VOSS Insights
Dashboard and Arbitrator Maintenance and Upgrade Guide

Release 24.1

May 29, 2024

Legal Information

-
- 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: 20240529151638

Contents

1. What's New

1.1. Dashboard and Arbitrator Maintenance and Upgrade Guide: Release 24.1

- EKB-18639: PostgreSQL v16 upgrade. See: *Upgrade*

  Added timing impacts of PgSQL version update.

2. Upgrade

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.

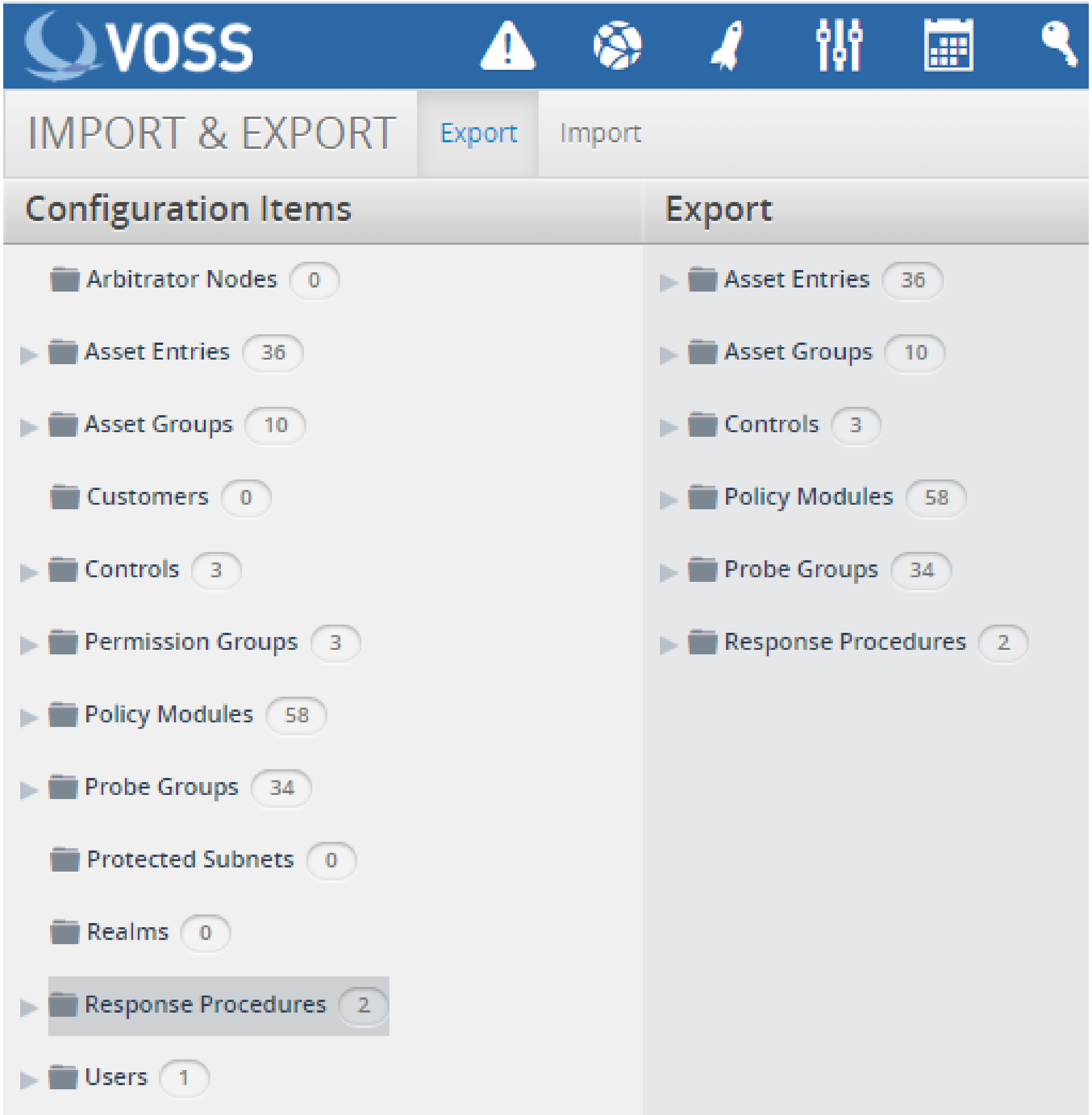
2.3. Backup Dashboards Before Upgrade

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.

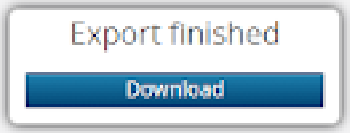
2.4. Backup Arbitrator Before Upgrade

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



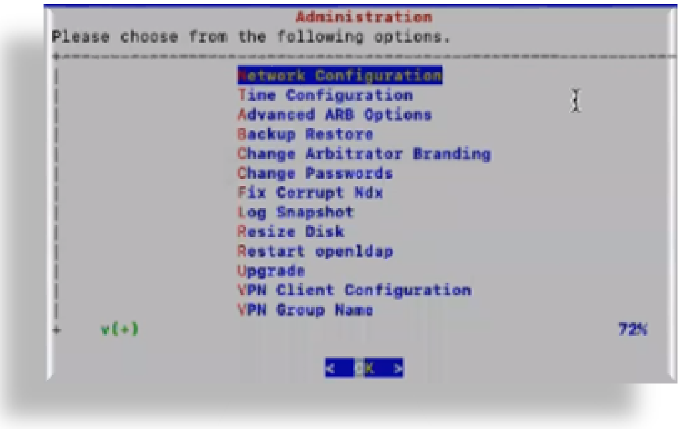
4. Click **Export**

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



2.4.1. Admin Menu Backup (Arbitrator or Dashboard)

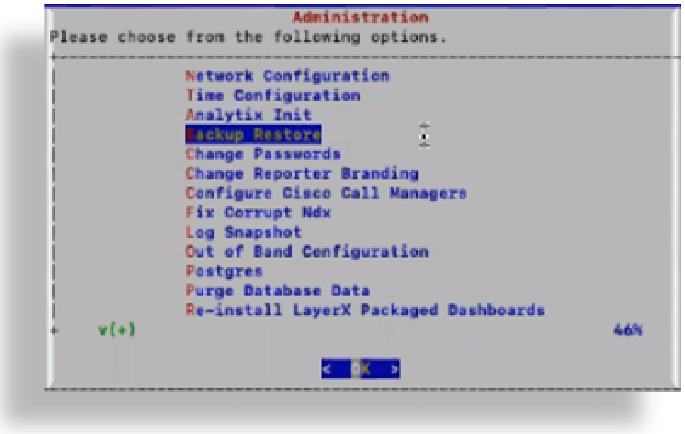
1. Log in to server using *Putty* via the admin account.
2. Go to the **Administration** menu (either Arbitrator or Dashboard):
   - Arbitrator



```
                          Administration
Please choose from the following options.
+-------------------------------------------------------------
|                      Network Configuration
|                      Time Configuration
|                      Advanced ARB Options
|                      Backup Restore
|                      Change Arbitrator Branding
|                      Change Passwords
|                      Fix Corrupt Ndx
|                      Log Snapshot
|                      Resize Disk
|                      Restart openldap
|                      Upgrade
|                      VPN Client Configuration
|                      VPN Group Name
+    v(+)                                                 72%

                           <  OK  >
```

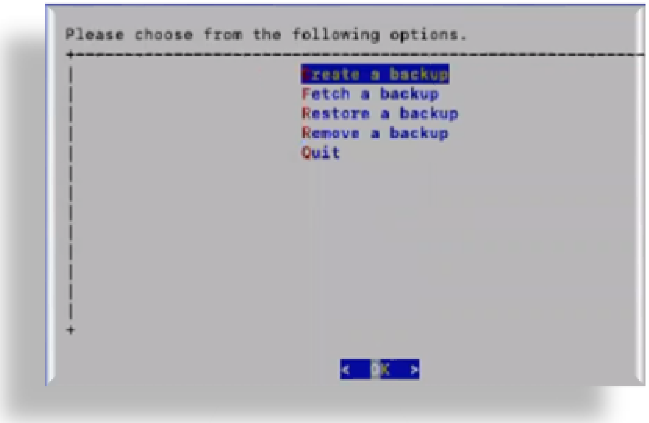
   - Dashboard



```
                          Administration
Please choose from the following options.
+-------------------------------------------------------------
|                 Network Configuration
|                 Time Configuration
|                 Analytix Init
|                 Backup Restore
|                 Change Passwords
|                 Change Reporter Branding
|                 Configure Cisco Call Managers
|                 Fix Corrupt Ndx
|                 Log Snapshot
|                 Out of Band Configuration
|                 Postgres
|                 Purge Database Data
|                 Re-install LayerX Packaged Dashboards
+    v(+)                                                 46%

                           <  OK  >
```

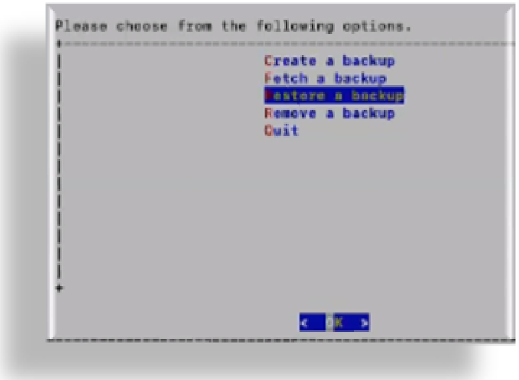
3. Select **Backup Restore**, and then choose **Create a backup**.



```
Please choose from the following options.
```

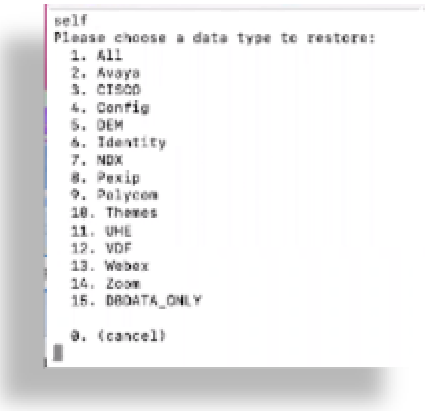
Note:

- 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.



```
Please choose from the following options.
```

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



```
self
Please choose a data type to restore:
  1. All
  2. Avaya
  3. CISCO
  4. Config
  5. DEM
  6. Identity
  7. NDX
  8. Pexip
  9. Polycom
  10. Themes
  11. UHE
  12. VDF
  13. Webex
  14. Zoom
  15. DBDATA_ONLY

  0. (cancel)
```

2.5. Upgrade

2.5.1. Upgrade Timings

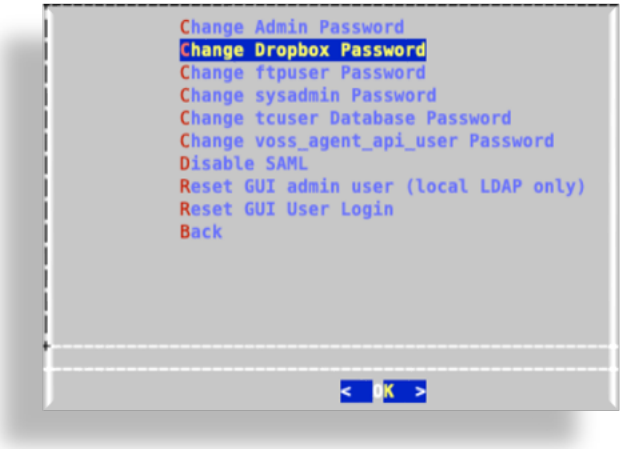
Note: Since various operating system components are updated during release 24.1, the total upgrade time is more than the averages for previous releases.

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

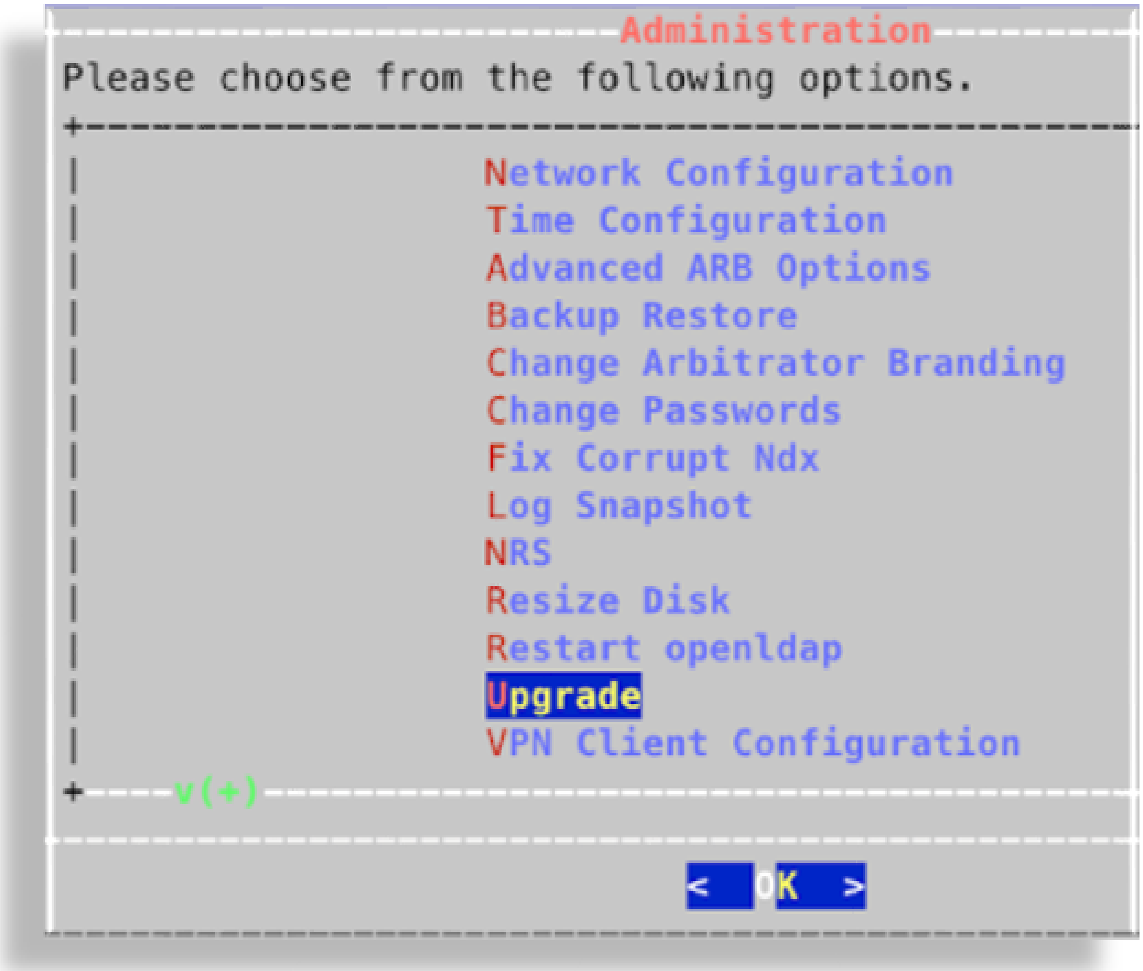
2.5.2. Upgrade Arbitrator or Dashboard

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.



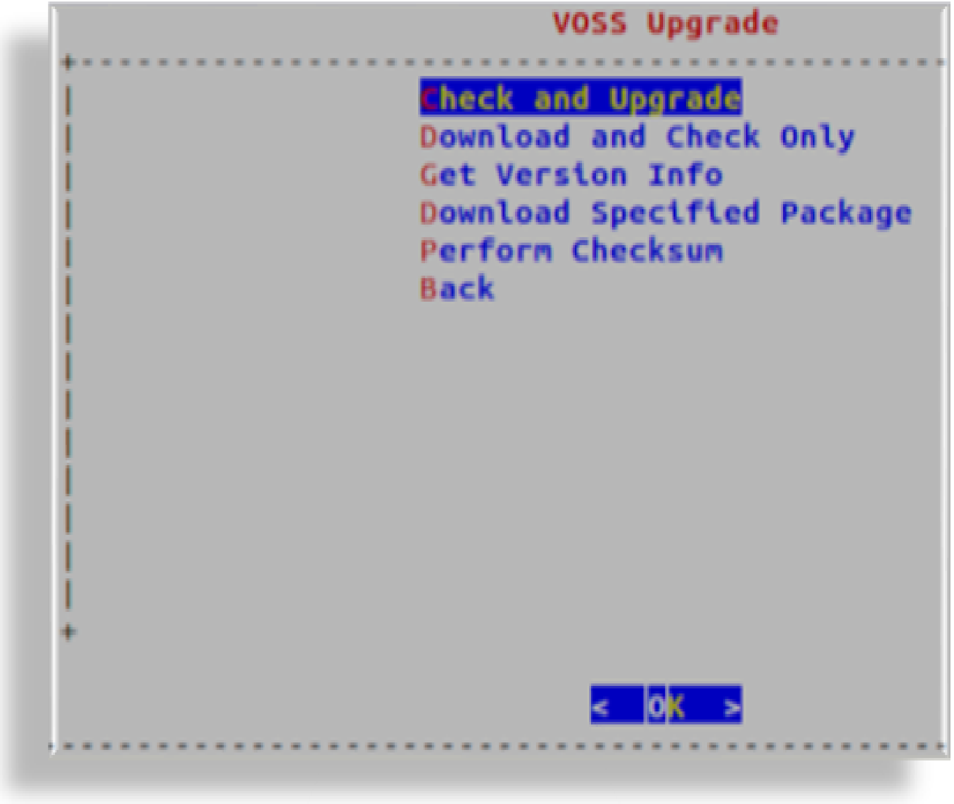
2. Log in to the server using *Putty* via the Admin account.
3. From the **Administration** menu, select **Upgrade**.



```
-----------------------------Administration--------
Please choose from the following options.
+-------------------------------------------------
|                  Network Configuration
|                  Time Configuration
|                  Advanced ARB Options
|                  Backup Restore
|                  Change Arbitrator Branding
|                  Change Passwords
|                  Fix Corrupt Ndx
|                  Log Snapshot
|                  NRS
|                  Resize Disk
|                  Restart openldap
|                  Upgrade
|                  VPN Client Configuration
+----v(+)-----------------------------------------

---------------------------------------------------
                             <  OK  >
---------------------------------------------------
```

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



2.5.3. Upgrade DS9

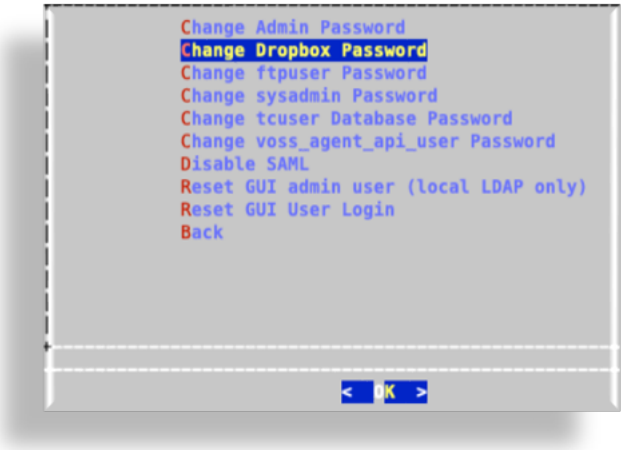
This procedure upgrades DS9.

Pre-requisites:

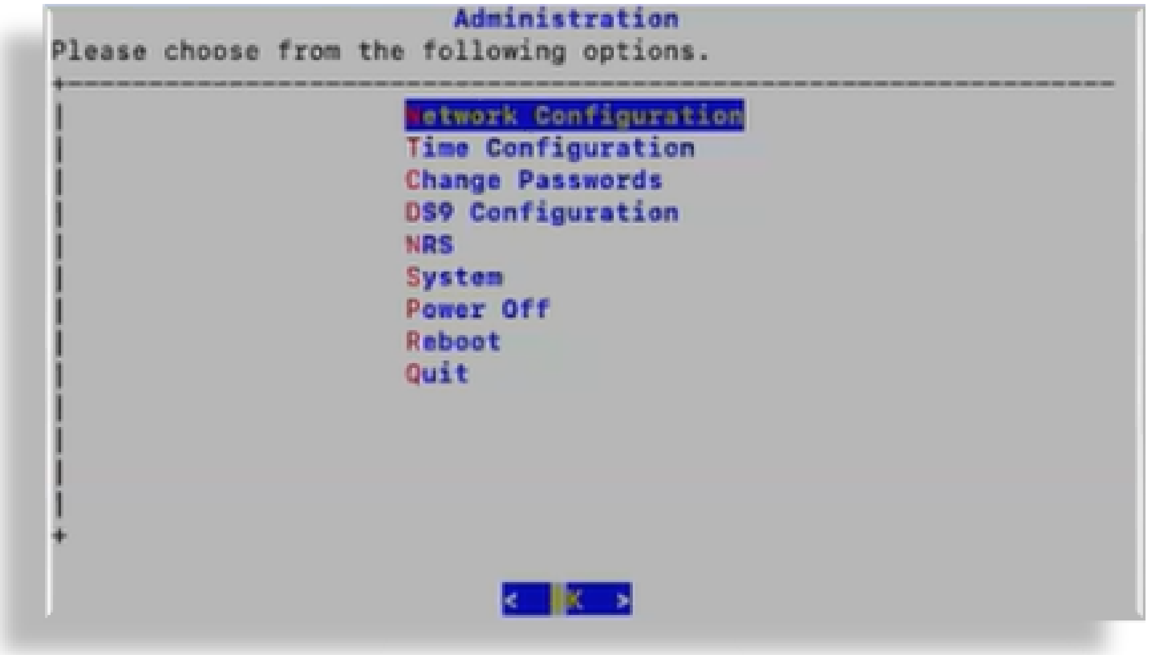
- Using *Winscp* and the drop account, copy the `*.lxsp` file to be used for the upgrade into the drop account's *lxt_upgrade* sub-directory.

  Note:

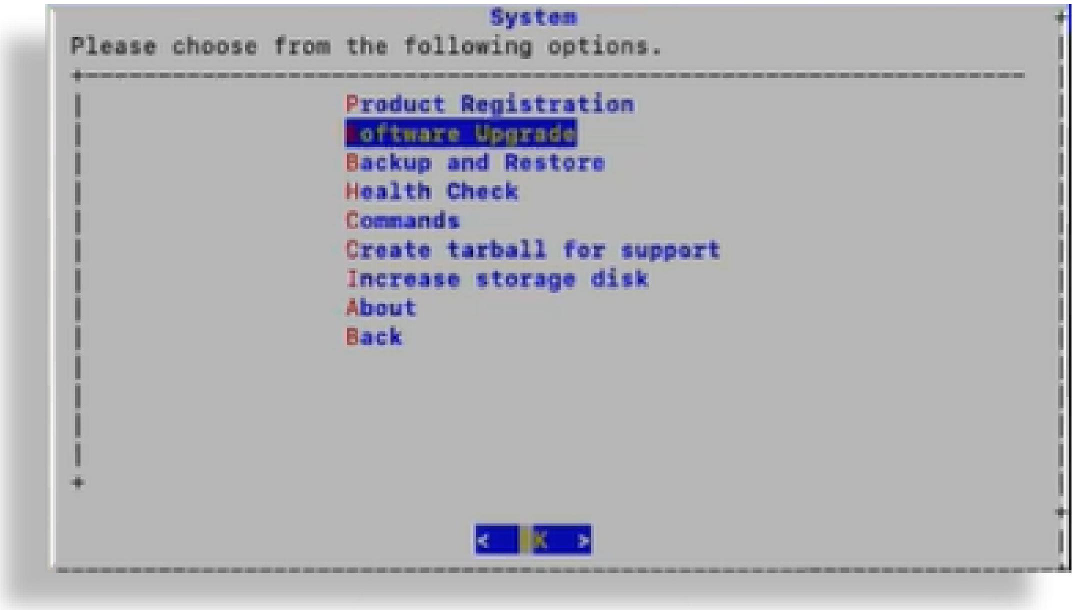
  - The naming convention for Insights upgrade files means that the system is able to detect the file to use for the upgrade. For Insights products, `*.lxsp` file is copied into the drop account's *lxt_upgrade* sub-directory, and the system fetches the file from that location.
  - The drop account username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



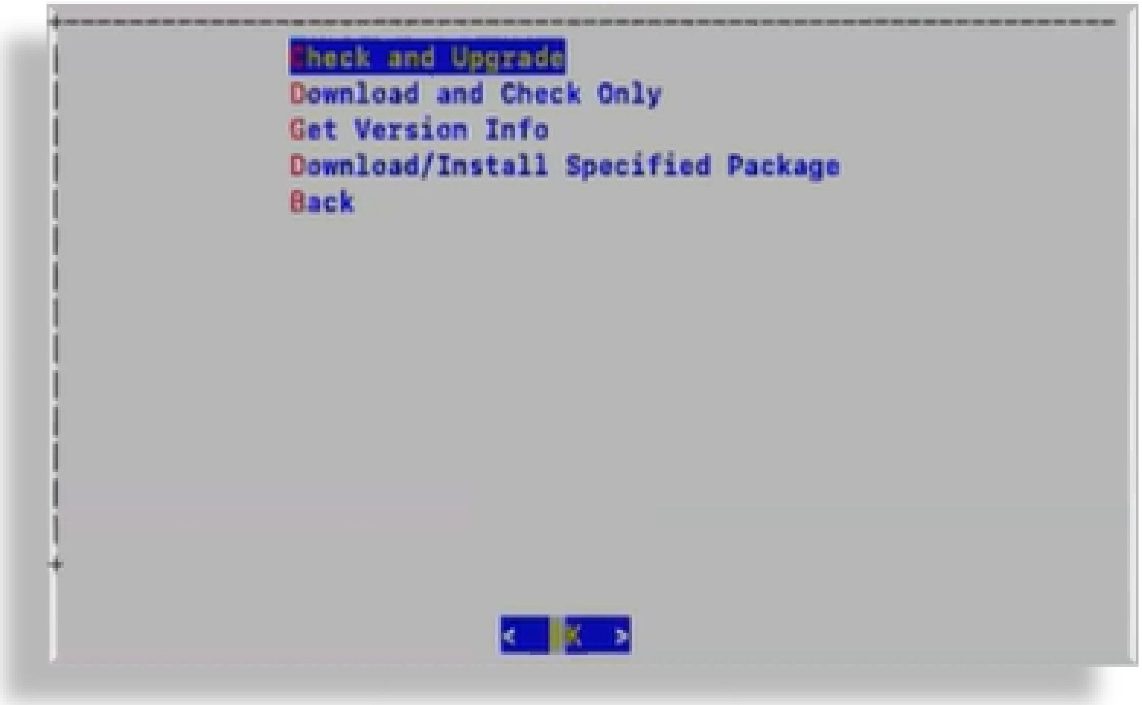
2. Select **System > Software Upgrade**.



System

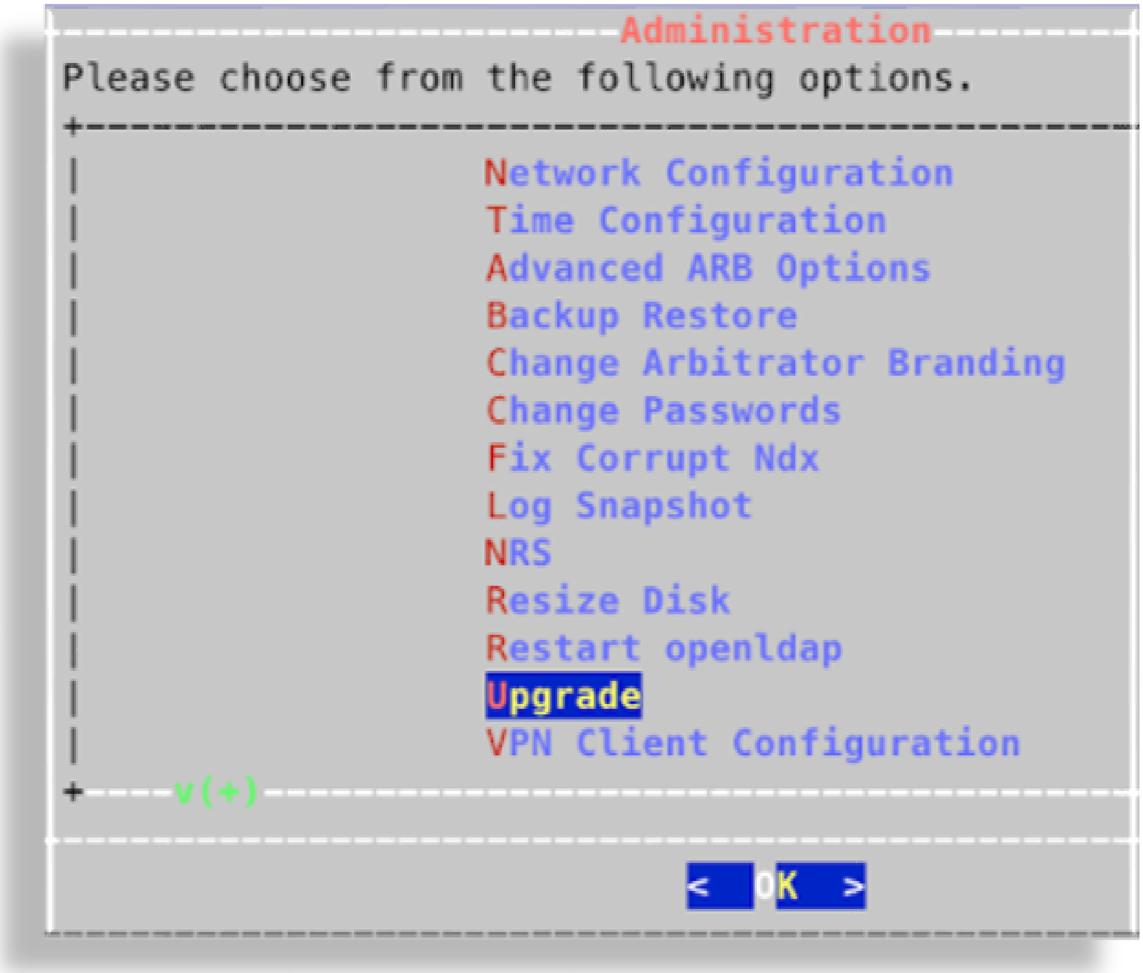
Please choose from the following options.

3. Select **Check and Upgrade**.



2.6. Patch Install Steps

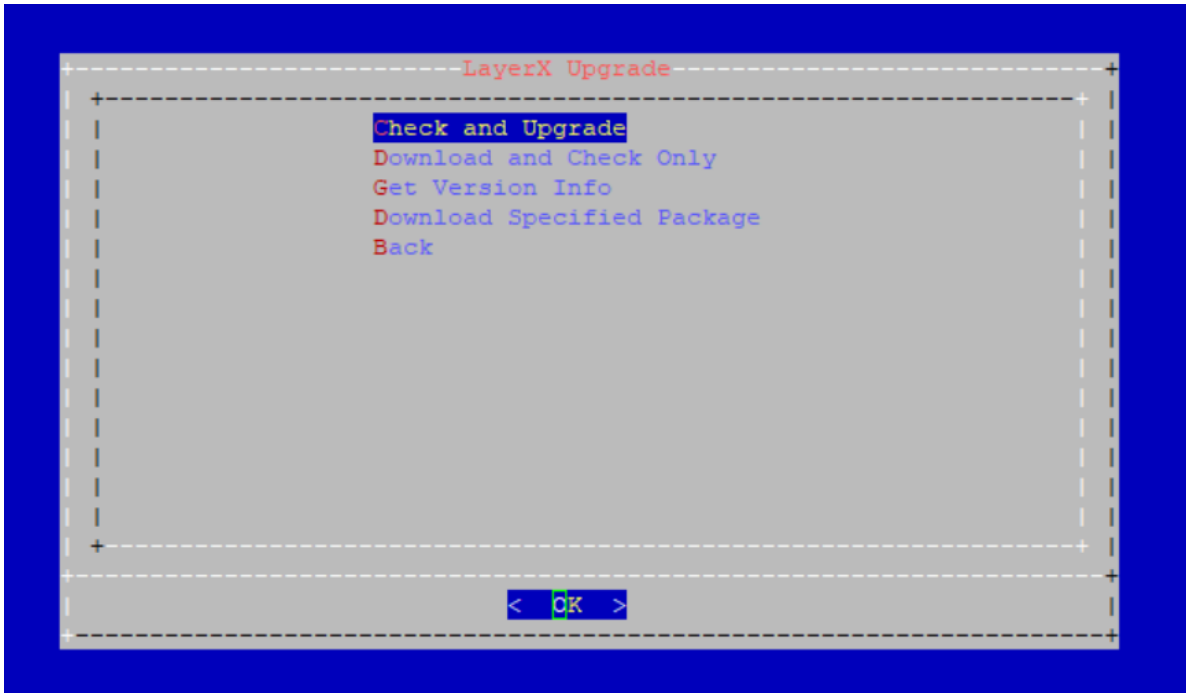
1. Using *Winscp* and the drop account, copy the file (example file for the arbitrator `insights-arbitrator-<from>-<to>.lxsp`) to the `lxt_upgrade` directory.
2. Log on to the server using *Putty* and the admin user credentials
3. From the **Administration** menu, select **Upgrade**



Please choose from the following options.

4. Select **Check and Upgrade**:

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

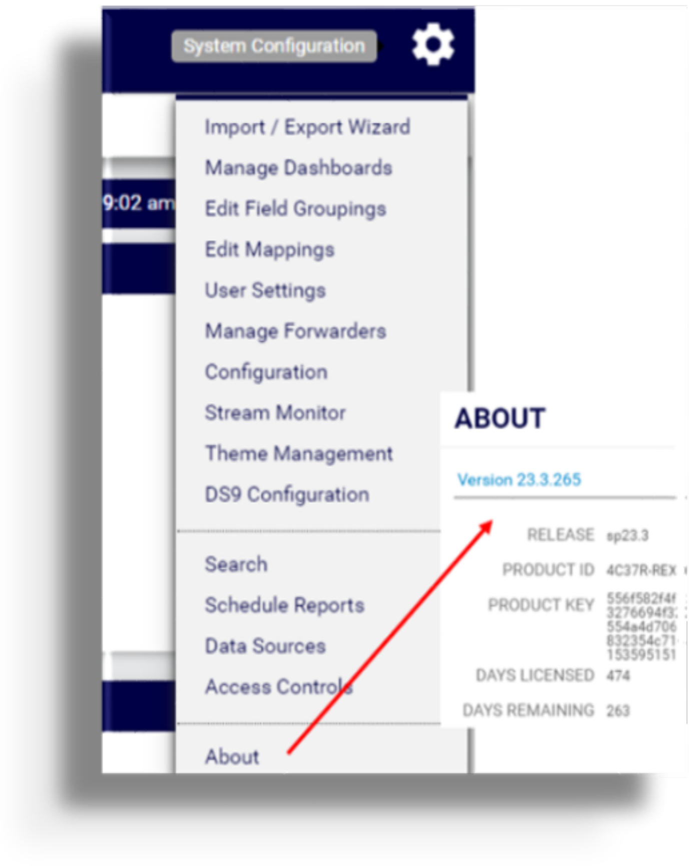


(Optional) Select **Perform Checksum** and enter the downloaded filename. This step will verify the downloaded file against its `.sha256` file.

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**.



ABOUT

Version 23.3.265

RELEASE sp23.3

PRODUCT ID 4C37R-REX

PRODUCT KEY 556f582f4f
3276694f3
554a4d706
832354c71
153595151

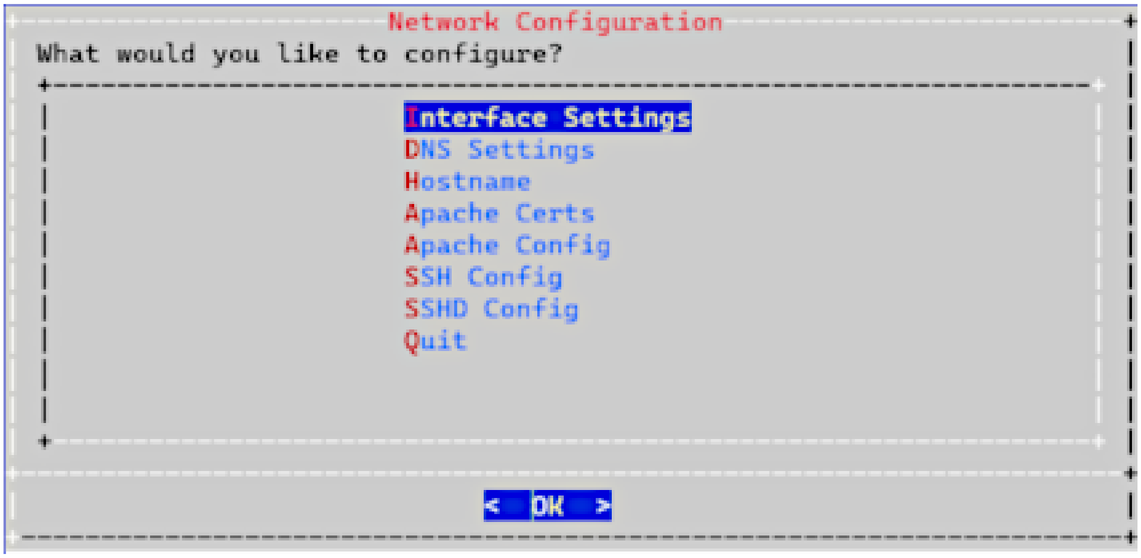
DAYS LICENSED 474

DAYS REMAINING 263

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

3. 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?

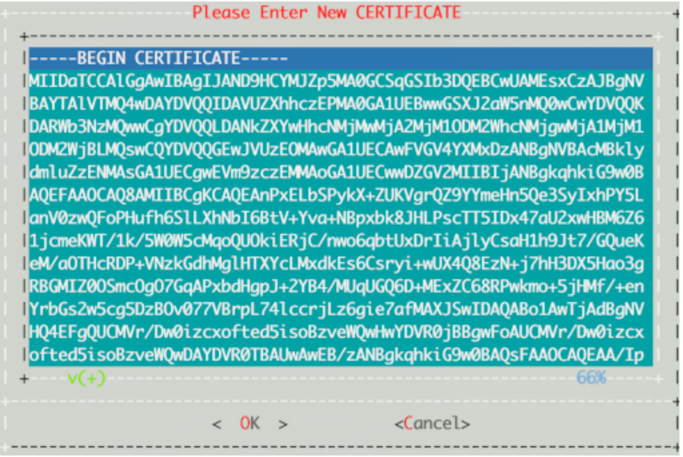
3.1. Add Certificates

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--
```

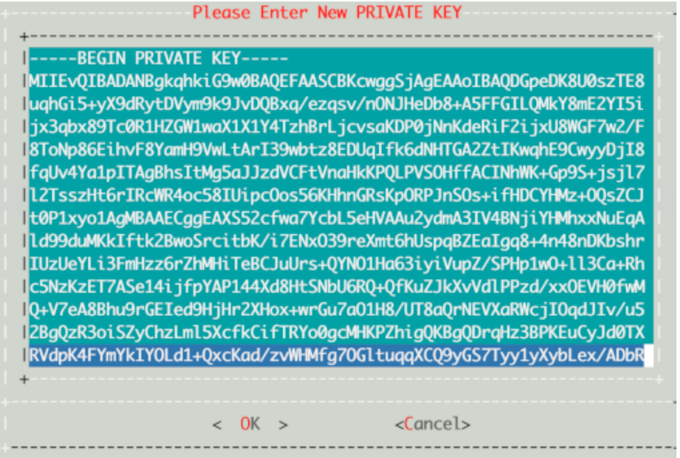


```
-----BEGIN CERTIFICATE-----
MIIDaTCCAlGgAwIBAgIJAND9HCYMJZp5MA0GCSqGSIb3DQEBCwUAMEsxCzAJBgNV
BAYTAlVTMQ4wDAYDVQQIDAVUZXhhczEPMA0GA1UEBwwGSXJ2aW5nMQ0wCwYDVQQK
DARWb3NzMQwwCgYDVQQLDANkZXYwHhcNMjMwMjA2MjM1ODM2WhcNMjgwMjA1MjM1
ODM2WjBLMQswCQYDVQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDzANBgNVBAcMBkly
dmluZzENMAsGA1UECgwEVm9zczEMMAoGA1UECwwDZGV2MIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAnPxELbSPykX+ZUKVgrQZ9YYmeHn5Qe3SyIxhPY5L
anV0zwQFoPHufh6SlLXhNbI6BtV+Yva+NBpxbk8JHLPscTT5IDx47aU2xwHBM6Z6
1jcmeKWT/1k/5W0W5cMqoQUOkiERjC/nwo6qbtUxDrIiAjlyCsaH1h9Jt7/GQueK
eM/aOTHcRDP+VNzkGdhMglHTXYcLMxdkEs6Csryi+wUX4Q8EzN+j7hH3DX5Hao3g
RBGMIZ00SmcOgO7GqAPxbdHgpJ+2YB4/MUqUGQ6D+MExZC68RPwkmo+5jHMf/+en
YrbGs2w5cg5DzBOv077VBrpL74lccrjLz6gie7afMAXJSwIDAQABo1AwTjAdBgNV
HQ4EFgQUCMVr/Dw0izcxofted5isoBzveWQwHwYDVR0jBBgwFoAUCMVr/Dw0izcx
ofted5isoBzveWQwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAA/Ip
```

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--
```



```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDGpeDK8U0szTE8
uqhGi5+yX9dRytDVym9k9JvDQBxq/ezqsv/nONJHeDb8+A5FFGILQMkY8mE2YI5i
jx3qbx89Tc0R1HZGW1waX1X1Y4TzhBrLjcvsaKDP0jNnKdeRiF2ijxU8WGF7w2/F
8ToNp86EihvF8YamH9VwLtArI39wbtz8EDUqIfk6dNHTGA2ZtIKwqhE9CwyyDjI8
fqUv4Ya1pITAgBhsItMg5aJJzdVCFtVnaHkKPQLPVSOHffACINhWK+Gp9S+jsjl7
l2TsszHt6rIRcWR4oc58IUipcOos56KHhnGRsKpORPJnSOs+ifHDCYHMz+OQsZCJ
t0P1xyo1AgMBAAECggEAXS52cfwa7YcbL5eHVAAu2ydmA3IV4BNjiYHMhxxNuEqA
ld99duMKkIftk2BwoSrcitbK/i7ENxO39reXmt6hUspqBZEaIgq8+4n48nDKbshr
IUzUeYLi3FmHzz6rZhMHiTeBCJuUrs+QYNO1Ha63iyiVupZ/SPHp1wO+ll3Ca+Rh
c5NzKzET7ASe14ijfpYAP144Xd8HtSNbU6RQ+QfKuZJkXvVdlPPzd/xxOEVH0fwM
Q+V7eA8Bhu9rGEIed9HjHr2XHox+wrGu7aO1H8/UT8aQrNEVXaRWcjIOqdJIv/u5
2BgQzR3oiSZyChzLml5XcfkCifTRYo0gcMHKPZhigQKBgQDrqHz3BPKEuCyJd0TX
RVdpK4FYmYkIYOLd1+QxcKad/zvWHMfg7OGltuqqXCQ9yGS7Tyy1yXybLex/ADbR
```

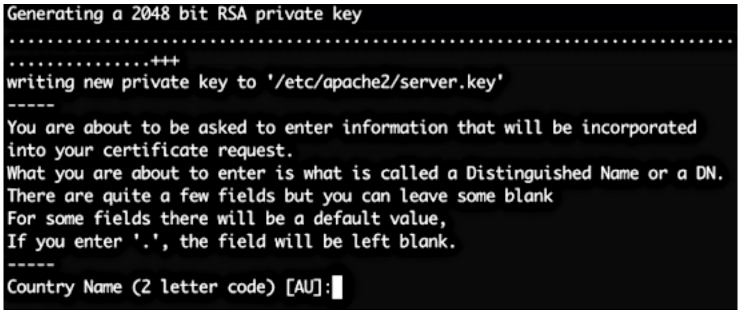
8. Select **Display Cert Details** to view certificate details.
9. Select **Back** and exit the menu.
10. Refresh the browser. The system should be using the new certificate.

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.