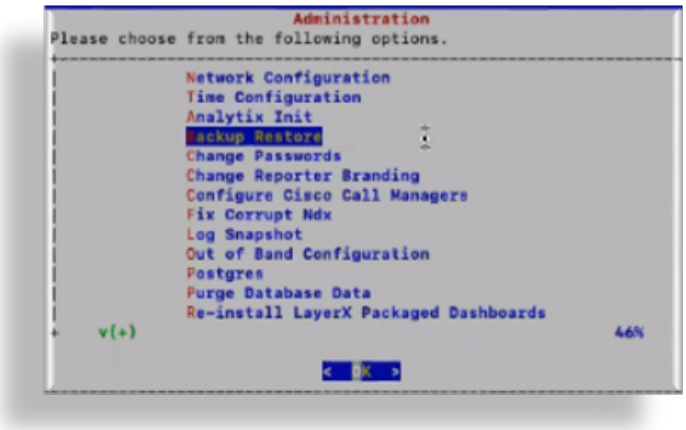


2.4.1. Admin Menu Backup (Arbitrator or Dashboard)

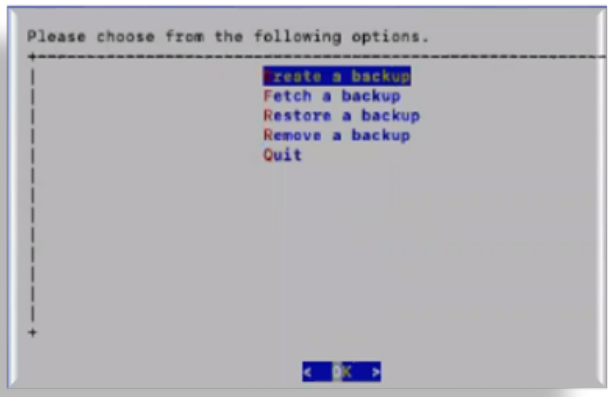
1. Log in to server using *Putty* via the admin account.
2. Go to the **Administration** menu (either Arbitrator or Dashboard):
   - Arbitrator



   - Dashboard

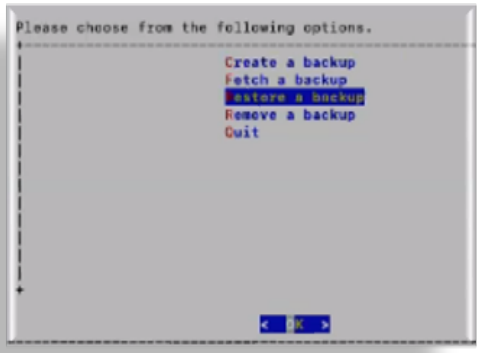


3. Select **Backup Restore**, and then choose **Create a backup**.



Note:

- This backup creates a backup `tar.bz2` file in the `lxt_archive/` directory. If required, the **Administration** menu can be used to restore a selected backup.



- Any themes that were present on the system are also backed up and will also be available from the restore list.

2.5. Upgrade

2.5.1. Upgrade Timings

Note: Since security updates have updated various operating system components, the total upgrade time is more than the averages for previous releases (doubled for DS9).

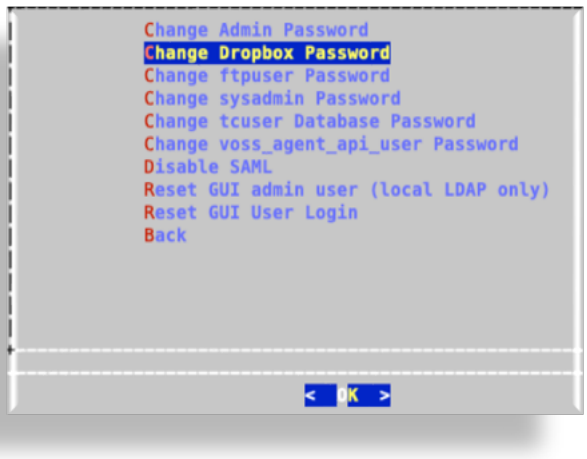
Averages:

- Arbitrator = Approx 40-60 Mins
- Dashboard = Approx 40-120 Mins
- DS9 = Approx 10-20 Mins

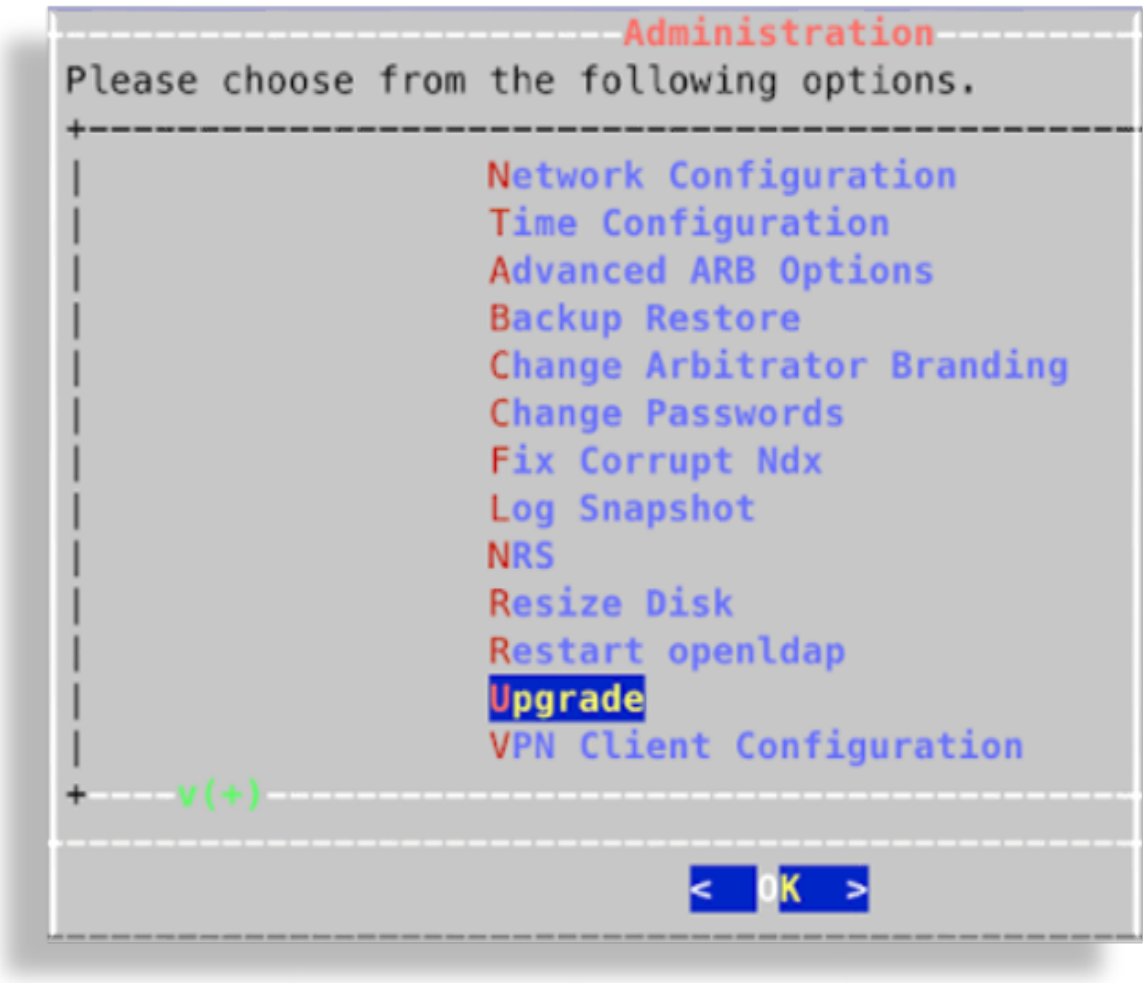
2.5.2. Upgrade Arbitrator or Dashboard

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.

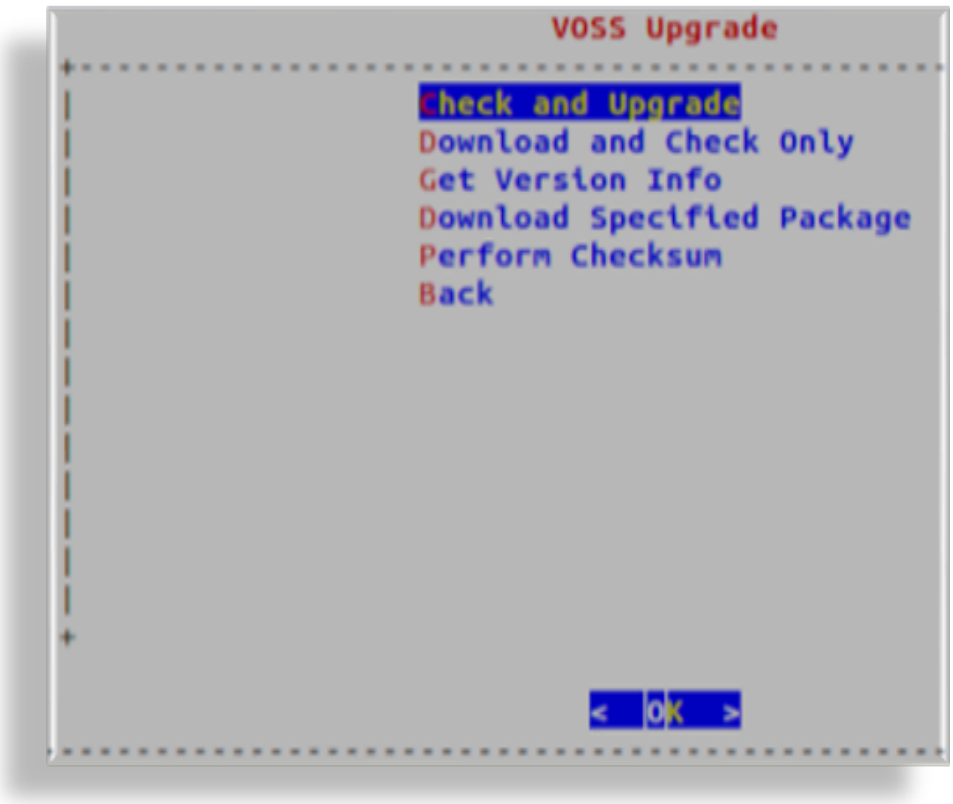
   Note: The drop account username is “drop”. You can set the password via the **Administration** menu.

2. Log in to the server using *Putty* via the Admin account.
3. From the **Administration** menu, select **Upgrade**.



4. On **VOSS Upgrade**, select **Check and Upgrade**, click **OK**.



2.5.3. Upgrade DS9

This procedure upgrades DS9.

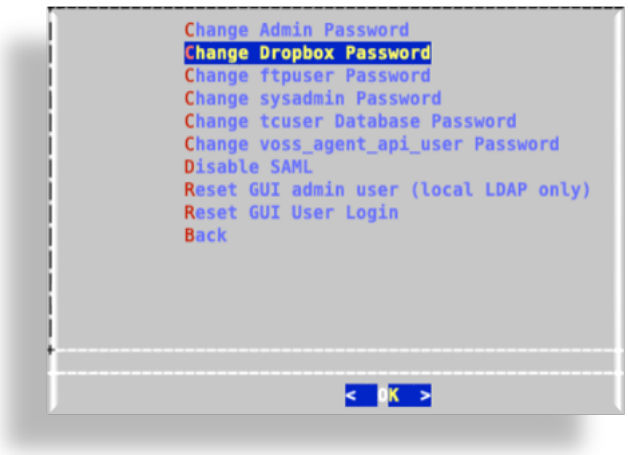
Pre-requisites:

- Using *Winscp* and the drop account, copy the `*.lxsp` file to be used for the upgrade into the drop account's *lxt_upgrade* sub-directory.

  Note:

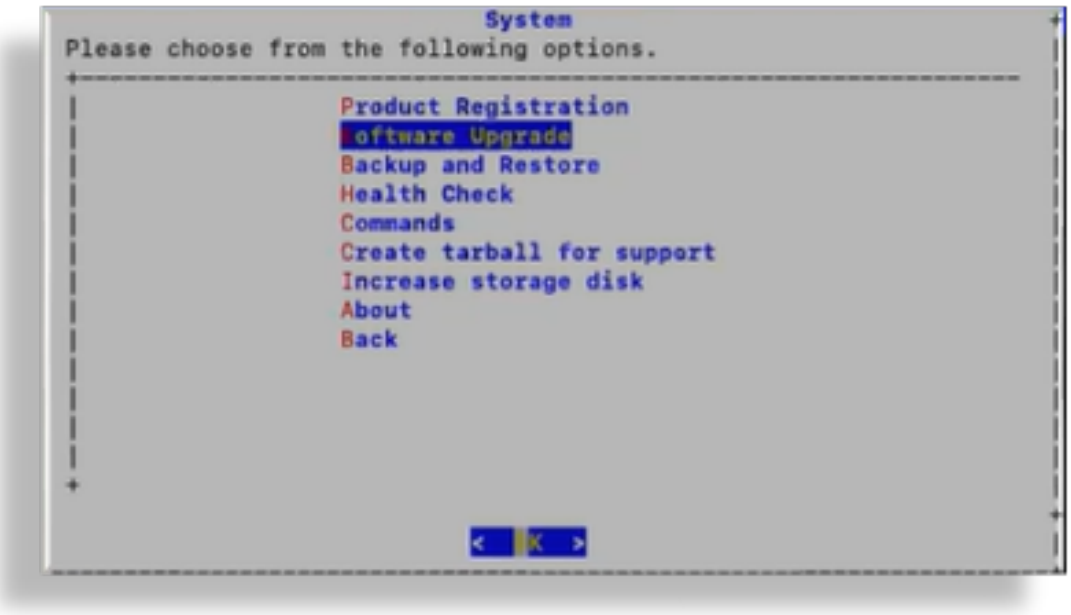
  – The naming convention for Insights upgrade files means that the system is able to detect the file to use for the upgrade. For Insights products, `*.lxsp` file is copied into the drop account's *lxt_upgrade* sub-directory, and the system fetches the file from that location.

  – The drop account username is "drop". You can set the password via the **Administration** menu.

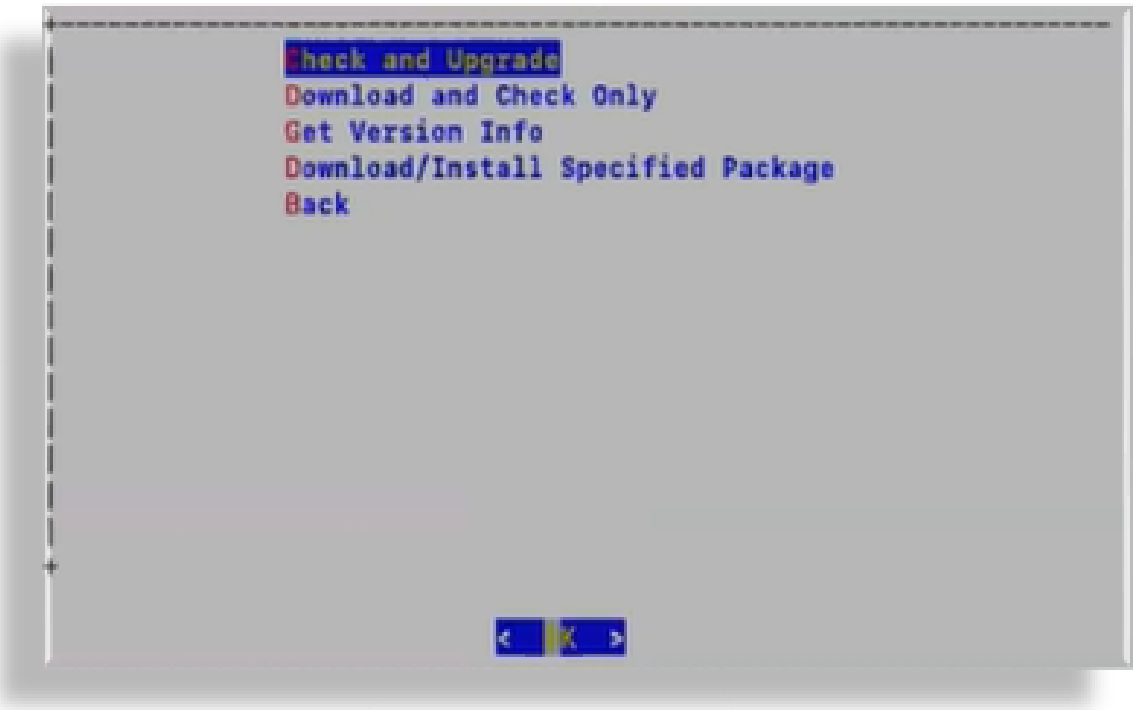


1. Connect to the DS9 server using an SSH client on port 22 and login using the admin credentials to access the **Administration** menu.

2. Select **System > Software Upgrade**.

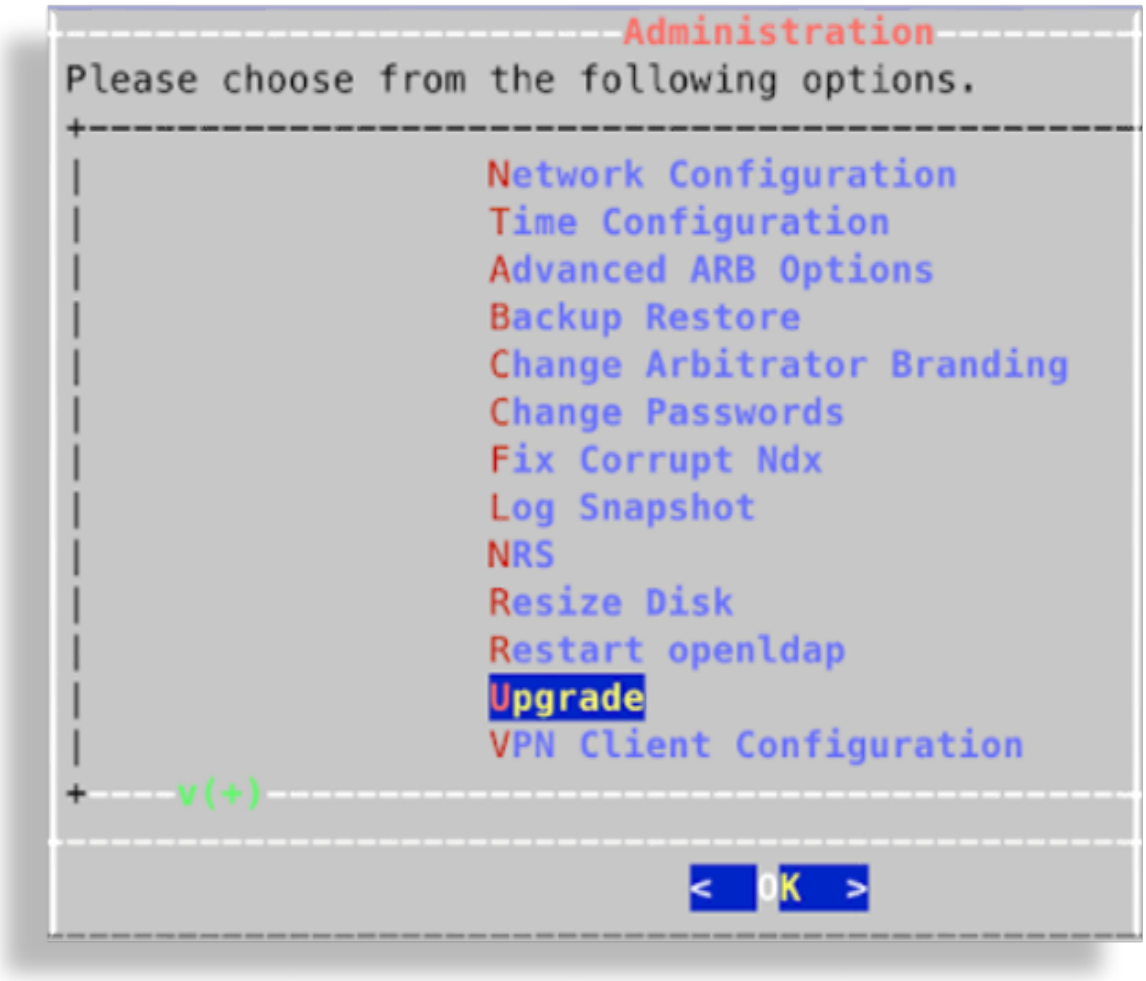


3. Select **Check and Upgrade**.

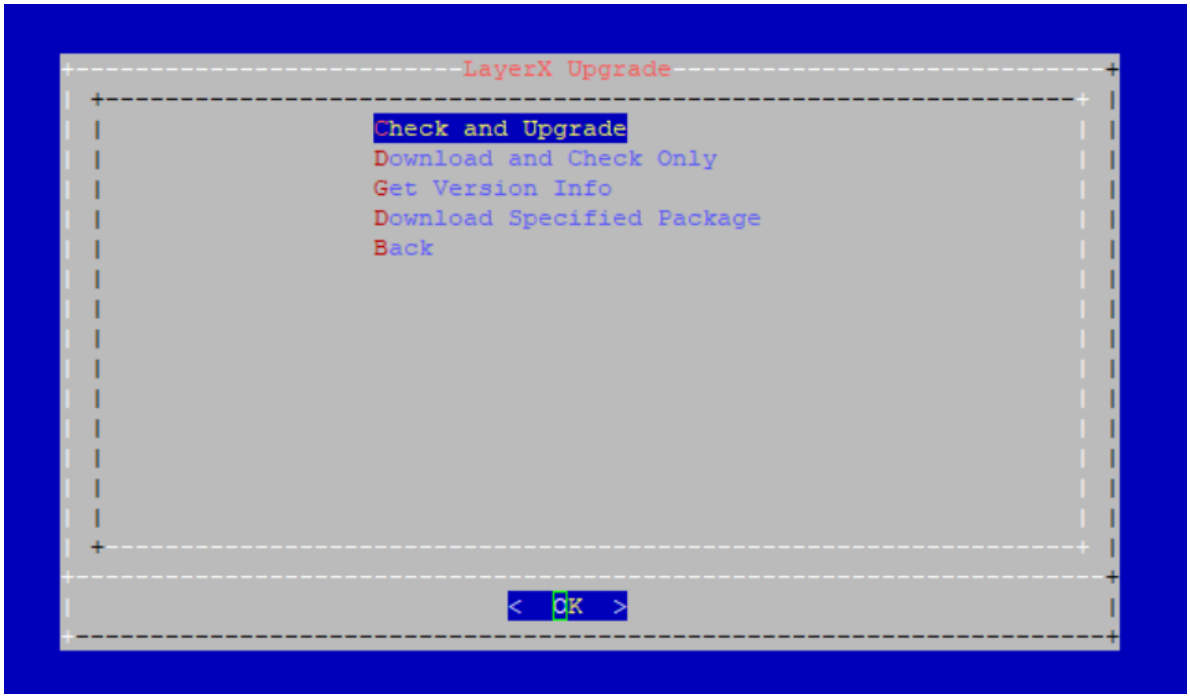


2.6. Patch Install Steps

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. From the **Administration** menu, select **Upgrade**



4. Select **Check and Upgrade**:

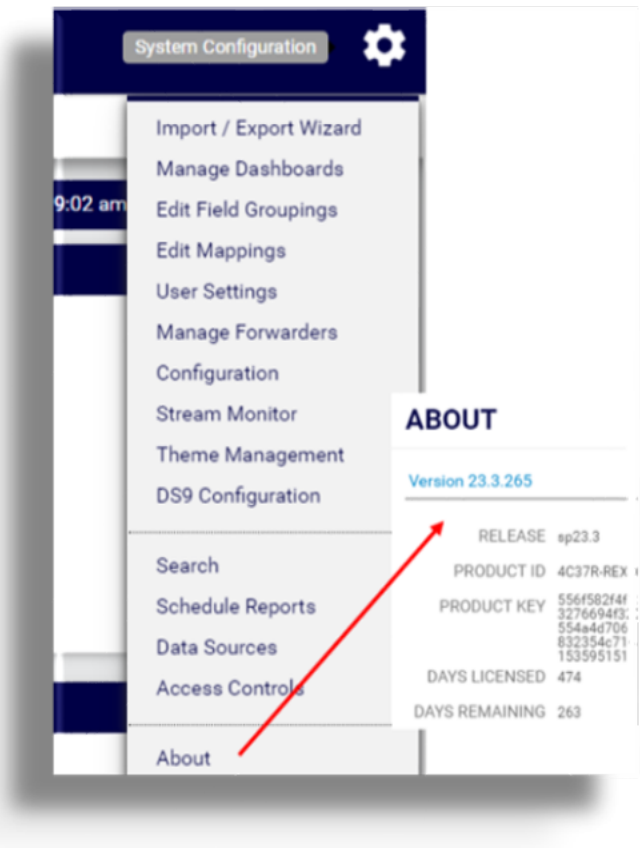


(Optional) Select **Perform Checksum** and enter the downloaded filename. This step will verify the downloaded file against its `.sha256` file.

5. Once the upgrade completes, reboot the server then log in again to verify.

2.7. Post Checks

Verify that the version of your system is updated. To do this via the GUI, click the **System Configuration** icon (Cog), then select **About**.



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

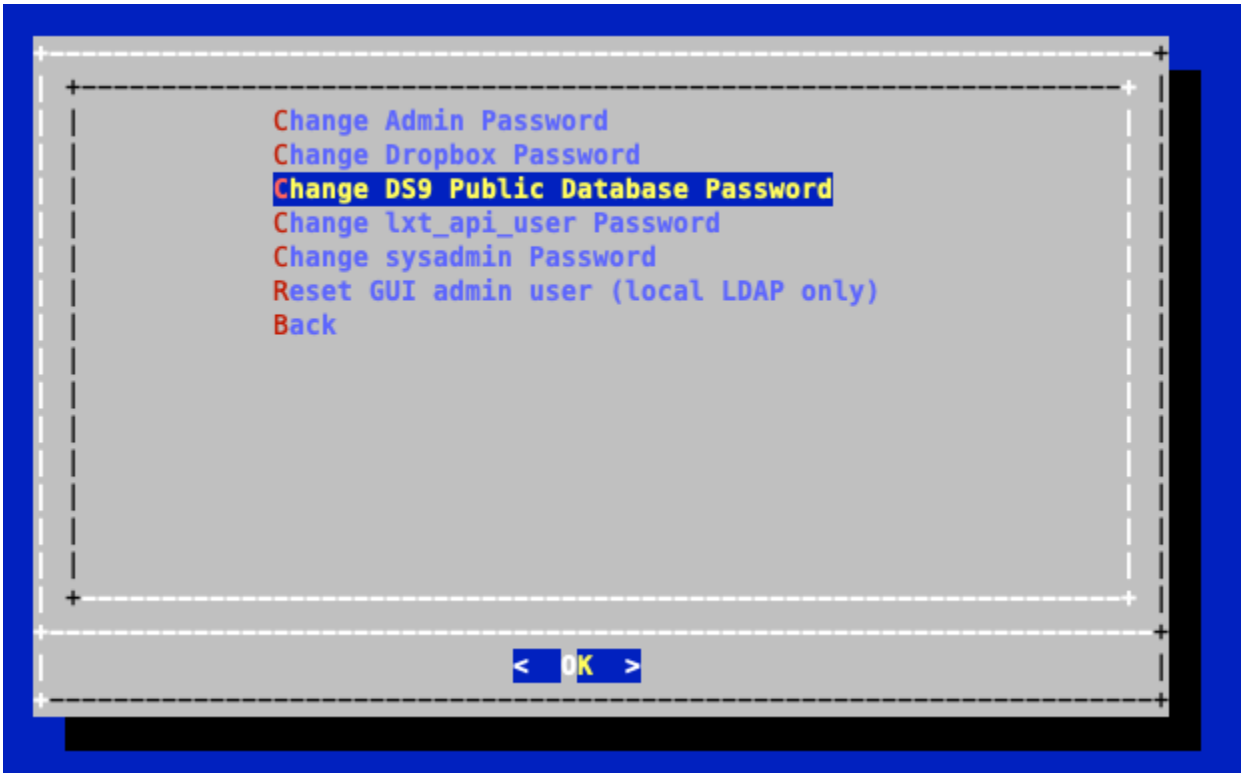
2.8. DS9 Database Password Management

DS9 is installed with a default, hidden password and Dashboard user `lxpublic`.

This database password can however be modified, as indicated below.

2.8.1. Maintain DS9 Database Password on DS9

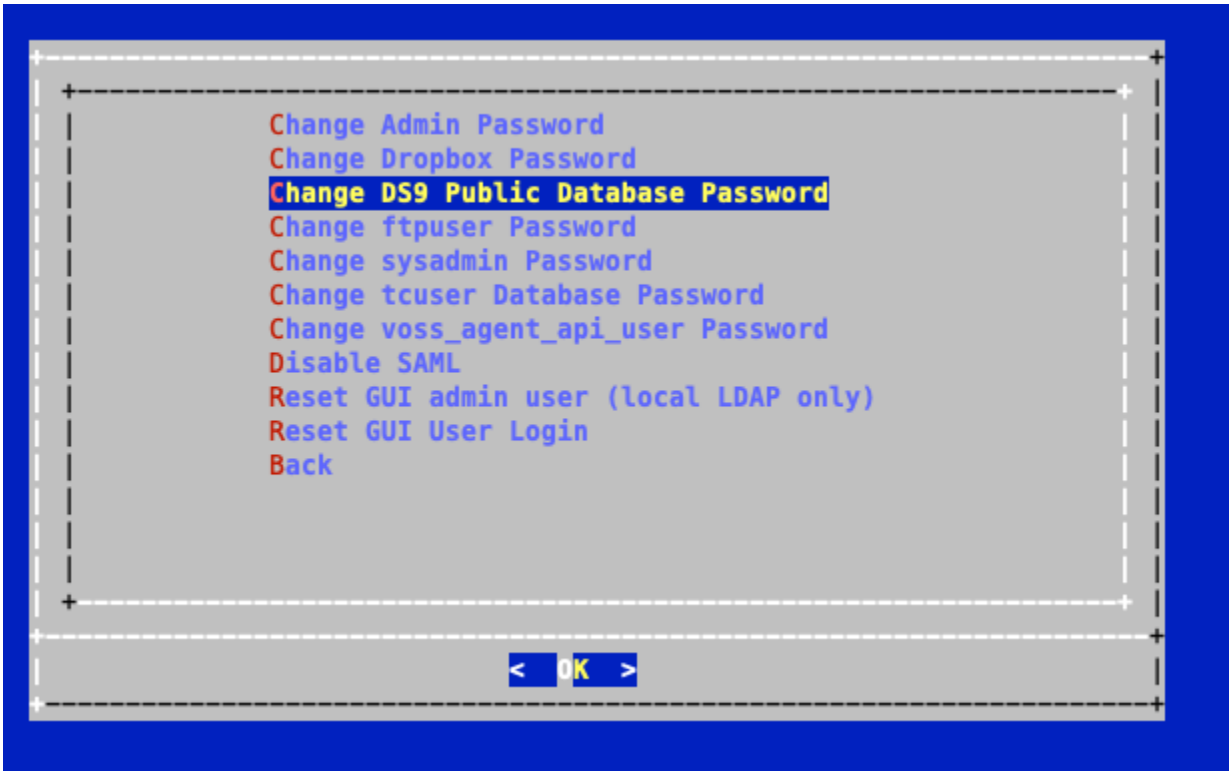
1. On the DS9 server, log in as `admin` from the console and from the **Administration** menu, select **Change Passwords**.
2. Select **Change DS9 Public Database Password** and modify the password. (Note: only alphanumeric characters are allowed)



3. Verify the credential configuration on the Arbitrator - see below.
4. Update the Dashboard **Data Sources** password for the DS9 server - see below.

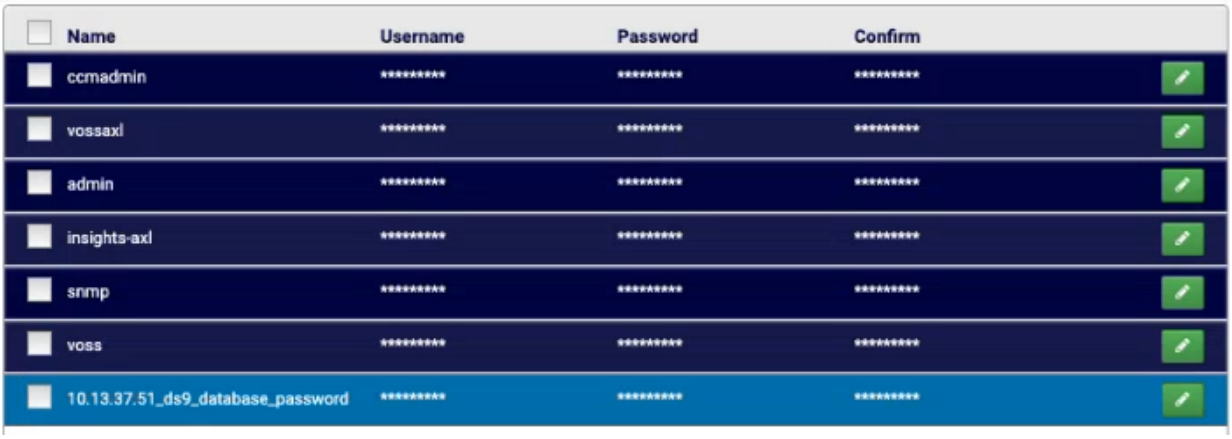
2.8.2. Maintain DS9 Database Password on Arbitrator

1. Log in as `admin` from the console and from the **Administration** menu, select **Change Passwords**.
2. Select **Change DS9 Public Database Password**.



3. Enter the DS9 IP address on the console and modify the password. (Note: only alphanumeric characters are allowed)

A change from the default credentials will also reflect on the Arbitrator menu: **CREDENTIAL CONFIGURATION**.



If this entry is removed, the DS9 credentials revert to the default, hidden credentials. While this entry can also be modified, it is advised to carry ou the task from the console **Change DS9 Public Database Password** menu.

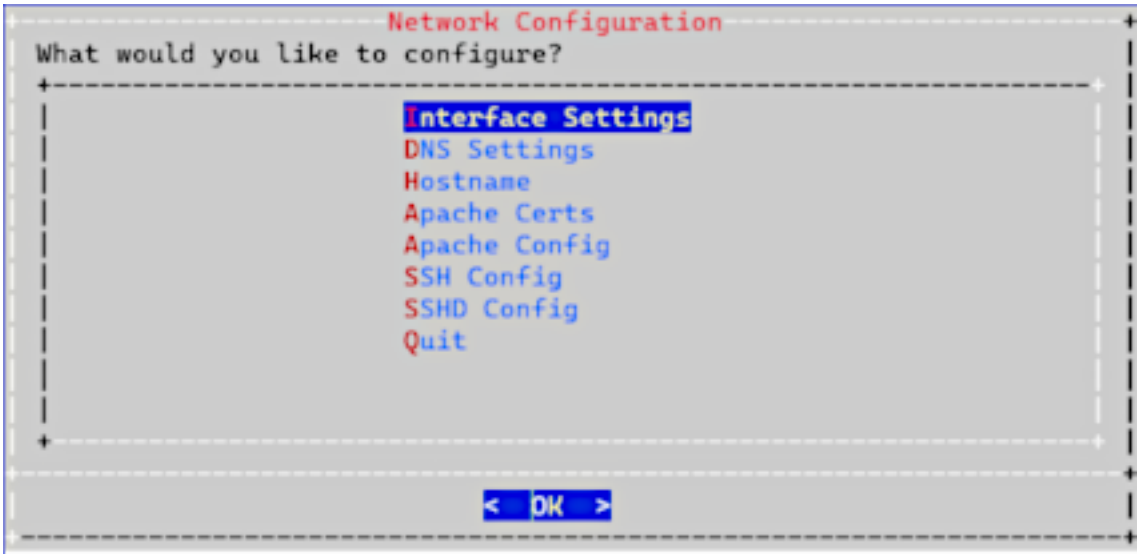
2.8.3. Maintain DS9 Database Password on Dashboard

When a DS9 server password is modified on DS9 or the Arbitrator as indicated above, the modified password needs to be updated on Dashboard the **Data Sources** entry.

1. From the **System Configuration** icon on the dashboard, select **Data Sources**.
2. Update the **Password** field for all **Data Sources** that match the related DS9 host.

3. Add or Update Certificates

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



3.1. 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.

3.2. 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.

6. Select **Back** and exit the menu.
7. Refresh browser. The system should be using the new unsigned certificate.