VOSS Automate
Upgrade Guide with Delta Bundle

Release 21.4

Nov 29, 2023

Legal Information

DOCUMENT ID: 20231129162534

Contents

1. What's New

1.1. Upgrade Guide with Delta Bundle: Release 21.4

- VOSS-872: License Enforcement. See: *Unified Node Topology: Upgrade a Multinode Environment with the Delta Bundle*

  Added details on license requirements.

- VOSS-872: License Enforcement. See: *Modular Cluster Topology: Upgrade a Multinode Environment with the Delta Bundle*

  Added details on license requirements.

- VOSS-872: License Enforcement. See: *Upgrade a Single Node Cluster Environment with the Delta Bundle*

  Added details on license requirements.

1.2. Upgrade Guide with Delta Bundle: Release 21.4-PB1

- N/A

1.3. Upgrade Guide with Delta Bundle: Release 21.4-PB2

- N/A

1.4. Upgrade Guide with Delta Bundle: Release 21.4-PB3

- N/A

1.5. Upgrade Guide with Delta Bundle: Release 21.4-PB4

- N/A

2. Introduction

Before starting with this upgrade, please read the following notes related to upgrades from earlier versions of the software.

Normal operations will be interrupted during an upgrade. Perform the upgrade in a maintenance window. Refer to the type of upgrade for details on the upgrade duration.

Upgrades to v21.4-PB1 and v21.4-PB2 - Web Portal Default Settings

VOSS Automate offers two graphical interfaces, or web portals - `admin` and `classic`.

Your system administrator defines, via the following command, the web portal that will be the default for your system: `web portal default set <admin|classic>`

Typically, the `admin` web portal is set as default, and the `classic` web portal is disabled (only `classic` can be disabled).

These settings should be preserved post-upgrade.

However, an issue was reported for upgrades from v21.4 to v21.4-PB1, where the web portal settings were not preserved post-upgrade. In this case, you would need to re-run the following commands to set `admin` as default, and to disable `classic`:

- `web portal default set admin`
- `web portal disable classic`

This issue was fixed for upgrades to v21.4-PB2, which means that the web portal settings you have in earlier versions are preserved when upgrading to 21.4-PB2.

For more information around these settings, see:

- *Web Portal Configuration* in the Platform Guide

Release 21.4 onwards - Product License Changes

From release 21.4 onwards, VOSS Automate allows for the registration and update of product licenses within the application. A licensing service is installed during installation or upgrade and a license token is associated with the platform on which it is installed.

Upgrades to a v2x.x Release from a v18.x or v19.x release - Impact of new *Usage* field added to Directory Numbers

From release 21.1 onwards, a new field called **Usage** has been added to Directory Numbers (DN).

This field tracks the type of device that the DN has been assigned to. For example, for Phones, Device Profiles, and Remote Destination Profiles, the usage is “Device”. For Hunt Groups, the usage is “Hunt_Pilot”, and so on.

The **Usage** field is automatically populated when the DNs are assigned to and removed from various devices from 21.1 onwards.

In order to populate the **Usage** field once-off for all existing Directory Number inventory instances, the Audit Number Inventory tool (`view/NumberInventoryAudit`) should be run once post-upgrade for each customer.

The tool only needs to be run once when initially upgrading to a 2x.x release from a 18.x or 19.x release.

If you ran the tool already when upgrading to 21.1 for example, then it does not need to be run again when upgrading to later versions, for example 21.2, 21.3, 22.1, and so on.

Before running the tool:

- Careful consideration must taken when selecting where the Number Inventory is deployed: Customer or Site - this is usually Dial Plan dependent.
- Review the Audit Number Inventory topic in the Core Feature Guide.

3. Upgrade Planning

3.1. Using the `screen` command

The **screen** command is available to execute long-running commands (for example, when upgrading) in the background.

The following commands require the running of **screen**:

- **cluster provision**
- **cluster upgrade**
- **app template**
- **voss export type <args>**
- **voss export group <args>**
- **voss subscriber_data_export**

A message is displayed to indicate that **screen** should be run first:

```
This is a potentially long-running command and should be executed in a screen session
Run `screen` and then execute the command again
```

The use of **screen** is *not affected* by the use of the `--force` parameter with any of these commands.

The commands then run in a screen session that can be reconnected. The standard screen command parameters are available, in particular:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

The version of **screen** used in VOSS Automate also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:

a. In screen command mode, type **logfile media/<screen-logfilename>.log**
b. Press **<Enter>**
c. Press **<Ctrl>-a** and then **H** to start writing to the log file
d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

$ sftp platform@<host>:media/<screen-logfilename>.log

4. Multinode Upgrade

4.1. Unified Node Topology: Upgrade a Multinode Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.

The standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

We recommend using the **screen** command to avoid failures if the connection is interrupted whilst running the command. If the connection is interrupted whilst running the command in `screen` then the session can be retrieved by first listing the sessions PID currently running in screen: **screen -ls**, and then reconnecting to the session using **screen -r [screen PID]**.

The version of **screen** used in VOSS Automate also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:

    a. In screen command mode, type **logfile media/<screen-logfilename>.log**

    b. Press **<Enter>**

    c. Press **<Ctrl>-a** and then **H** to start writing to the log file

    d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

$ sftp platform@<host>:media/<screen-logfilename>.log

4.1.1. Download Files and Check

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `XXX-Delta-Bundle.script` file, where XXX matches the release. Transfer the `XXX-Delta-Bundle.script` file to the `media/` folder *of the primary Unified node*. Two file transfer options: Either using SFTP: • **sftp platform@<primary_unified_node_hostname>** • **cd media** • **put <XXX-Delta-Bundle.script>** Or using SCP: • **scp <XXX-Delta-Bundle.script> platform@<primary_unified_node_hostname>** On the primary Unified node, verify that the `.script` file copied: • **ls -l media/** On the primary Unified node, verify that the original `.sha256` checksums on the SFTP server match. • **system checksum media/<XXX-Delta-Bundle.script>** `Checksum:  <SHA256>`	

4.1.2. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	

4.1.3. Schedules, Transactions and Version Check

Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. Schedules enabled on the CLI: 1. Run **schedule list** to check if any schedules exist and overlap with the maintenance window. 2. For overlapping schedules, disable. Run **schedule disable <job-name>**.	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as “Processing” and then choose each **Action** that starts with “Import”, for example, “Import Unity Connection”. b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	
Customized ``data/Settings`` If `data/Settings` instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: *Post Template Upgrade Tasks*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

4.1.4. Pre-Upgrade, Security and Health Steps

<table>
<tr><th>Description and Steps</th><th>Notes and Status</th></tr>
<tr><td>Verify that the primary node is the active primary node at the time of upgrade.
<b>database config</b>
Ensure that the node on which the installation will be initiated has the <code>stateStr</code> parameter set to <b>PRIMARY</b> and has the <b>highest</b> <code>priority</code> <b>number</b> (highest priority number could vary depending on cluster layout).
Example output
<pre>
<ip address>:27020:
  priority: <number>
  stateStr: PRIMARY
  storageEngine: WiredTiger
</pre>
Validate the system health.
On the Primary Unified Node, verify cluster connectivity:
<ul><li><b>cluster status</b></li></ul>
On each node verify network connectivity, disk status and NTP.
<ul><li><b>cluster check</b></li></ul>
If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
<pre>
/   (call support if over 80%)
/var/log   (run: log purge)
/opt/platform   (remove any unnecessary files from /media directory)
/tmp   (reboot)
</pre>
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes:
<ul><li><b>cluster run all security check</b></li></ul>
</td><td></td></tr>
<tr><td>As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.
VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.
Optional: If a backup is also required, use the <b>backup add <location-name&gt;</b> and <b>backup create <location-name&gt;</b> commands. For details, refer to the Platform Guide.</td><td></td></tr>
</table>

Description and Steps	Notes and Status

Before upgrading, check all services, nodes and weights for the cluster:
Make sure no services are stopped/broken. The message ‘suspended waiting for mongo’ is normal on the fresh unified nodes.
• **cluster run all app status**
Make sure all application nodes show 4 or 6 nodes.
• **cluster run application cluster list**
Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
• **cluster run application database weight list**
Example output:
`172.29.21.240:`
`    weight: 80`
`172.29.21.241:`
`    weight: 70`
`172.29.21.243:`
`    weight: 60`
`172.29.21.244:`
`    weight: 50`
Verify the primary node in the primary site and ensure no nodes are in the ‘recovering’ state (`stateStr` is not `RECOVERING`). On the primary node:
• **database config**	

4.1.5. Upgrade

Description and Steps	Notes and Status
On the primary unified node: • **screen** Run (optionally with command parameters below): `app install media/<script_file> delete-on-success yes --force` The upgrade will also silently run an updated version of **cluster check** and the upgrade will fail to proceed if any error conditions exist. Fix before proceeding. Refer to the Platform Guide for details on the new version of the **cluster check** command. Run: • **database config** and verify the number of nodes are *uneven*, i.e. either 5 or 7. If not, run: **cluster provision role database** and ensure an arbitrator shows when you run **database config** again (`stateStr: ARBITER`). From release 19.1.2 and later, the `delete-on-success` parameter and `yes` or `no` value have been added to remove or keep the the script file in the `media/` directory after successful installation. Note that during the upgrade, phone registration data is cleared. A message will show in the log: `Remove phone registration data`. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.	

4.1.6. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
On the primary unified node, verify the cluster status: • **cluster status** • **cluster check** • If any of the above commands show errors, check for further details to assist with troubleshooting: **cluster run all diag health**	
If upgrade is successful, the screen session can be closed by typing **exit** in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.	
Check for needed security updates. On the primary node, run: • **cluster run all security check** If one or more updates are required for any node, run on the primary Unified node: • **cluster run all security update** Note: *if the system reboots, do not carry out the next manual reboot step*. Manual reboot *only if needed*: • **cluster run notme system reboot** If node messages: `<node name> failed with timeout` are displayed, these can be ignored. • **system reboot** Since all services will be stopped, this takes some time.	

4.1.7. Post Template Upgrade Tasks

Description and Steps	Notes and Status
Restart the system from the command line if no reboot took place during the Post-Upgrade, Security and Health Steps. On the primary unified node, run: **cluster run notme system reboot** and then **system reboot**	
Import ``device/cucm/PhoneType`` In order for a security profile to be available for a Call Manager Analog Phone, the `device/cucm/PhoneType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/PhoneType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **SSO Login URL check if needed** Verify the SSO Login URL if needed. Go to **Single Sign On > SSO Identity Provider** and ensure your URL matches the **SSO Login URL** value. **Customized ``data/Settings``** Merge the previously backed up customized `data/Settings` with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON. **Support for VG400 and VG450 Analogue Gateways** Before adding the VG400 or VG450 Gateway, the `device/cucm/GatewayType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/GatewayType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **Verify the upgrade** Log in on the GUI and check the information contained in the **About > Extended Version** menu. Confirm that versions have upgraded: • **Release** should show `XXX` • **Platform Version** should show `XXX` where `XXX` corresponds with the release number of the upgrade. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again. Verify that the web portal is configured to the required setting, either admin or classic. For further details on this setting, see *Web Portal Configuration* in the Platform Guide.	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.1.8. Restore Adaptations

Description and Steps	Notes and Status
Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.	

4.1.9. Restore Schedules

Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. **Note:** Select the **Skip next execution** if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. Schedules enabled on the CLI: 1. For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

For overlapping schedules, disable. Run **schedule disable <job-name>**.

4.1.10. Release Specific Updates

Description and Steps	Notes and Status
When upgrading to release 21.3, users of Microsoft apps should after upgrade, select each Microsoft Tenant (`relation/MicrosoftTenant`) in the Admin GUI and click **Save** on it without making any changes. This step is required so that VOSS Automate can communicate with the Tenant post upgrade.	
Only if the following step was not carried out when upgrading to Release 21.3-PB1: On the primary node, run: `voss migrate_summary_attributes data/InternalNumberInventory`	

4.1.11. Log Files and Error Checks

Description and Steps	Notes and Status

Inspect the output of the command line interface for upgrade errors.
Use the **log view** command to view any log files indicated in the error messages, for example, run the command if the following message appears:
`For more information refer to the execution log file with`
`'log view platform/execute.log'`
For example, if it is required send all the install log files in the `install` directory to an SFTP server:
• **log send sftp://x.x.x.x install**	

Log in on the GUI as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.1.12. Licensing after Delta Bundle Upgrade

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary unified node CLI. 1. Obtain the required license token from VOSS. 2. Steps for GUI and CLI: a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

4.2. Modular Cluster Topology: Upgrade a Multinode Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.

The standard **screen** command should be used where indicated. See: *Using the screen command*.

4.2.1. Determine the Primary database and application node in a Modular Cluster Topology

Important: All upgrade steps are to be run from the *primary application node*. Where it is necessary to run database node commands from this application node, the primary database node IP will be passed in as a parameter with the command.

In order to run the commands for the upgrade on the nodes with the appropriate roles, determine:

- The *primary application node*
- The *primary database node*

1. Log in on a node in your modular cluster.
2. To find the *primary application node* in the cluster:

   ```
   $ cluster run all cluster primary role application
   ```

   Record the node entry where `is_primary: true`, for example:

   ```
   ---------- VOSS-UN-1, ip=192.168.100.3, role=webproxy,application, loc=cpt

       is_primary: true
   ```

3. To find the *primary database node* in the cluster:

   ```
   $ cluster run all cluster primary role database
   ```

   Record the node entry IP where `is_primary: true`, for example:

   ```
   ---------- VOSS-UN-2, ip=192.168.100.4, role=database, loc=cpt


       is_primary: true
   ```

   This IP address will be used in command parameters during upgrade.

Note: When the **cluster run all primary role <role>** command is run, web proxy nodes will return a failure - this can be ignored. For example:

```
---------- VOSS-WP-1, ip=192.168.100.9, role=webproxy, loc=cpt
Invalid command syntax - refer to help descriptions
```

4.2.2. Download Files and Check

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `XXX-Delta-Bundle.script` file, where `XXX` matches the release. Transfer the `XXX-Delta-Bundle.script` file to the `media/` folder *of the primary application node*. Two file transfer options: Either using SFTP: • **sftp platform@<primary_application_hostname>** • **cd media** • **put <XXX-Delta-Bundle.script>** Or using SCP: • **scp <XXX-Delta-Bundle.script> platform@<primary_application_hostname>:~** On the primary application node, verify that the `.script` file copied: • **ls -l media/** On the primary application node, verify that the original `.sha256` checksums on the Download site match. • **system checksum media/<XXX-Delta-Bundle.script>** `Checksum:  <SHA256>`	

4.2.3. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	

4.2.4. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. Schedules enabled on the CLI: on the primary application node: 1. Check if any schedules exist. Run: **cluster run all schedule list** Record the IP addresses of nodes with schedules overlapping with the maintenance window. 2. For overlapping schedules on a node, disable. Run: **cluster run <node IP> schedule disable <job-name>**	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as “Processing” and then choose each **Action** that starts with “Import”, for example, “Import Unity Connection”. b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	
Customized ``data/Settings`` If `data/Settings` instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: *Post Template Upgrade Tasks*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

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

4.2.5. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status

Have the IP address available of the node determined to be the *primary database node*.
Verify that the primary database node is the active primary node at the time of upgrade.
On the primary application node, run:
cluster run <primary db IP> database config
From the output, ensure that the primary database node `stateStr` parameter is set to **PRIMARY** and it has the *highest* `priority:<number>` (highest priority number could vary depending on cluster layout).
Example output
`<ip address>:27020:`
`  priority: <number>`
`  stateStr: PRIMARY`
`  storageEngine: WiredTiger`
Validate the system health on the primary application node:
Verify cluster connectivity
- **cluster run all cluster status**
Verify network connectivity, disk status and NTP.
- **cluster check verbose**
If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/              (call support if over 80%)`
`/var/log       (run: log purge)`
`/opt/platform  (remove any unnecessary files from /media directory)`
`/tmp           (reboot)`
On the primary application node, verify there are no pending Security Updates on any of the nodes:
- **cluster run all security check**	

As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application. Optional: If a backup is also required - Database node backup: – Find the database node with the *second* highest weight. On the primary application node, run **cluster run database database weight list** to find this node. – Log in on the database node with the *second* highest weight. – Run **backup add <SFTP-location-name>** and **backup create <SFTP-location-name>** commands. Backups for an application and web proxy type node are not required. A backup created on the secondary database node will include all the relevant data, excluding the web certificates. For details, refer to the Platform Guide.	

Description and Steps	Notes and Status

Before upgrading, check all services, nodes and weights for the cluster on the primary application node.
Make sure no services are stopped/broken. The message ‘suspended waiting for mongo’ is normal on the fresh database nodes.
• **cluster run all app status**
Make sure all application nodes show.
• **cluster run application cluster list**
Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. The command is run from the primary application node and is carried out on all database nodes
• **cluster run database database weight list**
Example output:
`---------- VOSS-UN-2, ip=192.168.100.4, role=database, loc=cpt`
`192.168.100.4:`
`    weight: 70`
`192.168.100.6:`
`    weight: 50`
`192.168.100.8:`
`    weight: 30`
`---------- VOSS-UN-4, ip=192.168.100.6, role=database, loc=cpt`
`[...]`
Verify the primary database node in the primary site and ensure no nodes are in the ‘recovering’ state (`stateStr` is not `RECOVERING`). Run on the primary application node and use the primary database IP as parameter:
• **cluster run <primary db IP> database config**	

4.2.6. Upgrade

Description and Steps	Notes and Status
On the primary application node: • **screen** Run (optionally with command parameters below): `app install media/<script_file> delete-on-success yes --force` The upgrade will also silently run an updated version of **cluster check** and the upgrade will fail to proceed if any error conditions exist. Fix before proceeding. Refer to the Platform Guide for details on the new version of the **cluster check** command. Run on the primary application node and use the primary database IP as parameter: • **cluster run <primary db IP> database config** and verify the number of nodes are *uneven*, i.e. either 5 or 7. If not, run: **cluster run <primary db IP> cluster provision role database** Ensure an arbitrator shows when you run the command again: **cluster run <primary db IP> database config** (output shows: `stateStr:  ARBITER`) Note that during the upgrade, phone registration data is cleared. A message will show in the log: `Remove phone registration data`. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.	

4.2.7. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
On the primary application node, verify the cluster status: • **cluster status** • **cluster check** • If any of the above commands show errors, check for further details to assist with troubleshooting: **cluster run all diag health**	
If upgrade is successful, the screen session can be closed by typing **exit** in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.	
Check for needed security updates. On the primary application node, run: • **cluster run all security check** If one or more updates are required for any node, run on the primary application node: • **cluster run all security update** Note: *if the system reboots, do not carry out the next manual reboot step*. Manual reboot *only if needed*: • **cluster run notme system reboot** If node messages: `<node name> failed with timeout` are displayed, these can be ignored. • **system reboot** Since all services will be stopped, this takes some time.	

4.2.8. Post Template Upgrade Tasks

Description and Steps	Notes and Status
Restart the system from the command line if no reboot took place during the Post-Upgrade, Security and Health Steps. On the primary application node, run: **cluster run notme system reboot** and then **system reboot**	
Import ``device/cucm/PhoneType`` In order for a security profile to be available for a Call Manager Analog Phone, the `device/cucm/PhoneType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/PhoneType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **SSO Login URL check if needed** Verify the SSO Login URL if needed. Go to **Single Sign On > SSO Identity Provider** and ensure your URL matches the **SSO Login URL** value. **Customized ``data/Settings``** For releases prior to 21.1, merge the previously backed up customized `data/Settings` with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON. **Support for VG400 and VG450 Analogue Gateways** Before adding the VG400 or VG450 Gateway, the `device/cucm/GatewayType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/GatewayType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **Verify the upgrade** Log in on the GUI and check the information contained in the **About > Version** menu. Confirm that versions have upgraded: • **Release** should show `XXX` where `XXX` corresponds with the release number of the upgrade. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again. Verify that the web portal is configured to the required setting, either admin or classic. For further details on this setting, see *Web Portal Configuration* in the Platform Guide.	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.2.9. Restore Adaptations

Description and Steps	Notes and Status
Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.	

4.2.10. Restore Schedules

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. **Note:** Select the **Skip next execution** if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. Schedules enabled on the CLI. On the primary application node: 1. For disabled schedules that were overlapping the maintenance window, enable. Verify disabled schedules: **cluster run all schedule list**. Record the IP addresses of nodes and scheduled jobs disabled. 2. Enable schedules: **cluster run <node IP> schedule enable <job-name>**	

4.2.11. Release Specific Updates

Description and Steps	Notes and Status
When upgrading to release 21.3, users of Microsoft apps should after upgrade, select each Microsoft Tenant (`relation/MicrosoftTenant`) in the Admin GUI and click **Save** on it without making any changes. This step is required so that VOSS Automate can communicate with the Tenant post upgrade.	
Only if the following step was not carried out when upgrading to Release 21.3-PB1: On the primary node, run: `voss migrate_summary_attributes data/InternalNumberInventory`	

4.2.12. Log Files and Error Checks

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors. On the primary application node, use the **log view** command to view any log files indicated in the error messages, for example, run the command if the following message appears: `For more information refer to the execution log file with 'log view platform/execute.log'` For example, if it is required send all the install log files in the `install` directory to an SFTP server: • **log send sftp://x.x.x.x install**	
Log in on the GUI as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.2.13. Licensing after Delta Bundle Upgrade

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary application node CLI. 1. Obtain the required license token from VOSS. 2. Steps for GUI and CLI: a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

5. Single Node Upgrade

5.1. Upgrade a Single Node Cluster Environment with the Delta Bundle

Note:

- While system upgrade takes approximately two hours at a single site, this may vary in accordance with your topology, number of devices and subscribers. Adjust your upgrade maintenance window to allow for your configuration.

The standard **screen** command should be used where indicated. See: *Using the screen command*.

5.1.1. Download Files and Check

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** where XXX is the release number. Download `XXX-Delta-Bundle.script` file. Transfer the `XXX-Delta-Bundle.script` file to the `media/` folder. Two transfer options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <XXX-Delta-Bundle.script>** Or using SCP: • **scp <XXX-Delta-Bundle.script> platform@<unified_node_ip_address>:~/medi** Verify that the `.script` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the SFTP server match. • **system checksum media/<XXX-Delta-Bundle.script>** `Checksum: <SHA256>`	

5.1.2. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	

5.1.3. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet. Schedules enabled on the CLI: 1. Run **schedule list** to check if any schedules exist and overlap with the maintenance window. 2. For overlapping schedules, disable. Run **schedule disable <job-name>**.	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as “Processing” and then choose each **Action** that starts with “Import”, for example, “Import Unity Connection”. b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	
Customized ``data/Settings`` If `data/Settings` instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: *Post Template Upgrade Tasks*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

5.1.4. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status

Validate the system health.
diag health
If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/              (call support if over 80%)`
`/var/log       (run: log purge)`
`/opt/platform  (remove any unnecessary files from /media directory)`
`/tmp           (reboot)`
Verify there are no pending Security Updates:
security check	

Create a restore point. As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. VOSS cannot guarantee that a restore point can be used to successfully restore VOSS Automate. If you cannot restore the application from a restore point, your only recourse is to reinstall the application. After the restore point has been created, restart. Optional: If a backup is required in addition to the restore point, use the **backup add <location-name>** and **backup create <location-name>** commands. For details, refer to the Platform Guide.	

Description and Steps	Notes and Status
Before upgrading, check all services: Make sure no services are stopped/broken. The message ‘suspended waiting for mongo’ is normal on a fresh node. • **app status** Verify the node is not in the ‘recovering’ state (`stateStr` is not `RECOVERING`) • **database config**	

5.1.5. Upgrade

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** Run (optionally with command parameters below): • **app install media/<script_file>** From release 19.1.2 and later, the `delete-on-success` parameter and `yes` or `no` value have been added to remove or keep the the script file in the `media/` directory after successful installation. Note that during the upgrade, phone registration data is cleared. A message will show in the log: `Remove phone registration data`. This is required so that old values are not displayed, since after the upgrade this information is no longer stored in the resource cache.	

Note: In order to carry out fewer upgrade steps, the updates of instances of the some models are skipped in the cases where:

- `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
- `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
- Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

5.1.6. Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
Verify the status: • **diag health**	
If upgrade is successful, the screen session can be closed by typing **exit** in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.	
Check for needed security updates. • **security check** If one or more updates are required, complete all the security updates. • **security update** Note: *if the system reboots, do not carry out the next manual reboot step.* Manual reboot *only if needed*: • **system reboot**	

5.1.7. Post Template Upgrade Tasks

Description and Steps	Notes and Status
Restart the system from the command line if no reboot took place during the Post-Upgrade, Security and Health Steps. **system reboot**	
Import ``device/cucm/PhoneType`` In order for a security profile to be available for a Call Manager Analog Phone, the `device/cucm/PhoneType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/PhoneType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **SSO Login URL check if needed** Verify the SSO Login URL if needed. Go to **Single Sign On > SSO Identity Provider** and ensure your URL matches the **SSO Login URL** value. **Customized ``data/Settings``** Merge the previously backed up customized `data/Settings` with the latest settings on the system by manually adding the differences or exporting the latest settings to JSON, merging the customized changes and importing the JSON. **Support for VG400 and VG450 Analogue Gateways** Before adding the VG400 or VG450 Gateway, the `device/cucm/GatewayType` model needs to be imported for each Unified CM. 1. Create a Model Type List which includes the `device/cucm/GatewayType` model. 2. Add the Model Type List to all the required Unified CM Data Syncs. 3. Execute the Data Sync for all the required Unified CMs. **Verify the upgrade** Log in on the GUI and check the information contained in the **About > Version** menu. Confirm that versions have upgraded. • **Release** should show `XXX` • **Platform Version** should show `XXX` where `XXX` corresponds with the release number of the upgrade. If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again. Verify that the web portal is configured to the required setting, either admin or classic. For further details on this setting, see *Web Portal Configuration* in the Platform Guide.	
• Check themes on all roles are set correctly	

5.1.8. Restore Adaptations

Description and Steps	Notes and Status
Restore and adaptations prior to upgrade. If the release is accompanied by Upgrade Notes, refer to the details on adaptation impact.	

5.1.9. Restore Schedules

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet. **Note:** Select the **Skip next execution** if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. Schedules enabled on the CLI: 1. For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

5.1.10. Release Specific Updates

Description and Steps	Notes and Status
When upgrading to release 21.3, users of Microsoft apps should after upgrade, select each Microsoft Tenant (`relation/MicrosoftTenant`) in the Admin GUI and click **Save** on it without making any changes. This step is required so that VOSS Automate can communicate with the Tenant post upgrade.	
Only if the following step was not carried out when upgrading to Release 21.3-PB1: On the primary node, run: `voss migrate_summary_attributes data/InternalNumberInventory`	

5.1.11. Log Files and Error Checks

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors. Use the **log view** command to view any log files indicated in the error messages, for example, run the command if the following message appears: `For more information refer to the execution log file with 'log view platform/execute.log'` For example, if it is required send all the install log files in the `install` directory to an SFTP server: • **log send sftp://x.x.x.x install**	
Log in on the GUI as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

5.1.12. Licensing after Delta Bundle Upgrade

Description and Steps	Notes and Status
From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** on the CLI. 1. Obtain the required license token from VOSS. 2. Steps for GUI and CLI: a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide. b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide.	

Index