VOSS Automate
Upgrade Guide with ISO and Template

Release 21.4

Mar 26, 2024

Legal Information

DOCUMENT ID: 20240326221227

Contents

1 What's New **1**
- 1.1 Upgrade Guide with ISO and Template: Release 21.4-PB5 . . . 1
- 1.2 Upgrade Guide with ISO and Template: Release 21.4-PB4 . . . 1
- 1.3 Upgrade Guide with ISO and Template: Release 21.4-PB3 . . . 1
- 1.4 Upgrade Guide with ISO and Template: Release 21.4-PB2 . . . 1
- 1.5 Upgrade Guide with ISO and Template: Release 21.4-PB1 . . . 1
- 1.6 Upgrade Guide with ISO and Template: Release 21.4 . . . 1

2 Introduction **3**

3 Upgrade Planning **5**
- 3.1 Upgrade and Data Migration . . . 5
- 3.2 Using the `screen` command . . . 5

4 Multinode Upgrade **7**
- 4.1 Unified Node Topology: Upgrade a Multinode Environment with the ISO and Template . . . 7
- 4.2 Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template . . . 24

5 Single Node Upgrade **37**
- 5.1 Upgrade a Single Node Cluster Environment with the ISO and Template . . . 37

6 Upgrade Sheets **50**
- 6.1 Multinode Upgrade Sheet . . . 50

Index **60**

1. What's New

1.1. Upgrade Guide with ISO and Template: Release 21.4-PB5

- N/A

1.2. Upgrade Guide with ISO and Template: Release 21.4-PB4

- N/A

1.3. Upgrade Guide with ISO and Template: Release 21.4-PB3

- N/A

1.4. Upgrade Guide with ISO and Template: Release 21.4-PB2

- N/A

1.5. Upgrade Guide with ISO and Template: Release 21.4-PB1

- N/A

1.6. Upgrade Guide with ISO and Template: Release 21.4

- VOSS-872: License Enforcement. See: *Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template*

  Added details on license requirements.

- VOSS-872: License Enforcement. See: *Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template*

  Added details on license requirements.

- VOSS-872: License Enforcement. See: *Upgrade a Single Node Cluster Environment with the ISO and Template*

  Added details on license requirements.

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.

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 from 19.X or earlier - Model and Workflow Changes

When upgrading from 19.X or earlier, refer to the VOSS-4-UC 21.1 Release Changes and Impact document for details on model and workflow changes. Customizations related to these changes may be affected.

Release 19.2.1 onwards - Minimum Hardware Requirements

From release 19.2.1 onwards, the minimum RAM hardware requirements for all unified nodes is 16GB.

Refer to the topic on Memory (RAM) Increase for Large End User Capacity in the Platform Guide for steps to upgrade your virtual machine.

Patches Required for Upgrades from v19.1.2, v19.2.1, v19.3.1, v19.3.2

When upgrading from any of the following versions, first obtain and apply the patch corresponding to your version:

From the VOSS secure FTP site:

- 19.1.2 - `/software/patches/19.1.2/Recommended_Patches/EKB-3853-19.1.2_patch`
- 19.2.1 - `/software/patches/19.2.1/Recommended_Patches/EKB-3853-19.2.1_patch`

From **Downloads > VOSS-4-UC** on voss.portalshape.com:

- **19.3.1 > Patches > EKB-3853-19.3.1_patch**
- **19.3.2 > Patches > EKB-3853-19.3.2_patch**

Microsoft/Cisco Hybrid Adaptation not Supported for Upgrades to v21.2

Customers using the Microsoft/Cisco Hybrid (Direct Routing) adaptation will not be able to upgrade to the 21.2 release. This adaptation is only supported on release 19.3.4 and has not been made compatible with some of the core functionality in release 21.2.

Customers using this adaptation and wish to upgrade to release 21.3 should first contact VOSS Global Services.

Upgrading From v19.3.x with FIPS Enabled

If you have FIPS enabled on your system, then before continuing with the upgrade, see:

The *Upgrading from Release 19.3.x with FIPS enabled* section in the Platform Guide.

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. Upgrade and Data Migration

After the upgrade of the system with **app upgrade <file.ISO>** or **cluster upgrade <file.ISO>**, any changes and updates to core model schemas need to be added to the system database. It is recommended that this step is run in a terminal opened with the **screen** command.

This database upgrade is carried out from the Command Line Interface (CLI) by means of **voss upgrade_db**. It is recommended that this step is run in a terminal opened with the **screen** command.

From instructions in the newly upgraded ISO, the schemas of system core models are updated as required and existing data is migrated to these updated model schemas. Schema updates would include updated version numbers and may for example add or remove new model attributes to schemas and add new default data.

Migration instructions from existing model versions to new updated versions are used to create the updated model schemas and update data to be stored in the system database.

In the case of the installation of an updated template, the **app template <template_file>** command will also execute any migration instructions included in the template file to upgrade the database with the updated template data.

3.2. 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 ISO and Template

Note:

- When upgrading from VOSS-4-UC 18.1.3, refer to *Upgrading from 18.1.3 to Current Release - Summary*.
- Upgrading to release 21.1 *requires a system on 19.x, with security updates completed*. The upgrade includes:
  - an upgrade to the underlying operating system to Ubuntu 18.04.4.
  - the installation of a new **cluster check** command available from the 21.1 ISO by running **app install check_cluster**.
- While template installation and 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.

  You can follow the progress on the Admin Portal transaction list.
- When upgrading from CUCDM 11.5.3 Patch Bundle 2 or VOSS-4-UC 18.1 Patch Bundle 2 and earlier, re-import specified CUC models according to your current version. Refer to the final upgrade procedure step.
- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.
- If any Microsoft integrations exist in VOSS Automate pre-upgrade, then the existing device connections configured for Microsoft Entra ID will not be automatically migrated to MS Graph and will have to be manually migrated to MSGraph prior to the upgrade to 21.3.

  Note: Microsoft changed the name of Azure Active Directory to Microsoft Entra ID in August 2023.

  Service Providers who are operating with release 19.3.4 of the Cisco-Microsoft Adaptation should contact VOSS Global Services first.

  The MS Graph connection configuration requires additional details, which must be obtained prior to upgrade. Please see the *VOSS Automate Configuration and Sync* and *Microsoft Configuration Setup* topics in the Core Feature Guide.

  - Ensure MicrosoftTenant, MSTeamsOnline and MSGraph instance have the same name by renaming instances.

- If you have FIPS enabled on your system, the before continuing with the upgrade, see:

  The Upgrading from Release 19.3.x with FIPS enabled section in the Platform Guide.

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

4.1.1. Download Files and Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso`/`.ova` and `.template` files, where XXX matches the release. • Transfer the `.iso`/`.ova` file to the `media/` folder of all nodes. • Transfer the `.template` file to the `media/` folder of the primary node. Two transfer options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_or_ova_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_or_ova_file> platform@<unified_node_ip_address>:~/med** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso`/`.ova` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site server match. • **system checksum media/<upgrade_iso_or_ova_file>** `Checksum: <SHA256>` • **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

4.1.2. Security and Health Check Steps (Prior to Maintenance Window)

Description and Steps	Notes and Status

Verify that the primary node is the active primary node at the time of upgrade.
database config
Ensure that the node on which the installation will be initiated has the `stateStr` parameter set to **PRIMARY** and 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. Carry out the following (19.x only):
• **system mount** - mount upgrade ISO.
• **app install check_cluster** - install the new version of the **cluster check** command. For details, refer to the "Cluster Check" topic in the Platform Guide.
• **cluster check** - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details. While warnings will not prevent an upgrade, it is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading.
For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example 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)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes.
--- 	
Note: If you run **cluster status** after installing the new version of **cluster check**, any error message regarding a failed command can be ignored. This error message will not show after upgrade.
--- 	
• **Adaptation check** - if the *GS SME Adaptation* is installed, check for duplicate instances of of `GS_SMETemplateData_DAT` and deleted any duplicates before upgrading to 21.2.	

4.1.3. Schedules, Transactions and Version Check (Maintenance Window)

Description and Steps	Notes and Status
Run **cluster check** and verify that no warnings and errors show. 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 Admin Portal 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 Admin Portal, 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 Admin Portal 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 (Maintenance Window)*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the menu: **About > Version**	

4.1.4. Pre-Upgrade Steps (Maintenance Window)

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. Optional: If a backup is also required, 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

After restore point creation and before upgrading: validate system health and check all services, nodes and weights for the cluster:
• **cluster run application cluster list**
Make sure all application nodes show 4 or 6 nodes.
• **cluster check** - inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.
– Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
– Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. 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:	

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/`
`↪csrbackup`	

4.1.5. Upgrade (Maintenance Window)

Note: By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. Verify that the ISO has been uploaded to the `media/` directory on each node. This will speed up the upgrade time. On the primary unified node: • **screen** • **cluster upgrade media/<upgrade_iso_file>** Note: If the system reboots, do not carry out the next manual reboot step. When upgrading from pre-19.1.1, an automatic reboot should be expected. 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. Close **screen**: `Ctrl-a \`	

All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

4.1.6. Post-Upgrade, Security and Health Steps (Maintenance Window)

Description and Steps	Notes and Status
On the primary unified node, verify the 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**	
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.	
To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run: **cluster run all app cleanup**	
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.	

4.1.7. Database Filesystem Conversion (if required, Maintenance Window)

Important: This step is to be carried out *only if* you have not converted the file system before.

To check if the step is *not* required:

- Run **drives list** and ensure that the LVM storage shows for *all converted database nodes* under `Volume Groups`. If the output of the **drives list** command contains `dm-0 - mongodb:dbroot`, the step is *not* required. Refer to the **drives list** command output example below.

The **database convert_drive** command provides parameters that allow for a flexible upgrade schedule in order to limit system downtime.

When the **database convert_drive** command is run, the `voss-deviceapi` service will be stopped first and started after completion. The command should therefore be run during a maintenance window while there are no running transactions.

The procedure and commands in this step depend on:

- your topology
- latency between data centers
- upgrade maintenance windows - **Window 1** to **Window 3** represent chosen maintenance windows.

First inspect the table below for guidance on the commands to run according to your configuration and preferences.

- Run all commands on the primary unified node:
  - Ensure states of database nodes are not DOWN - otherwise the command will fail

    database config (`stateStr` is not `DOWN`)
  - Ensure database weights are set and have 1 maximum weight - otherwise the command will fail

    database weight list (one `weight` value is maximum)
- For 2 and 3 maintenance windows: after the upgrade (prior to Windows 2 and 3), only nodes with converted drives will generate valid backups.

  For example, if the primary drive is converted, backups from the primary node can be used to restore the database. If there is a database failover to the highest weight secondary node that was not converted, it will not be possible for backups to be generated on that secondary node until the drive is converted.

Topology	Window 1	Window 2	Window 3	Commands (DC = valid data center name)	Description
multinode	Y			**database convert_drive primary** **database convert_drive secondary all**	Recommended for a system with latency < 10ms.
multinode	Y	Y		Window 1: **database convert_drive primary** Window 2: **database convert_drive secondary all**	Can be used for a system with latency < or > 10ms. Allows for smaller maintenance windows. Cluster is not available during maintenance windows.
multinode	Y	Y	Y	Window 1: **database convert_drive primary** Window 2: **database convert_drive secondary <first DC>** Window 3: **database convert_drive secondary <second DC>**	Can be used for a system with latency > 10ms. Allows for smaller maintenance windows. Cluster is not available during maintenance windows.

Description and Steps	Notes and Status
Database Filesystem Conversion step Shut down all the nodes. Since all services will be stopped, this takes some time. • **cluster run all system shutdown** • Create restore point for all the unified servers so that the system can easily be reverted in the case of a conversion error. 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. • Run the **convert_drive** command *with parameters according to the table above*. Wait until it completes successfully. • **database config** Ensure that the storage engine for *all converted database nodes* shows as `storageEngine: WiredTiger`. • **drives list** Ensure that the LVM storage shows for *all database nodes* under `Volume Groups`.	

In the example below, `dbroot/dm-0` shows under `Volume Groups`, `Logical volumes`

```
$ drives list
Used disks and mountpoints:
sdc1 - services:backups
dm-0 - mongodb:dbroot

Unused disks:
none - if disks have been hot-mounted, it may be necessary to reboot the system

Unused mountpoints:
services:SWAPSPACE

Volume Groups
voss - 10.0 GB free, 60.0 GB total
Physical volumes:
sdd1
Logical volumes:
dbroot/dm-0 - 50.0 GB
```

4.1.8. Database Schema Upgrade (Maintenance Window)

Important: When upgrading from 19.X or earlier, please refer to the VOSS-4-UC 21.1 Release Changes and Impact document for details on model and workflow changes. Customizations related to these changes may be affected by this step.

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary unified node: • **screen** • **voss upgrade_db** Check cluster status • **cluster check**	

4.1.9. Template Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary unified node: • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

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

The template upgrade automatically detects the deployment mode: “Enterprise”, “Provider with HCM-F” or “Provider without HCM-F”. A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay_Hcmf.json ...

Importing ProviderOverlay_Decoupled.json ...
```

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

Description and Steps	Notes and Status
Review the output from the **app template** command and confirm that the upgrade message appears:	

```
Deployment summary of PREVIOUS template solution
(i.e. BEFORE upgrade):
-----------------------------------------------


Product: [PRODUCT]
Version: [PREVIOUS PRODUCT RELEASE]
Iteration-version: [PREVIOUS ITERATION]
Platform-version: [PREVIOUS PLATFORM VERSION]
```

This is followed by updated product and version details:

```
Deployment summary of UPDATED template solution
(i.e. current values after installation):
-----------------------------------------------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

Description and Steps	Notes and Status
• If no errors are indicated, create a restore point. This restore point can be used if post-upgrade patches that may be required, fail. 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.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin`
`and see Transaction logs for more detail.`
You can roll back as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
Verify the `extra_functions` have the *same checksum* across the cluster. • **cluster run application voss get_extra_functions_version -c**	
Post upgrade migrations: On a single node of a cluster, run: • **voss post-upgrade-migrations**	

Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.

A transaction is queued on VOSS Automate and its progress is displayed as it executes.

Description and Steps	Notes and Status
Check cluster status and health • **cluster status**	

4.1.10. Post Template Upgrade Tasks (Maintenance Window)

Description and Steps	Notes and Status
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 Admin Portal 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.	
• Check themes on all roles are set correctly	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.1.11. Restore Schedules (Maintenance Window)

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 Admin Portal 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** option 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>**.	

4.1.12. Release Specific Updates (Maintenance Window)

Description and Steps	Notes and Status
When upgrading from CUCDM 11.5.3 Patch Bundle 2 or VOSS-4-UC 18.1 Patch Bundle 2 and earlier, re-import the following from all CUCM devices, since this upgrade deleted obsolete CUC timezone codes from the VOSS Automate database: • CUC models: `device/cuc/TimeZone` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
After upgrading, obtain and install the following patch according to its accompanying MOP file, where XXX matches the release.: • **Server Name**: `https://voss.portalshape.com` • **Path**: **Downloads > VOSS Automate > XXX > Upgrade** • **Patch Directory**: `Update_CUC_Localization_patch` • **Patch File**: `Update_CUC_Localization_patch.script` • **MOP File**: `MOP-Update_CUC_Localization.pdf` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.x, then it does not have to be repeated.	
Re-import the following from all CUCM devices: • CUCM models: `device/cucm/PhoneType` For steps to create a custom data sync, refer to the chapter on Data Sync in the Core Feature Guide. Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
User Management migration updates default authentication types on SSO Identity Providers. If an SSO Identity Provider exists at the provider hierarchy level, the default authentication settings: • Authentication Scope: Current hierarchy level and below • User Sync Type: All users will not allow any non-SSO user logins (typically local administrators). The solution is to log in as higher level administrator account (full access) and set the SSO Identity Provider: • Authentication Scope: Current hierarchy level only • User Sync Type: LDAP synced users only Please refer to the *SSO Identity Provider: Field Reference* topic in the Core Feature Guide.	
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`	

When upgrading to release 21.3, users of Microsoft apps should 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.

4.1.13. Log Files and Error Checks (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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 Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.1.14. Licensing (outside, after Maintenance Window)

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.	

4.1.15. Upgrading from 18.1.3 to Current Release - Summary

Below are the summarized steps to upgrade from 18.1.3.

- The steps require the necessary scripts, templates and ISOs to be in the `media/` directory.
- For details on the specific commands, refer to the corresponding steps above.
- For general usage of commands to carry out tasks, refer to the *Platform Guide*.

Command and task sequence	Comment
`cluster status`	no service mismatch, all nodes ok
`cluster run all diag disk`	check for disks over 90% full
`database config`	ensure all unified nodes have a weight, and are in a good state: primary, secondary,arbiter
manual check	stop / check for transactions running, stop where possible
external task	create restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.
`cluster run all app install media/EKB-4124-18.1.3_patch.script`	refer to steps details above
`cluster upgrade media/platform-install-19.2.1-1570776653.iso --force`	refer to steps details above
`cluster run all security update --force`	refer to steps details above
external task	create restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.
`cluster upgrade media/platform-install-<current>-<nnnnnnnnnn>.iso`	refer to preliminary and upgrade steps details above; `<current>-<nnnnnnnnnn>` matches the downloaded release ISO
`cluster run all security update`	refer to steps details above
`database config`	make sure all databases are in the correct state
`database convert_drive <params>`	Run the **convert_drive** command with *parameters* according to the table at: Database Filesystem Conversion section.
`voss upgrade_db`	refer to steps details above
`app template media/<VOSS Automate.template>`	refer to steps details above

4.2. Modular Cluster Topology: Upgrade a Multinode Environment with the ISO and Template

Note:

- When upgrading from an existing Modular Cluster Topology that was available since VOSS Automate 21.1, use the steps listed here.
- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.

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

Primary database and application node in a Modular Cluster Topology

- Verify the *primary application node* (UN2) with the **cluster primary role application** command run on the node. The output should be *true*, for example:

```
platform@UN2:~$ cluster primary role application
is_primary: true
```

- Verify the *primary database node* (UN1) with the **cluster primary role database** command run on the node. The output should be *true*, for example:

```
platform@UN1:~$ cluster primary role database
is_primary: true
```

4.2.1. Download Files and Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso`/`.ova` and `.template` files, where XXX is the release number. • Transfer the `.iso` file to the `media/` folder of the primary database node. • Transfer the `.template` file to the `media/` folder of the primary application node. Two transfer options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_or_ova_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_or_ova_file> platform@<unified_node_ip_address>:~/med** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site match. • primary database node: **system checksum media/<upgrade_iso_or_ova_file>** `Checksum: <SHA256>` • primary application node: **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

4.2.2. Security and Health Check Steps (Prior to Maintenance Window)

Description and Steps	Notes and Status

Verify that the primary database node is the active primary node at the time of upgrade.
database config
Ensure that the node on which the installation will be initiated has the `stateStr` parameter set to **PRIMARY** and 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`
• **cluster check** - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details. While warnings will not prevent an upgrade, it is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading.
For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example 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)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes.
Note: If you run **cluster status** after installing the new version of **cluster check**, any error message regarding a failed command can be ignored. This error message will not show after upgrade.
• **Adaptation check** - if the *GS SME Adaptation* is installed, check for duplicate instances of of `GS_SMETemplateData_DAT` and deleted any duplicates before upgrading to 21.2.	

4.2.3. Schedules, Transactions and Version Check (Maintenance Window)

Description and Steps	Notes and Status
Run **cluster check** and verify that no warnings and errors show. 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 Admin Portal 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 Admin Portal, 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 primary application node 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 Admin Portal 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**.	
Version Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the menu: **About > Version**	

4.2.4. Pre-Upgrade Steps (Maintenance Window)

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. Optional: If a backup is also required - on the primary database node, 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

After restore point creation and before upgrading: validate system health and check all services, nodes and weights for the cluster:
• **cluster run application cluster list**
Make sure all application nodes show.
• **cluster check** - inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.
– Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh database nodes.
– Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. 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:
On the primary application node, verify there are no pending Security Updates on any of the nodes:
• **cluster run all security check**	

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/`
`↪csrbackup`	

4.2.5. Upgrade (Maintenance Window)

Note: By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. Verify that the ISO has been uploaded to the `media/` directory on each node. This will speed up the upgrade time. On the primary database node: • **screen** • **cluster upgrade media/<upgrade_iso_file>** Close **screen**: `Ctrl-a \`	

All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

4.2.6. Post-Upgrade and Health Steps (Maintenance Window)

Description and Steps	Notes and Status
On the primary database node, verify the 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**	
To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run: **cluster run all app cleanup** on the primary database node.	
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.	
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.	

4.2.7. Database Schema Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary application node: • **screen** • **voss upgrade_db** Check cluster status • **cluster check**	

4.2.8. Template Upgrade (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary application node: • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

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

The template upgrade automatically detects the deployment mode: “Enterprise”, “Provider with HCM-F” or “Provider without HCM-F”. A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json
```

(continues on next page)

(continued from previous page)

```
Importing ProviderOverlay_Hcmf.json ...

Importing ProviderOverlay_Decoupled.json ...
```

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

Description and Steps	Notes and Status
Review the output from the **app template** command and confirm that the upgrade message appears:	

```
Deployment summary of PREVIOUS template solution
(i.e. BEFORE upgrade):
-------------------------------------------------


Product: [PRODUCT]
Version: [PREVIOUS PRODUCT RELEASE]
Iteration-version: [PREVIOUS ITERATION]
Platform-version: [PREVIOUS PLATFORM VERSION]
```

This is followed by updated product and version details:

```
Deployment summary of UPDATED template solution
(i.e. current values after installation):
-------------------------------------------------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

Description and Steps	Notes and Status
• If no errors are indicated, 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.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin`
`and see Transaction logs for more detail.`
You can roll back as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
On the primary application node, verify the `extra_functions` have the *same checksum* across the cluster. • **cluster run application voss get_extra_functions_version -c**	
Post upgrade migrations: On a single application node of a cluster, run: • **voss post-upgrade-migrations**	

Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.

A transaction is queued on VOSS Automate and its progress is displayed as it executes.

Description and Steps	Notes and Status
Check cluster status and health • on the primary database node: • **cluster status**	

4.2.9. Post Template Upgrade Tasks (Maintenance Window)

Description and Steps	Notes and Status
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 Admin Portal 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.	
• Check themes on all roles are set correctly	
• For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary.	

4.2.10. Restore Schedules (Maintenance Window)

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 Admin Portal 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** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter. Schedules enabled on the CLI of the primary application node: 1. For disabled schedules that were overlapping the maintenance window, enable. Run **schedule enable <job-name>**.	

4.2.11. Release Specific Updates (Maintenance Window)

Description and Steps	Notes and Status
When upgrading from CUCDM 11.5.3 Patch Bundle 2 or VOSS-4-UC 18.1 Patch Bundle 2 and earlier, re-import the following from all CUCM devices, since this upgrade deleted obsolete CUC timezone codes from the VOSS Automate database: • CUC models: `device/cuc/TimeZone` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
After upgrading, obtain and install the following patch according to its accompanying MOP file: • **Server Name**: `secure.voss-solutions.com` • **Path**: `/software/voss4uc/releases/Release-19.2.1` • **Patch Directory**: `Update_CUC_Localization_patch` • **Patch File**: `Update_CUC_Localization_patch.script` • **MOP File**: `MOP-Update_CUC_Localization.pdf` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
Re-import the following from all CUCM devices: • CUCM models: `device/cucm/PhoneType` For steps to create a custom data sync, refer to the chapter on Data Sync in the Core Feature Guide. Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
User Management migration updates default authentication types on SSO Identity Providers. If an SSO Identity Provider exists at the provider hierarchy level, the default authentication settings: • Authentication Scope: Current hierarchy level and below • User Sync Type: All users will not allow any non-SSO user logins (typically local administrators). The solution is to log in as higher level administrator account (full access) and set the SSO Identity Provider: • Authentication Scope: Current hierarchy level only • User Sync Type: LDAP synced users only Please refer to the *SSO Identity Provider: Field Reference* topic in the Core Feature Guide.	
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 (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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 Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

4.2.13. Licensing (outside, after Maintenance Window)

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 ISO and Template

Important:

- Upgrading to release 21.1 *requires a system on 19.x, with security updates completed*.
- While template installation and 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.
- When upgrading from CUCDM 11.5.3 Patch Bundle 2 or VOSS-4-UC 18.1 Patch Bundle 2 and earlier, re-import specified CUC models according to your current version. Refer to the final upgrade procedure step.
- Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduce down time.

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

5.1.1. Download Files and Check (Prior to Maintenance Window)

Description and Steps	Notes and Status
VOSS files: **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade** Download `.iso`/`.ova` and `.template` files, where XXX matches the release. Transfer the file to the `media/` folder. Two options: Either using SFTP: • **sftp platform@<unified_node_hostname>** • **cd media** • **put <upgrade_iso_or_ova_file>** • **put <upgrade_template_file>** Or using SCP: • **scp <upgrade_iso_or_ova_file> platform@<unified_node_ip_address>:~/med** • **scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media** Verify that the `.iso`/`.ova` image and `.template` file copied: • **ls -l media/** Verify that the original `.sha256` checksums on the Download site match. • **system checksum media/<upgrade_iso_or_ova_file>** `Checksum: <SHA256>` • **system checksum media/<upgrade_template_file>** `Checksum: <SHA256>`	

5.1.2. Security and Health Steps single node cluster (Prior to Maintenance Window)

Description and Steps	Notes and Status
Validate the system health. Verify there are no pending Security Updates: **security check**	

Check system health.
• **diag disk**
If there is any sign of the paths below are over 80% full, a clean-up is needed, for example 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)`
• **Adaptation check** - if the *GS SME Adaptation* is installed, check for duplicate instances of of `GS_SMETemplateData_DAT` and deleted any duplicates before upgrading to 21.2.	

5.1.3. Schedules, Transactions and Version Check (Maintenance Window)

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 Admin Portal 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 Admin Portal, 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 Admin Portal 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 single node cluster (Maintenance Window)*. **Version** Record the current version information. This is required for upgrade troubleshooting. • Log in on the Admin Portal and record the information contained in the **About > Extended Version**	

5.1.4. Pre-Upgrade Steps single node cluster (Maintenance Window)

Create a restore point and then restart server. 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. If you cannot restore the application from a restore point, your only recourse is to reinstall the application. When the backup is complete and you do not need the restore point for restore activities, you can remove it. 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**	

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run on the CLI as `root` user, the following command:
`for LST in /opt/platform/apps/nginx/config/csr/*;`
`do openssl x509 -in $LST -text -noout >/dev/null`
`2>&1 && SIGNED="$LST"; done`
 	
`echo $SIGNED`
If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`	

5.1.5. Upgrade single node cluster (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. On the primary unified node: • **screen** • If upgrading from *earlier* than release 20.1.1: **app upgrade media/<upgrade_iso_file>** **Note:** If upgrading from release 20.1.1, on the *primary unified* node, use the command: **cluster upgrade media/<upgrade_iso_file>** If upgrading from release 21.1 and up, on the *primary application* node, **cluster upgrade media/<upgrade_iso_file>** All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage. Note: If the system reboots, do not carry out the next manual reboot step. When upgrading from pre-19.1.1, an automatic reboot should be expected. To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run: **cluster run all app cleanup** Manual reboot *only if needed*: • **system reboot** If node messages: `<node name> failed with timeout` are displayed, these can be ignored. Since all services will be stopped, this takes some time. Close **screen**: `Ctrl-a \`	

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 single node cluster (Maintenance Window)

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.	
Complete all the security updates. • **security update** The docker images `selfservice` and `voss_ubuntu` will be removed from the system at this stage. Note: If the system reboots, do not carry out the next manual reboot step . When upgrading from pre-19.1.1, an automatic reboot should be expected. Manual reboot *only if needed*: • **system reboot**	

5.1.7. Database Filesystem Conversion single node cluster (Maintenance Window, if required)

Important: To check if the step is *not* required:

- Run **drives list** and ensure that the LVM storage shows for *all converted database nodes* under `Volume Groups`. If the output of the **drives list** command contains `dm-0 - mongodb:dbroot`, the step is *not* required. Refer to the **drives list** command output example below.

The **database convert_drive** command provides parameters that allow for a flexible upgrade schedule in order to limit system downtime.

When the **database convert_drive** command is run, the `voss-deviceapi` service will be stopped first and started after completion. The command should therefore be run during a maintenance window while there are no running transactions.

For a single node cluster system drive conversion, ensure the `standalone` parameter is used.

Description and Steps	Notes and Status

Shut down. Since all services will be stopped, this takes some time.
• **system shutdown**
Create a restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed so that the system can easily be reverted in the case of a conversion error.
Stop transactions from being scheduled.
Run:
• **database convert_drive standalone**
Note: this step may take a few hours. Wait until it completes successfully.
• **database config**
Ensure that the storage engine for the *database node* shows as `storageEngine: WiredTiger`
• **drives list**
Ensure that the LVM storage for the *database node* shows under `Volume Groups`
In the example below, `dbroot/dm-0` shows under `Volume Groups`, `Logical volumes`
`$ drives list`
`Used disks and mountpoints:`
`sdc1 - services:backups`
`dm-0 - mongodb:dbroot`
`Unused disks:`
`none - if disks have been hot-mounted, it may be necessary to reboot the system`
`Unused mountpoints:`
`services:SWAPSPACE`
`Volume Groups`
`voss - 10.0 GB free, 60.0 GB total`
`Physical volumes:`
`sdd1`
`Logical volumes:`
`dbroot/dm-0 - 50.0 GB`	

5.1.8. Database Schema Upgrade single node cluster (Maintenance Window)

Important: When upgrading from 19.X or earlier, please refer to the VOSS-4-UC 21.1 Release Changes and Impact document for details on model and workflow changes. Customizations related to these changes may be affected by this step.

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** • **voss upgrade_db**	

5.1.9. Template Upgrade single node cluster (Maintenance Window)

Description and Steps	Notes and Status
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** • **app template media/<VOSS Automate.template>**	

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

The template upgrade automatically detects the deployment mode: “Enterprise”, “Provider with HCM-F” or “Provider without HCM-F”. A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay_Hcmf.json ...

Importing ProviderOverlay_Decoupled.json ...
```

The template install automatically restarts necessary applications.

Description and Steps	Notes and Status

Review the output from the **app template** command and confirm that the upgrade message appears:
`Deployment summary of PREVIOUS template solution (i.e. BEFORE upgrade):`
`---`
`Product: [PRODUCT]`
`Version: [PREVIOUS PRODUCT RELEASE]`
`Iteration-version: [PREVIOUS ITERATION]`
`Platform-version: [PREVIOUS PLATFORM VERSION]`
This is followed by updated product and version details:
`Deployment summary of UPDATED template solution (i.e. current values after installation):`
`---`
`Product: [PRODUCT]`
`Version: [UPDATED PRODUCT RELEASE]`
`Iteration-version: [UPDATED ITERATION]`
`Platform-version: [UPDATED PLATFORM VERSION]`	

Description and Steps	Notes and Status
• If no errors are indicated, make a backup or restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. This restore point can be used if post-upgrade patches that may be required, fail.	

For an unsupported upgrade path, the install script stops with the message:
`Upgrade failed due to unsupported upgrade path.`
`Please log in as sysadmin and see Transaction logs for more detail.`
You can restore to the backup or rollback/revert to the restore point made before the upgrade.	

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support.	
Post upgrade migrations: • **voss post-upgrade-migrations** Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows. A transaction is queued on VOSS Automate and its progress is displayed as it executes.	

Description and Steps	Notes and Status
Check status and health • **diag health** • **app status**	

5.1.10. Post Template Upgrade Tasks single node cluster (Maintenance Window)

Description and Steps	Notes and Status
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. **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 Admin Portal 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.	
• Check themes on all roles are set correctly	

5.1.11. Restore Schedules single node cluster (Maintenance Window)

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 Admin Portal 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>**.	

5.1.12. Release Specific Updates single node cluster (Maintenance Window)

Description and Steps	Notes and Status
When upgrading from CUCDM 11.5.3 Patch Bundle 2 or VOSS-4-UC 18.1 Patch Bundle 2 and earlier, re-import the following from all CUCM devices, since this upgrade deleted obsolete CUC timezone codes from the VOSS Automate database: • CUC models: `device/cuc/TimeZone` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
After upgrading, obtain and install the following patch according to its accompanying MOP file, where XXX matches the release: • **Server Name**: `https://voss.portalshape.com` • **Path**: **Downloads > VOSS Automate > XXX > Upgrade** • **Patch Directory**: `Update_CUC_Localization_patch` • **Patch File**: `Update_CUC_Localization_patch.script` • **MOP File**: `MOP-Update_CUC_Localization.pdf` Note: This is a once off data migration step. If this was performed previously when upgrading to 19.x, then it does not have to be repeated.	
Re-import the following from all CUCM devices: • CUCM models: `device/cucm/PhoneType` For steps to create a custom data sync, refer to the chapter on Data Sync in the Core Feature Guide. Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x, then it does not have to be repeated.	
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`	

5.1.13. Log Files and Error Checks single node cluster (Maintenance Window)

Description and Steps	Notes and Status
Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`. 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 Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors.	

5.1.14. Licensing (outside, after Maintenance Window)

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. 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.	

For Upgrading from 18.1.3 to the current release, see: *Upgrading from 18.1.3 to Current Release - Summary*.

6. Upgrade Sheets

6.1. Multinode Upgrade Sheet

To download this sheet, refer to the HTML documentation.

Table 1: Multinode Upgrade Sheet

Description	Steps
Download Files and Check Steps	**Download Files and Check Steps**
**********	**********
Download VOSS files - XXX is the release number	https://voss.portalshape.com > **Downloads > VOSS Automate > XXX > Upgrade**
Download .iso and .template files	Transfer the .iso file to the media/ folder of all nodes
Download .iso and .template files	Transfer the .template file to the media/ folder of the primary node
Two transfer options:	
Either using SFTP:	
	sftp platform@<unified_node_hostname>
	cd media
	put <upgrade_iso_file>
	put <upgrade_template_file>
Or using SCP:	
	scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media
	scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media
Verify that the .iso image and .template file copied:	**ls -l media/**
Verify that the original .sha256 checksums on the SFTP server match.	**system checksum media/<upgrade_iso_file>**
	`Checksum: <SHA256>`
	system checksum media/<upgrade_template_file>

continues on next page

Table 1 – continued from previous page

Description	Steps
	`Checksum: <SHA256>`
Security and Health Check Steps	**Security and Health Check Steps**
==========	==========
Verify that the primary node is the active primary node at the time of upgrade	**database config**
Ensure that the node on which the installation will be initiated has the stateStr parameter set to **PRIMARY** and 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. Carry out the following (19.x only):	**system mount** - mount the upgrade ISO.
	app install check_cluster - install the new version of the **cluster check** command.
For details: refer to the 'Cluster Check' topic in the Platform Guide.	
cluster check - inspect the output of this command for warnings and errors. You can also use **cluster check verbose** to see more details. While warnings will not prevent an upgrade. It is advisable that these be resolved prior to upgrading where possible. Some warnings may be resolved by upgrading.	**cluster check**
For troubleshooting and resolutions: also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.	
If there is any sign of the paths below are over 80% full: a clean-up is needed. For example 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
On the Primary Unified Node: verify there are no pending Security Updates on any of the nodes.	
Note: If you run **cluster status** after installing the new version of **cluster check**: any error message regarding a failed command can be ignored. This error message will not show after upgrade.	

continues on next page

Table 1 – continued from previous page

Description	Steps
Schedules, Transactions and Version Check steps	**Schedules, Transactions and Version Check steps**
==================================	==================================
Run **cluster check** and verify that no warnings and errors show.	**cluster check**
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 Admin Portal 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 Admin Portal: 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 Admin Portal as a high level administrator above Provider level.

continues on next page

Table 1 – continued from previous page

Description	Steps
	2. Select the **Transaction** menu to view transactions.
	3. Filter the **Action** column
	3a. Choose **Status** as Processing and then choose each **Action** that starts with Import for example 'Import Unity Connection'.
	3b. Click **Search** and confirm there are no results.
	3c. 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: Window Post Template Upgrade Tasks.	
Version	
Record the current version information. This is required for upgrade troubleshooting.	Log in on the Admin Portal and record the information contained in the **About > Extended Version**
Pre-Upgrade Steps	**Pre-Upgrade Steps**
==========	**==========**
VOSS cannot guarantee that a restore point can be used to successfully restore VOSS-4-UC. If you cannot restore the application from a restore point, your only recourse is to reinstall the application.	
Create a restore point as per the guidelines for the infrastructure on which the VOSS-4-UC platform is deployed.	
Optional: If a backup is also required	**backup add <location-name>**
	backup create <location-name>
For details, refer to the *Platform Guide*.	
After restore point creation and before upgrading: validate system health and check all services nodes and weights for the cluster:	**cluster run application cluster list**
Make sure all application nodes show 4 or 6 nodes.	**cluster check**
	inspect the output of this command, for warnings and errors. You can also use **cluster check verbose** to see more details.

continues on next page

Table 1 – continued from previous page

Description	Steps
	Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
	Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
	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).
Upgrade steps	**Upgrade steps**
==========	==========
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	
Verify that the ISO has been uploaded to the 'media/' directory on each node. This will speed up the upgrade time.	
On the primary unified node:	**screen**
	cluster upgrade media/<upgrade_iso_file>
Note: The **cluster upgrade** command will also silently first run **cluster check** and the upgrade will fail if any error conditions exist.	
Note: A check for security updates will also be made, with message 'Checking for security updates . . . '. If updates are found, a message will show the number and carry out the update. If no updates are found, a message 'No security updates found' shows.	
Note: If the system reboots, do not carry out the next manual reboot step. When upgrading from pre-19.1.1, an automatic reboot should be expected.	
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.	
Post-Upgrade, Security and Health Steps	**Post-Upgrade, Security and Health Steps**
==========	==========
On the primary unified node, verify the cluster status:	**cluster check**

continues on next page

Table 1 – continued from previous page

Description	Steps
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**
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.	
Database Filesystem Conversion Steps	**Database Filesystem Conversion Steps**
**********	**********
Shut down all the nodes. Since all services will be stopped this takes some time.	**cluster run all system shutdown**
	Create a restore point as per the guidelines for the infrastructure on which the VOSS-4-UC platform is deployed - in the case of a conversion error.
Database Schema Upgrade steps	**Database Schema Upgrade steps**
**********	**********
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	On the primary unified node: **screen**
	voss upgrade_db
Check cluster status	**cluster check**
Template Upgrade steps	**Template Upgrade steps**
**********	**********
It is recommended that the upgrade steps are run in a terminal opened with the **screen** command.	On the primary unified node: **screen**
	app template media/<VOSS-4-UC.template>
	Review the output from the **app template** command and confirm that the upgrade message appears.

continues on next page

Table 1 – continued from previous page

Description	Steps
	If no errors are indicated: make a backup or create a restore point as per the guidelines for the infrastructure on which the VOSS-4-UC platform is deployed. This restore point can be used if post-upgrade patches that may be required, fail.
For an unsupported upgrade path: the install script stops with the message:	
Upgrade failed due to unsupported upgrade path. Please log in as sysadmin and see Transaction logs for more detail.	You can restore to the backup or rollback, i.e. revert to the restore point made before the upgrade.
If there are errors for another reason: the install script stops with a failure message listing the problem.	Contact VOSS support.
Verify the 'extra_functions' have the *same checksum* across the cluster.	**cluster run application voss get_extra_functions_version -c**
Post upgrade migrations:	On a single node of a cluster: run: **voss post-upgrade-migrations**
Check cluster status and health	**cluster status**
Post Template Upgrade steps	**Post Template Upgrade steps**
**********	**********
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.
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	

continues on next page

Table 1 – continued from previous page

Description	Steps
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 Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded.
	Release should show 'XXX', where this matches the upgrade release.
	Check themes on all roles are set correctly
	For configurations that make use of the Northbound Billing Integration (NBI): please check the service status of NBI and restart if necessary.
Restore Schedules	**Restore Schedules**
==========	==========
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 Admin Portal 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.

continues on next page

Table 1 – continued from previous page

Description	Steps
	2. Import the bulk load sheet.
Schedules enabled on the CLI:	1. For disabled schedules that were overlapping the maintenance window, enable.
	Run **schedule enable <job-name>**.
Release Specific Updates	**Release Specific Updates**
==================================	==================================
Re-import the following from all CUCM devices:	
CUCM models:	device/cucm/PhoneType
For steps to create a custom data sync: refer to the chapter on Data Sync in the Core Feature Guide.	
Note: This is a once off data migration step. If this was performed previously when upgrading to 19.1.x then it does not have to be repeated.	
User Management migration updates default authentication types on SSO Identity Providers. If an SSO Identity Provider exists at the provider hierarchy level - default authentication settings:	
Authentication Scope: Current hierarchy level and below	
User Sync Type: All users	
Will not allow any non-SSO user logins (typically local administrators). The solution is to log in as higher level administrator account (full access) and set the SSO Identity Provider:	Authentication Scope: Current hierarchy level only
	User Sync Type: LDAP synced users only
Please refer to the SSO Identity Provider: Field Reference topic in the *Core Feature Guide*.	
Users of Microsoft apps	
	When upgrading to release 21.3, after upgrading, users of Microsoft apps should 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.

continues on next page

Table 1 – continued from previous page

Description	Steps
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**
Log Files and Error Checks	**Log Files and Error Checks**
==========	==========
Inspect the output of the command line interface for upgrade errors - for example: File import failed! or Failed to execute command.	
To view any log files indicated in the error messages - for example run the command if the following message appears:	**log view**
For more information refer to the execution log file with log view platform/execute.log	
If it is for example 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 Admin Portal as system level administrator	Go to **Administration Tools > Transaction** and inspect the transactions list for errors

Index

A

app
    app cleanup, 7, 24, 37
    app template, 5

C

cluster
    cluster check, 7, 24
    cluster provision, 5
    cluster upgrade, 5, 7, 24

D

database
    database convert_drive, 7, 24, 37

S

screen, 5, 7, 24, 37

V

voss
    voss post-upgrade-migrations, 37
    voss upgrade_db, 5
voss export
    voss export group, 5
    voss export type, 5
voss subscriber_data_export, 5