



VOSS



**VOSS Insights
Dashboard and Arbitrator Maintenance
and Upgrade Guide**

Release 24.2

November 22, 2024

Legal Information

- Copyright © 2024 VisionOSS Limited. All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20241122150530

Contents

- 1 What's New** **1**
 - 1.1 Dashboard and Arbitrator Maintenance and Upgrade Guide: Release 24.2 1

- 2 Upgrade and Maintenance** **2**
 - 2.1 Pre Checks 2
 - 2.2 Backup VM Before Upgrade 2
 - 2.3 Backup Dashboards Before Upgrade 2
 - 2.4 Backup Arbitrator Before Upgrade 3
 - 2.5 Upgrade 7
 - 2.6 Patch Install Steps 12
 - 2.7 Post Checks 13
 - 2.8 DS9 Database Password Management 14

- 3 Add or Update Certificates** **18**
 - 3.1 Add Certificates 18
 - 3.2 Update Certificates 19

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.

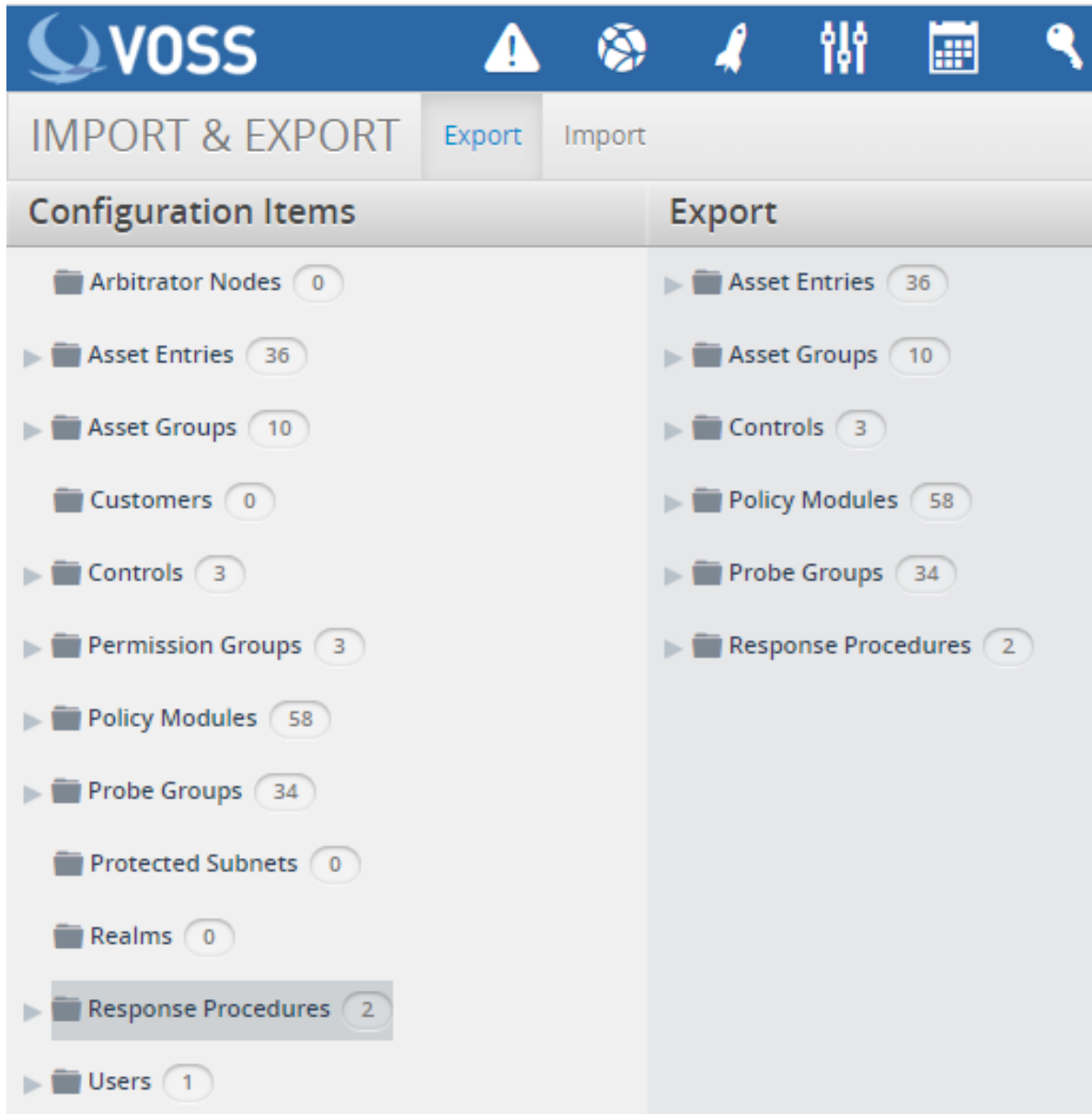
2.3. Backup Dashboards Before Upgrade

This procedure backs up dashboards before you start the upgrade.

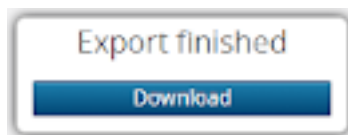
1. Log in to the Dashboard user interface as admin (superuser).
2. Click on the **System Configuration** icon (Cog), then select **Import/Export Wizard**.
3. On the **Export** tab, select all the dashboards.
4. Select all the dashboards.
5. Click the **Export .ixtr** button on the top right.
6. Click **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

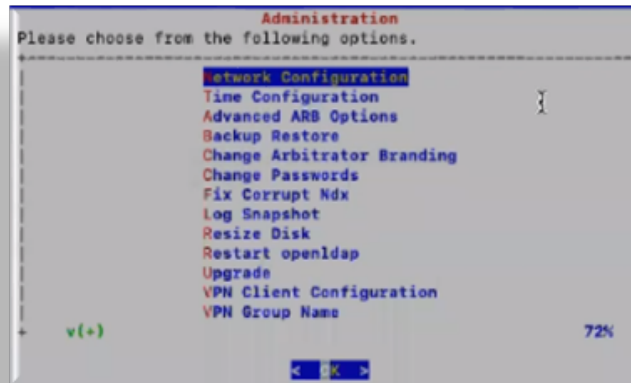


4. Click **Export**
5. Click **Download**, then save to your local computer or a secure network location.

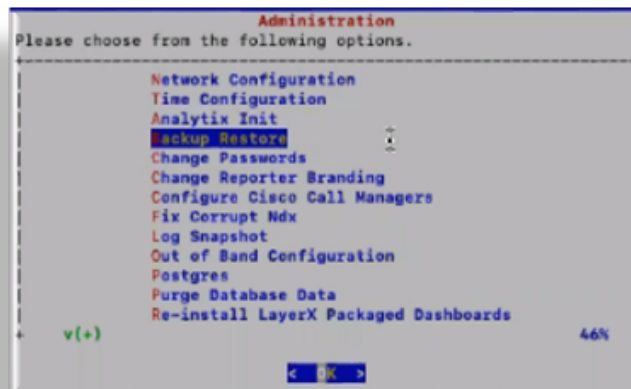


2.4.1. Admin Menu Backup (Arbitrator or Dashboard)

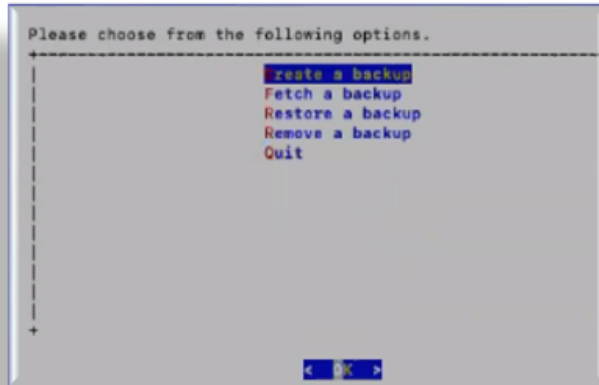
1. Log in to server using *Putty* via the admin account.
2. Go to the **Administration** menu (either Arbitrator or Dashboard):
 - Arbitrator



- Dashboard

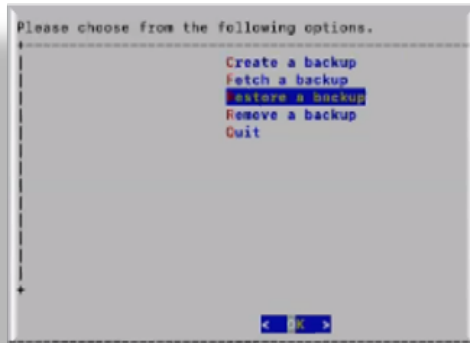


3. Select **Backup Restore**, and then choose **Create a backup**.



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).

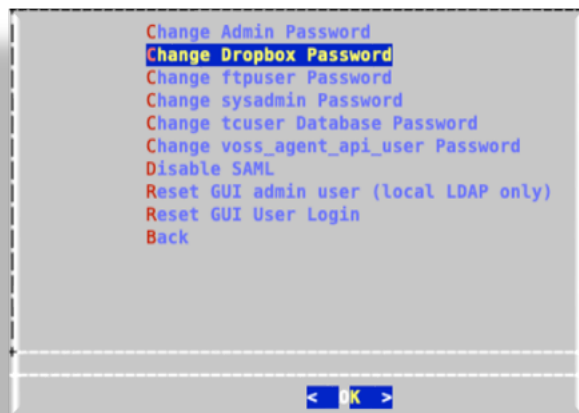
Averages:

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

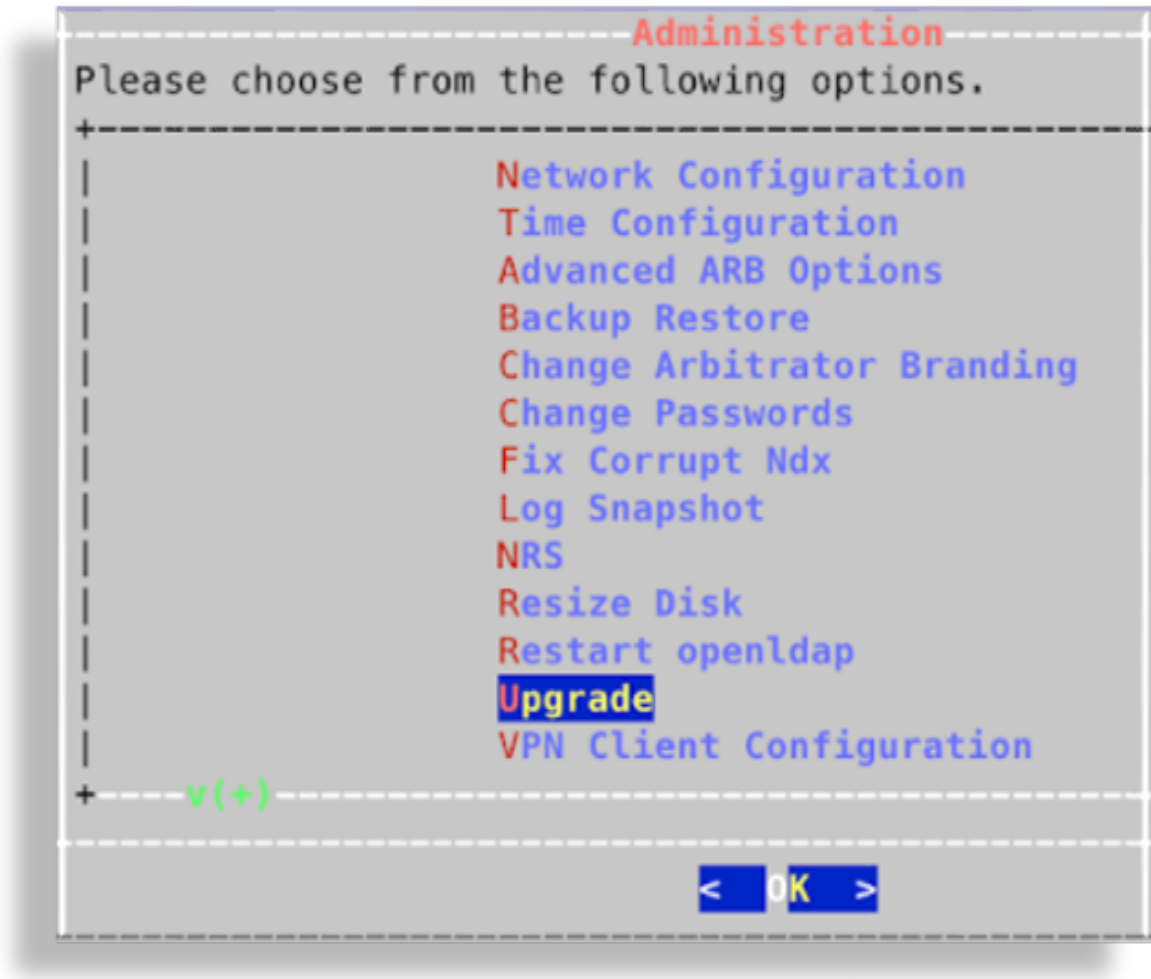
2.5.2. Upgrade Arbitrator or Dashboard

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.

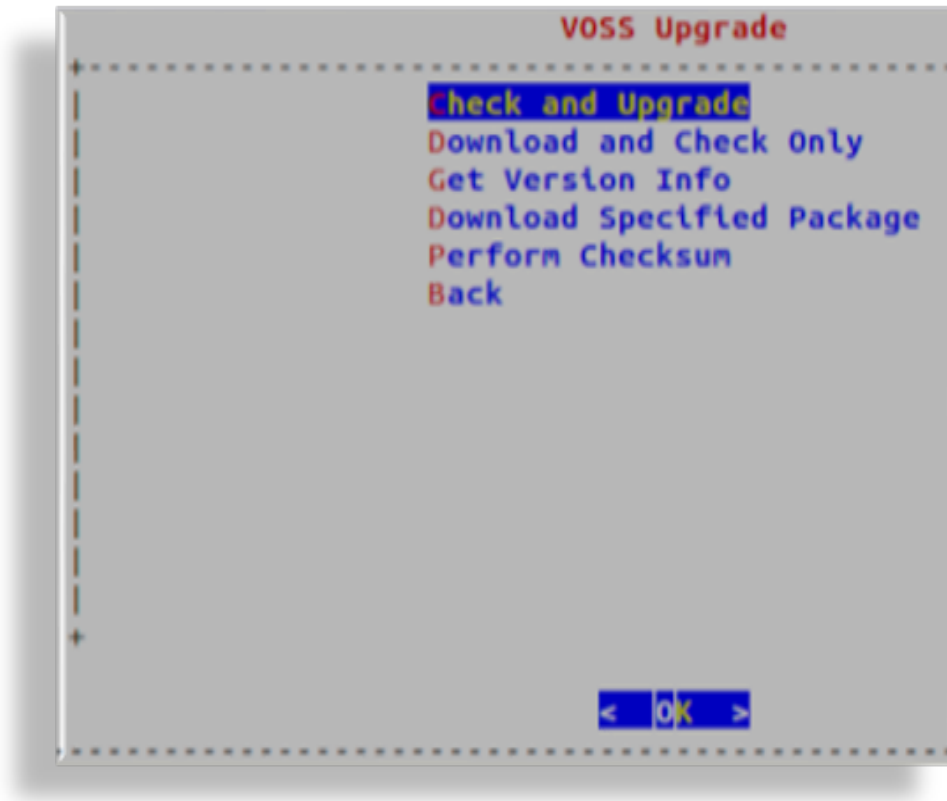
Note: The drop account username is “drop”. You can set the password via the **Administration** menu.



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:

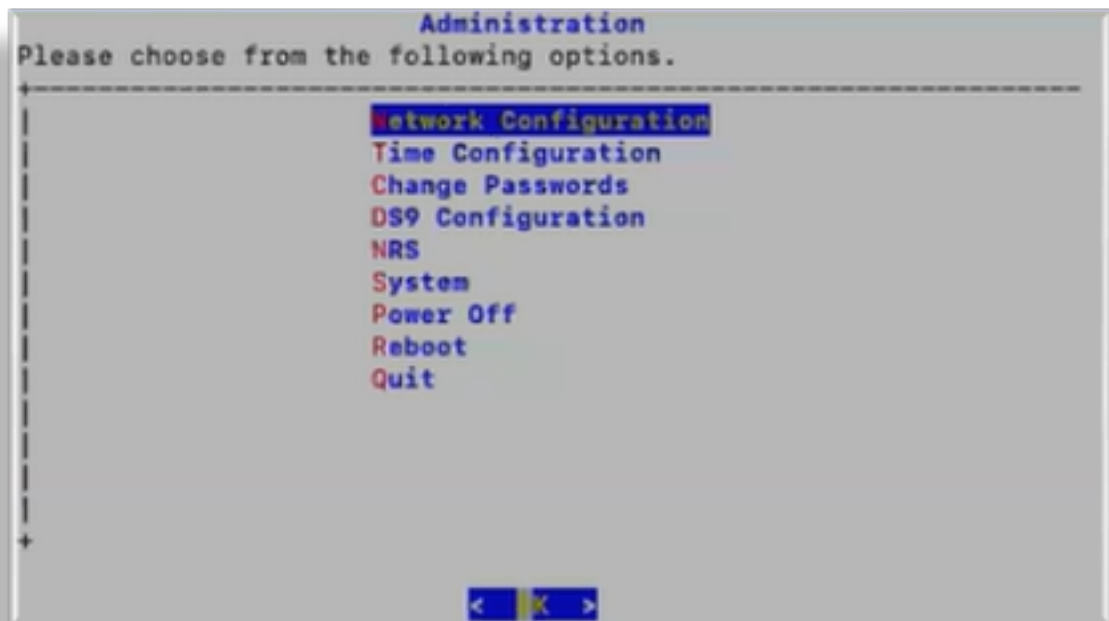
- Using *Winscp* and the drop account, copy the *.1xsp file to be used for the upgrade into the drop account's *lxt_upgrade* sub-directory.

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, *.1xsp 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.



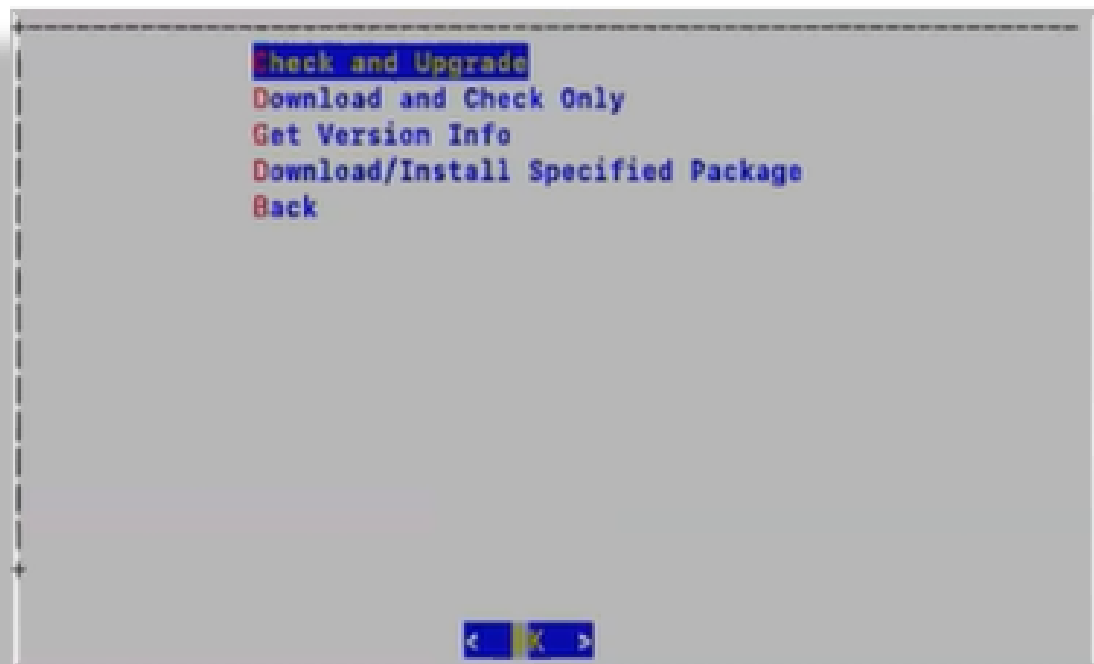
1. Connect to the DS9 server using an SSH client on port 22 and login using the admin credentials to access the **Administration** menu.



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

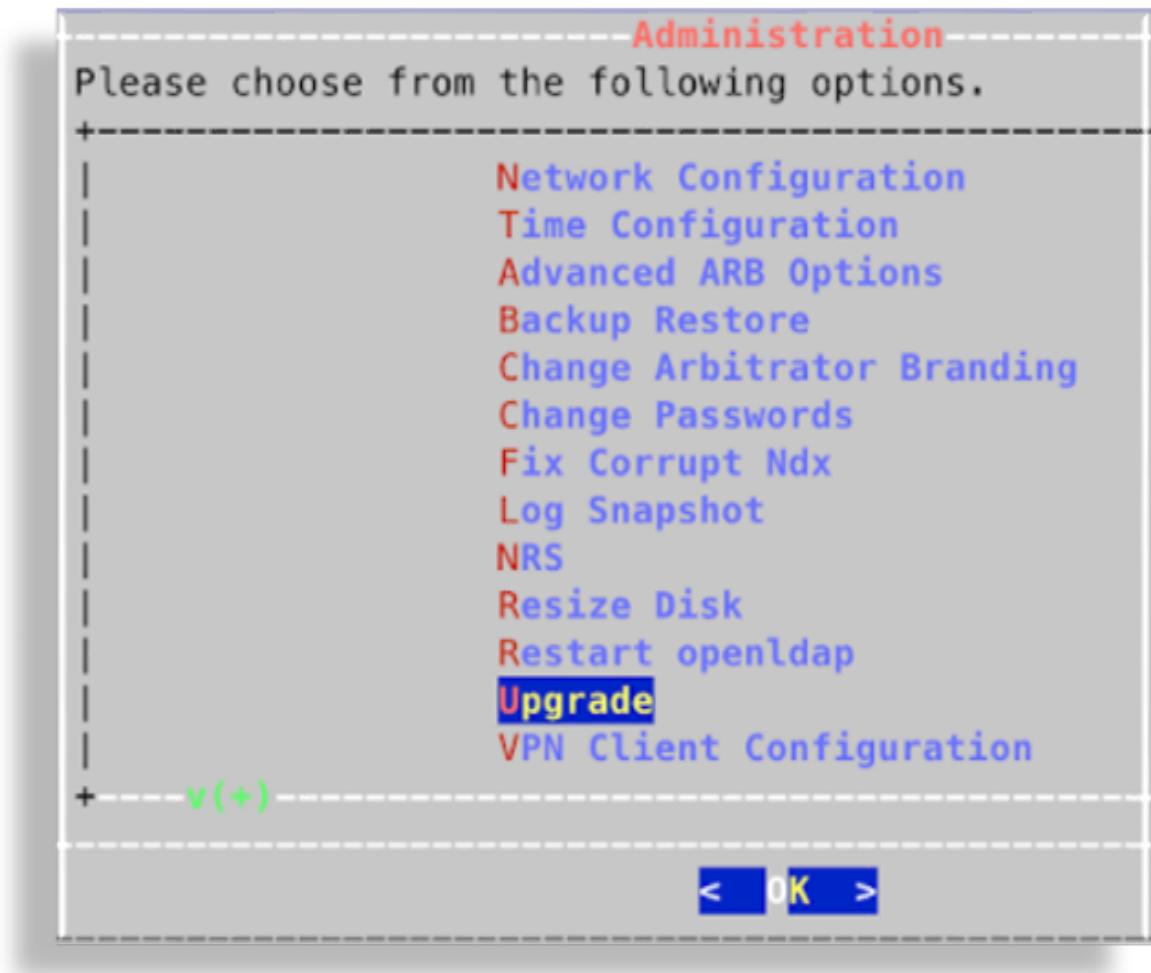


3. Select **Check and Upgrade**.

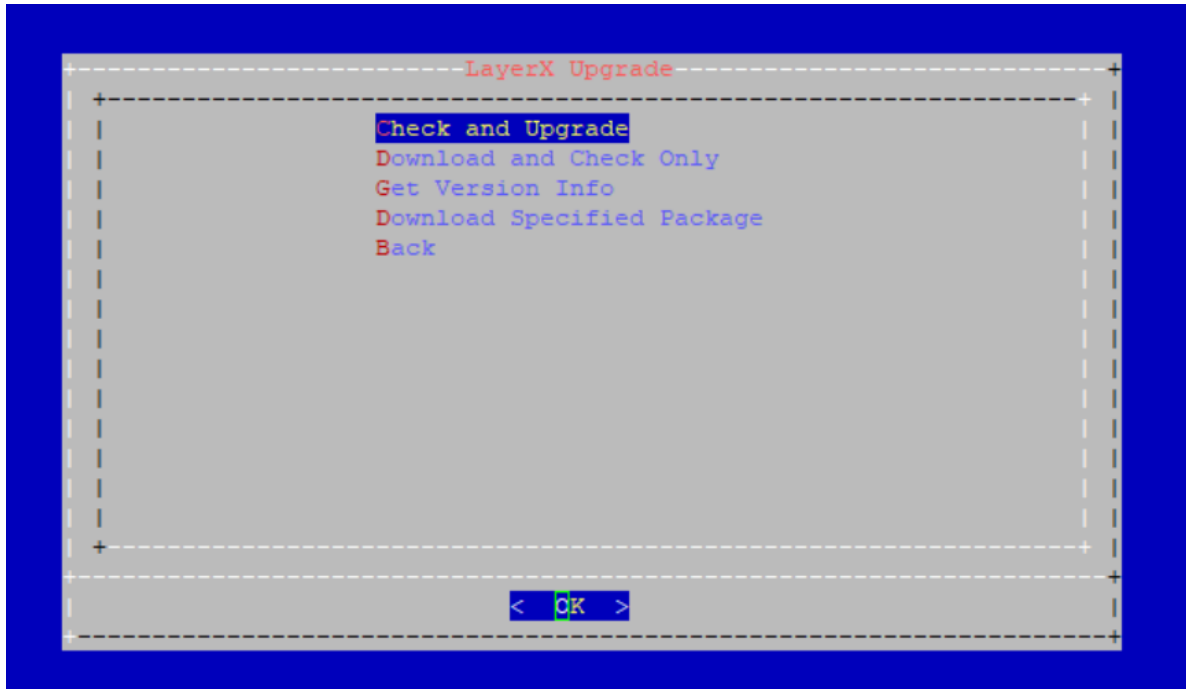


2.6. Patch Install Steps

1. Using *Winscp* and the drop account, copy the file (example file for the arbitrator insights-arbitrator-<from>-<to>.lisp) 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**:

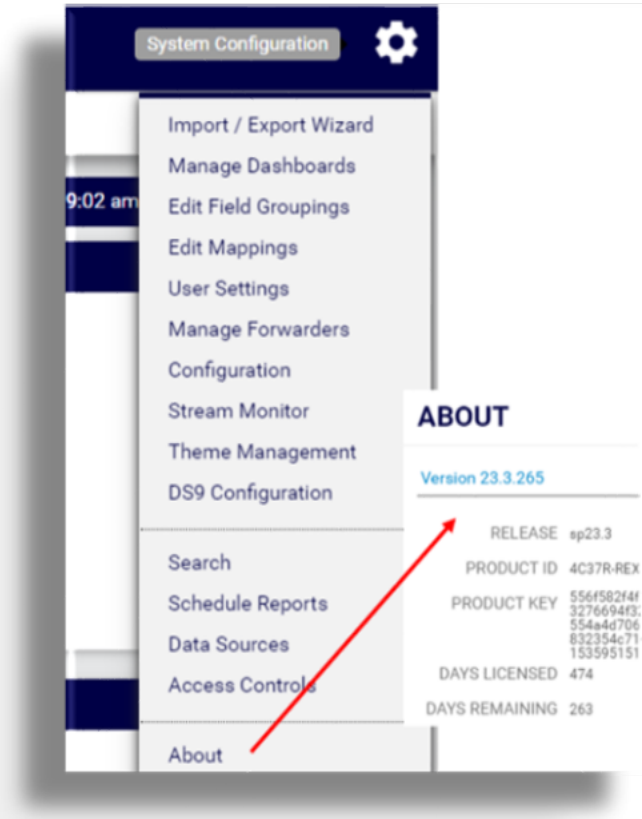


(Optional) Select **Perform Checksum** and enter the downloaded filename. This step will verify the downloaded file against its .sha256 file.

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.

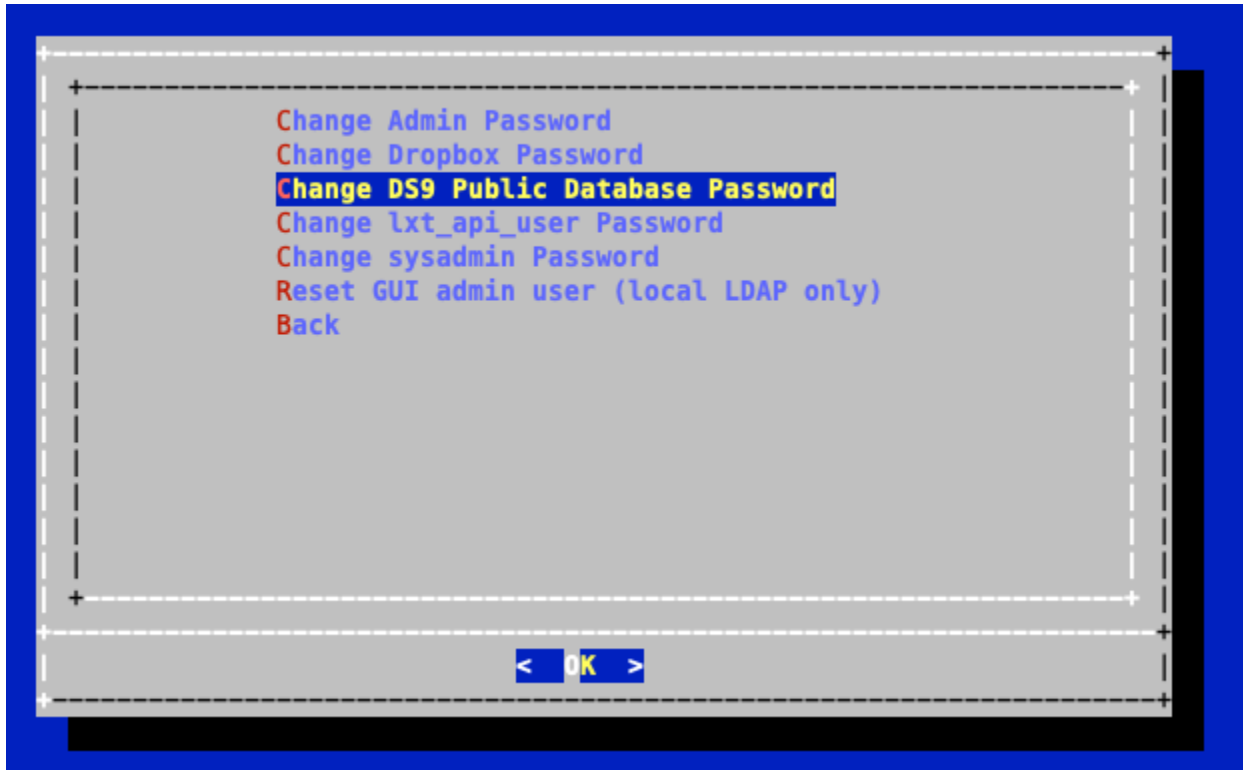
2.8. DS9 Database Password Management

DS9 is installed with a default, hidden password and Dashboard user `1xpublic`.

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

2.8.1. Maintain DS9 Database Password on DS9

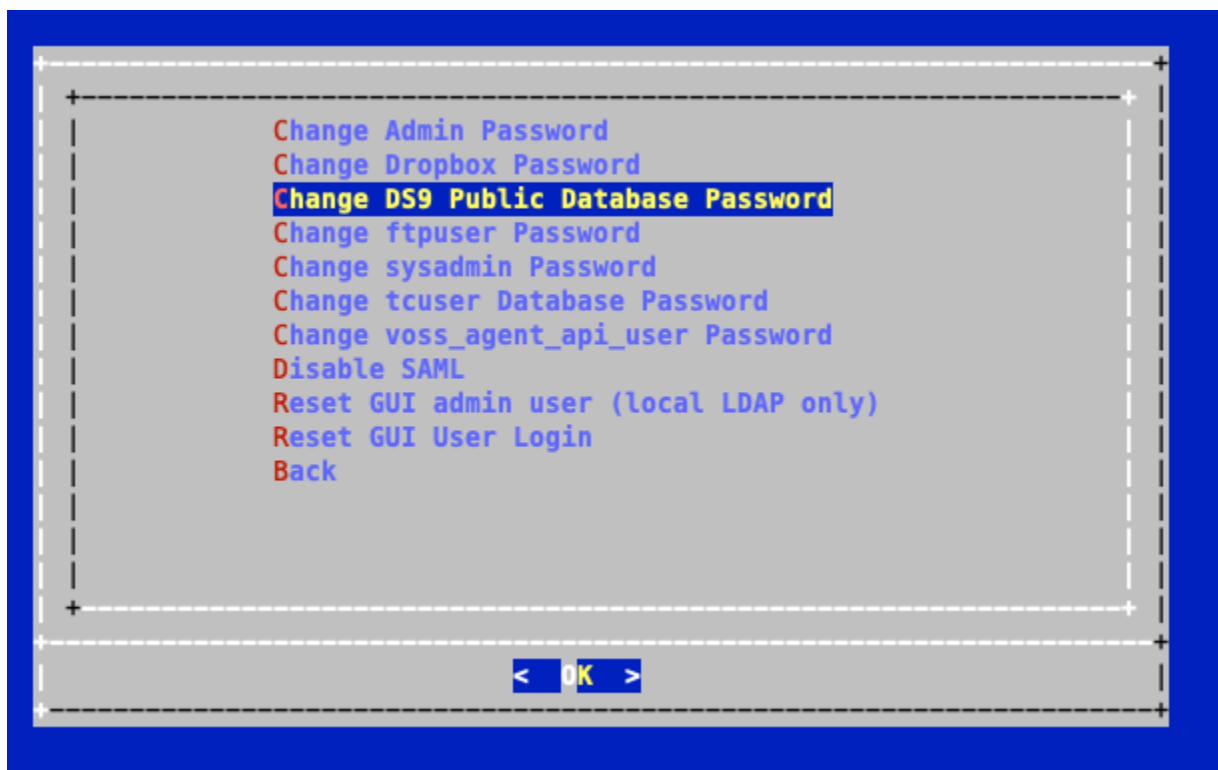
1. On the DS9 server, log in as `admin` from the console and from the **Administration** menu, select **Change Passwords**.
2. Select **Change DS9 Public Database Password** and modify the password. (Note: only alphanumeric characters are allowed)



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**.

<input type="checkbox"/> Name	Username	Password	Confirm	
<input type="checkbox"/> ccmadmin	*****	*****	*****	
<input type="checkbox"/> vossaxl	*****	*****	*****	
<input type="checkbox"/> admin	*****	*****	*****	
<input type="checkbox"/> insights-axl	*****	*****	*****	
<input type="checkbox"/> snmp	*****	*****	*****	
<input type="checkbox"/> voss	*****	*****	*****	
<input type="checkbox"/> 10.13.37.51_ds9_database_password	*****	*****	*****	

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 out 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.

Data Sources

DS9 SNMP Postgres Database - 10.13.3

New Data Source

Name

DS9 SNMP Postgres Database - 10.13.3

Data Source Type

DS9 SNMP Postgres Database

Host

10.13.37.52

Port

5432

Username

ixpublic

Password

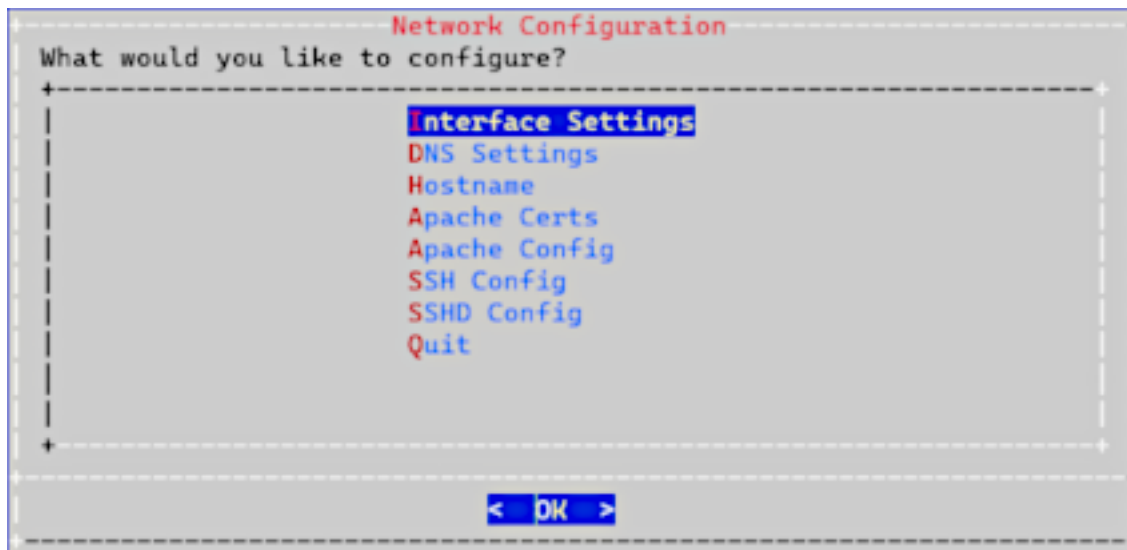
.....

Delete

Save

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--
```

```

Please Enter New CERTIFICATE
+-----BEGIN CERTIFICATE-----
MIIDaTCCA1GgAwIBAgIJAAND9HCYMJZp5MA0GCSqGSIb3DQEBCwUAMEsx CzAJBgNV
BAYTA1VTMQ4wDAYDVQQIDAVUZXhpczEPMA0GA1UEBwwGSXJ2aW5rMQ0wCwYDVQQK
DARWb3NzZkQwYmVzYXZlLnVzZS51LXh0b3R0LmVzZS51LXh0b3R0LmVzZS51LXh0
ODM2WjBlMQswCQYDVQGEwJVUzEOMAwGA1UECAwFVG4YXMcDzANBgNVBACMBkly
dm1uZzEENMAsGA1UECgwEVm9zczEOMAAoGA1UECwwDZGVZMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnPxELbSPykX+ZUKVgrQZ9YmeHn5Qe35yIxpPY5L
anV0zwQoFPHufh6S1LXhNbI68tV+Yva+NBpxbk8JHLpscTT5IDx47aU2xwHBM6Z6
1jcmekWT/1k/5W0W5cMqoQU0kiERjC/nwo6qbtUxDrTiAjlyCsaH1h9Jt7/GQueK
eM/a0THcRDP+VNzkGdhMgLTXYcLmxdkEs6Csryi+wJX4Q8EzN+ j7hHBDXSHao3g
RBGMIZ00Smc0g07GqAPxbdHgpJ+2YB4/MJqUGQ6D+MExZC68RPwkmo+5jHMF/+en
YrbGs2w5cg5Dz80v077VBrpL74lccrjLz6gie7afMAXJSwIDAQABo1AwTjAdBgNV
HQ4EFgQUCMvr/Dw0izcxofTed5isoBzvelWQhwYDVR0jBBgwFoAUCMvr/Dw0izcx
ofTed5isoBzvelWQDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEA/Tp
+-----+
v(+)
66%
< OK > <Cancel>

```

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--
```

```

Please Enter New PRIVATE KEY
+-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAwggSjAgEAAoIBAQGpeDK8U0szTE8
uqhGi5+y9dRytDVym9k9JvDQBxq/eqzsqv/nONJHeDb8+A5FFGILQmky8mE2YI5i
jx3qbx89Tc0R1HZGW1waX1X1Y4TzhBrLjcvsaKDP0jNnKdeRiF2i jxU8WGF7w2/F
8ToNp86EihvF8YamH9VvL tArI39wbzt8EDUqI fkdNHTGA2ZtIKwqhE9CwyyDjI8
fqUv4Ya1pITAg8hsI tMg5aJzdvCFtVnaHkKPLPV50HfFACINhWk+Gp9S+jsjL7
L2TsszHt6rIRcWR4oc58IUi pc0os56KHhnGRsKp0RPJnS0s+i fHDCYHmz+00sZCJ
t0P1xyo1AgMBAACggEAXS52cfwa7YcbL5eHVAAu2ydmA3IV48NjiYHmxxNuEqA
ld99duMKkI ftk2BwoSrci tbK/i7ENx039reXmt6hUspqBZEaIggq8+4n48nDKbshr
IUzUeUli3FmHzz6rZhmHi Te8CJulUrs+QYN01Ha63iyiVupZ/SPHp1w0+1L3Ca+Rh
c5NzKzET7ASe14ijfpYAP144Xd8HtSNbU6RQ+QFKuZJkXvVdLPPzd/xx0EVH0fWm
Q+V7eA88hu9rGEIed9HjHr2XHox+wrGu7a01H8/UT8aQrNEVXarWcjIOqdJIV/u5
ZBggQzR3oiSZyChzLmL5XcfkCiFTRYo0gcmHKPZhi gQKBgQDrqhz3BPKEuCyJd0TX
RVdpK4FYmYkLY0ld1+QxcKad/zvWfmg70GLtuqqXC09yGS7TyylyXyblLex/AdBR
+-----+
< OK > <Cancel>

```

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.

```
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.