VOSS-4-UC
Upgrade Guide with Delta Bundle

Release 19.3.2

Aug 20, 2020

Legal Information

Please take careful note of the following legal notices:

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

Important:

- 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`
  - 19.3.1 - `/software/patches/19.3.1/Recommended_Patches/EKB-3853-19.3.1_patch`
- When upgrading to 19.3.2, first obtain and apply the patch from one of the following:
  - VOSS secure FTP site:

    `/software/patches/19.3.2/Pre Upgrade Patches/EKB-4769_patch`
  - Customer Portal:

    `/downloads/VOSS-4-UC/19.3.2/Patches/Pre Upgrade Patches/EKB-4769_patch`

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

1 Multinode Upgrade

1.1. Upgrade a Multinode Environment with the Delta Bundle

Note:

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

From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, the standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

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

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

The version of **screen** used in VOSS-4-UC 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

1.1.1. Download Files and Check

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

1.1.2. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	
Run template customization audits at the `sys` and `sys.hcs` hierarchy levels to identify template definitions and instances that were not delivered in the standard template packages during an installation or upgrade. The audit report includes custom model schema definitions as well as data, domain, and view instances created on the hierarchy node as a result of workflow execution. If the release is accompanied by Upgrade Notes, refer to the details. 1. Log in as an administrator above Provider level that has access to the hierarchies. 2. Choose **Administration Tools > Reports > Audit Template Customization**. 3. Choose the hierarchy node for which you want to audit customized templates. 4. Click **Save**. View the audit report: 5. Choose **Administration Tools > Reports > Template Customization Reports**. A list of template customization audit reports is displayed. 6. Click a report to view the details. The message field shows how many customized templates were found at the hierarchy node. The details fields lists the model type and instance of each customized template.	

1.1.3. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet.	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as “Processing” and then choose each **Action** that starts with “Import”, for example, “Import Unity Connection”. b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	
Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

1.1.4. Pre-Upgrade, Security and Health Steps

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.
On the Primary Unified Node, verify cluster connectivity:
• **cluster status**
On each node verify network connectivity, disk status and NTP.
• **cluster check**
If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/ (call support if over 80%)`
`/var/log (run: log purge)`
`/opt/platform (remove any unnecessary files from /media directory)`
`/tmp (reboot)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes:
• **cluster run all security check**	

Shutdown servers and take snapshots from VMWare and then power on all servers, starting with the primary: Use VMware snapshots. Consider the following: • VOSS cannot guarantee that a VMware snapshot can be used to successfully restore VOSS-4-UC or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application. • When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space. • **cluster run notme system shutdown –force && system shutdown –force** Log into VMWare and take snapshots of all unified nodes and all web proxies. After snapshots, restart the servers: • Power up the servers via VMWare. Optional: If a backup is required in addition to the snapshot, 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, nodes and weights for the cluster:
Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
• **cluster run all app status**
Make sure all application nodes show 3 or 5 nodes.
• **cluster run application cluster list**
Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
• **cluster run application database weight list**
Example output:
`172.29.21.240:`
`  weight: 80`
`172.29.21.241:`
`  weight: 70`
`172.29.21.243:`
`  weight: 60`
`172.29.21.244:`
`  weight: 50`
Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:
• **database config**	

1.1.5. Upgrade

Description and Steps	Notes and Status
On the primary unified node: • **screen** Run (optionally with command parameters below): • **app install media/<script_file> delete-on-success yes –force** From release 19.1.2 and later, the `delete-on-success` parameter and `yes` or `no` value have been added to remove or keep the the script file in the `media/` directory after successful installation.	

1.1.6. Post-Upgrade, Security and Health Steps

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

1.1.7. Database Filesystem Conversion

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:

1. Run **database config** and ensure that the storage engine for *all database nodes* shows as `storageEngine: WiredTiger`.
2. Run **drives list** and ensure that the LVM storage shows for *all converted database nodes* under `Volume Groups`.

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.

For the Database Filesystem Conversion step below, *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 there is 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.

Note: The **database convert_drive** command can also be run on a single node only by running the following command and parameter from the specific node: **database convert_drive standalone**. This option can for example be used for performance reasons in cases where a node is in a remote location.

Topology	Window 1	Window 2	Window 3	Commands (DC = valid data center name)	Description
multinode	Y			**database convert_drive secondary all** **database convert_drive primary**	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.
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.

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 notme system shutdown –force && system shutdown –force**
Create a VMWare snapshot for all the unified servers so that the system can easily be reverted in the case of a conversion error. Boot all the systems in VMWare.
• 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 converted 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`	

1.1.8. Post Template Upgrade Tasks

Description and Steps	Notes and Status
Verify the upgrade: Log in on the GUI and check the information contained in the **About > Extended Version** menu. Confirm that versions have upgraded: • **Release** should show 19.3.2 • **Platform Version** should show 19.3.2 If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.	

1.1.9. Restore Adaptations

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

1.1.10. Restore Schedules

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet.	

1.1.11. Log Files and Error Checks

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

1.2. Upgrading from VOSS-4-UC 18.1.3 to 19.3.2

Note:

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

  You can follow the progress on the GUI transaction list.

- The `screen` command can be used - see: *Notes on the screen command*

The upgrade process is in two stages:

1. *18.3.1 to 19.2.1 ISO Upgrade*
2. *19.2.1 to 19.3.2 Delta Bundle Upgrade*

Important: The process in this document only applies for the *full* upgrade from 18.3.1 to 19.3.2, and cannot be used for the upgrade to intermediate versions. Refer to the upgrade documents accompanying individual releases for intermediate version upgrades.

Note:

- For each stage, the required upgrade files need to be downloaded.
- A database filesystem conversion is required during the second, delta bundle upgrade.

1.2.1. 18.3.1 to 19.2.1 ISO Upgrade

Upgrade a Multinode Environment with the ISO and Template

Note:

- 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.

Download Files and Check

Description and Steps	Notes and Status

VOSS SFTP server: `secure.voss-solutions.com`
Download:
• `platform-install-19.2.1-1570776653.iso` and
• `V4UC-19.2.1.280-build-14.template` from the VOSS SFTP server.
• Transfer the `.iso` file to the `media/` folder of the primary node.
• 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: <ISO SHA256>`
• **system checksum media/<upgrade_template_file>**
`Checksum: <Template SHA256>`
See values below.	

- ISO SHA256: `b2d1c5df04d0791d0de3d8d4aa2b3d1d9b62ea1d1df3bd61967a0dfa7836f985`
- Template SHA256: `249fd0b1d797fdbebba03c136211ae1f7a79ea309f3049546b0152698586f9fa`

Schedules, Transactions and Version Check

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet.	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as "Processing" and then choose each **Action** that starts with "Import", for example, "Import Unity Connection". b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	

Record the current version information. This is required for upgrade troubleshooting.
• Log in on the GUI and record the information contained in the **About > Extended Version**
`Release 18.1.75`
`Platform 11.5.3-1521045619`
`Version 116.0`
`Build no 1558`	

Pre-Upgrade, Security and Health Steps

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. On the Primary Unified Node, verify cluster connectivity and health:
• **cluster status**
• From VOSS-4-UC 19.1.1 onwards:
cluster check
• Prior to VOSS-4-UC 19.1.1:
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)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes:
• **cluster run all security check**	

Shutdown servers and take snapshots from VMWare and then start all servers: Use VMware snapshots. Consider the following: • VOSS cannot guarantee that a VMware snapshot can be used to successfully restore VOSS-4-UC or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application. • When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space. • **cluster run notme system shutdown** followed by: **system shutdown** Log into VMWare and take snapshots of all unified nodes and all web proxies. After snapshots, restart the servers: • Power up the servers via VMWare. Optional: If a backup is required in addition to the snapshot, 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, nodes and weights for the cluster:
Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
• **cluster run all app status**
Make sure all application nodes show 3 or 5 nodes.
• **cluster run application cluster list**
Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
• **cluster run application database weight list**
Example output:
`172.29.21.240:`
`  weight: 80`
`172.29.21.241:`
`  weight: 70`
`172.29.21.243:`
`  weight: 60`
`172.29.21.244:`
`  weight: 50`
Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:
• **database config**	

Upgrade

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. For backwards compatibility, this command is the same as for example **cluster upgrade <upgrade_iso_file> backup none fast**.

Use the **cluster upgrade <upgrade_iso_file> serial** command if the VMware host is under load.

Description and Steps	Notes and Status
From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, it is recommended that the upgrade steps are run in a terminal opened with the **screen** command and to use a log file. See: *Notes on the screen command*. On the primary unified node: • **screen** • **cluster upgrade media/<upgrade_iso_file>**	

Post-Upgrade, Security and Health Steps

Description and Steps	Notes and Status
On the primary unified node, verify the cluster status: • **cluster status** • From VOSS-4-UC 19.1.1 onwards, also run: **cluster check** • If any of the above commands show errors, check for further details to assist with troubleshooting: **cluster run all diag health**	
If upgrade is successful, the screen session can be closed by typing **exit** in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.	
Complete all the security updates. • **cluster run all security update** 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 security updates needed to be applied*: • **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 Schema Upgrade

Description and Steps	Notes and Status
From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, 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** Append `--force` for no prompt or type `y` for yes to confirm this command. Check cluster status • **cluster status**	

Template Upgrade

Description and Steps	Notes and Status
From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, 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>**	

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. 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, make a backup or snapshot.	

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 revert to the VM snapshot 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** 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-4-UC and its progress is displayed as it executes.	

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

Post Template Upgrade Tasks

Description and Steps	Notes and Status
Verify the upgrade: Log in on the GUI and check the information contained in the **About > Extended Version** menu. Confirm that versions have upgraded. • **Release** should show 19.2.1 • **Platform Version** should show 19.2.1	
• Check themes on all roles are set correctly	

Release Specific Updates

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-4-UC 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.	
On VOSS-4-UC 18.1, an enhancement populates the E164 Inventory field on Directory Numbers (DNs) when associating E164 numbers to DNs. In order to populate the E164 field for existing associations, please execute the workflow: `FixINIPostUpgradePWF`. This will populate the E164 Field on the DN. To run the workflow, login with `tdkadmin`, select the hierarchy to run the workflow at, e.g. Provider, and then execute the workflow. This can be run at lower hierarchy levels as well for a phased migration approach, e.g. at Customer level. The task can be performed by partners who have access to the `tdkadmin` user account. Alternatively, contact your VOSS Account Manager/Support representative for assistance. Usage: Select the desired hierarchy, find and Execute the workflow named `FixINIPostUpgradePWF`.	

Log Files and Error Checks

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

1.2.2. 19.2.1 to 19.3.2 Delta Bundle Upgrade

Upgrade a Multinode Environment with the Delta Bundle

Download Files and Check

- Bundle SHA256: `01c06d4b6c3abf9f6fc45339aa4fbd59431bb38a1a37368cc1f2132d50b295c3`

Version Check

Description and Steps	Notes and Status
Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

Pre-Upgrade, Security and Health Steps

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.
On the Primary Unified Node, verify cluster connectivity:
• **cluster status**
On each node verify network connectivity, disk status and NTP.
• **cluster check**
If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:
`/ (call support if over 80%)`
`/var/log (run: log purge)`
`/opt/platform (remove any unnecessary files from /media directory)`
`/tmp (reboot)`
On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes:
• **cluster run all security check**	

Shutdown servers and take snapshots from VMWare and then power on all servers, starting with the primary: Use VMware snapshots. Consider the following: • VOSS cannot guarantee that a VMware snapshot can be used to successfully restore VOSS-4-UC or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application. • When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space. • **cluster run notme system shutdown –force && system shutdown –force** Log into VMWare and take snapshots of all unified nodes and all web proxies. After snapshots, restart the servers: • Power up the servers via VMWare. Optional: If a backup is required in addition to the snapshot, 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, nodes and weights for the cluster:
Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
• **cluster run all app status**
Make sure all application nodes show 3 or 5 nodes.
• **cluster run application cluster list**
Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster.
• **cluster run application database weight list**
Example output:
`172.29.21.240:`
`  weight: 80`
`172.29.21.241:`
`  weight: 70`
`172.29.21.243:`
`  weight: 60`
`172.29.21.244:`
`  weight: 50`
Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:
• **database config**	

Upgrade

Description and Steps	Notes and Status
On the primary unified node, use `screen` and a log file - see: *Notes on the screen command*. • **screen** Run (optionally with command parameters below): • **app install media/<script_file>**	

Post-Upgrade, Security and Health Steps

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

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:

1. Run **database config** and ensure that the storage engine for *all database nodes* shows as `storageEngine: WiredTiger`.
2. Run **drives list** and ensure that the LVM storage shows for *all converted database nodes* under `Volume Groups`.

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.

For the Database Filesystem Conversion step below, *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 there is 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.

Note: The **database convert_drive** command can also be run on a single node only by running the following command and parameter from the specific node: **database convert_drive standalone**. This option can for example be used for performance reasons in cases where a node is in a remote location.

Topology	Window 1	Window 2	Window 3	Commands (DC = valid data center name)	Description
multinode	Y			**database convert_drive secondary all** **database convert_drive primary**	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.
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.

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 notme system shutdown –force && system shutdown –force**
Create a VMWare snapshot for all the unified servers so that the system can easily be reverted in the case of a conversion error. Boot all the systems in VMWare.
• 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 converted 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`	

Post Template Upgrade Tasks

Description and Steps	Notes and Status
Verify the upgrade: Log in on the GUI and check the information contained in the **About > Extended Version** menu. Confirm that versions have upgraded: • **Release** should show 19.3.2 • **Platform Version** should show 19.3.2 If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again.	

Restore Schedules

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet.	

Phone Based Registration Feature Installation (Optional)

Description and Steps	Notes and Status

If the phone based registration feature is required, you will need to download the latest Phone Based Registration install script to all unified nodes before continuing with the installation steps below in order to install the latest version.
The required files can be located on the secure downloads server under:
`/software/voss4uc/releases/Release-19.3.2/pbr`
Refer to the accompanying document *MOP-PBR-19.3.2.pdf*.
Note that a full service restart is initiated on initial startup of the PBR web service on each VOSS-4-UC unified node.
Verify the downloaded script:
`phone-based-registration_install-19.3.2.script`
with the accompanying SHA256 file:
`phone-based-registration_install-19.3.2.script.sha256`
• *On a cluster*:
1. Run the following command on all unified nodes in serial:
`app install media/phone-based-registration_install-19.3.2.script --force`
2. Run the following command on the primary node:
`cluster provision --force`
• *On a standalone system*:
1. Run the following command on the unified node:
`app install media/phone-based-registration_install-19.3.2.script --force`
2. Run the following command:
`system provision --force`
The PBR web service is assigned the same web weights as the `selfservice` and `voss-deviceapi` service. For example, when running **web weight list** from a web proxy, the output should be similar to the example below:
`platform@VOSS-WP-1:~$ web weight list`
`Default service weights`
`upstreamservers:`
`phonebasedreg:`
`phoneservices:`
`192.168.100.10:443: 0`
`192.168.100.3:443: 1`
`192.168.100.4:443: 1`
`192.168.100.5:443: 1`
`192.168.100.6:443: 1`
`192.168.100.9:443: 0`
`voss-deviceapi:`
`selfservice:`
`192.168.100.10:443: 0`
`192.168.100.3:443: 1`
`192.168.100.4:443: 1`
`192.168.100.5:443: 1`
`192.168.100.6:443: 1`
`192.168.100.9:443: 0`
`voss-deviceapi:`
`192.168.100.10:443: 0`
`192.168.100.3:443: 1`
`192.168.100.4:443: 1`
`192.168.100.5:443: 1`
`192.168.100.6:443: 1`
`192.168.100.9:443: 0`	

Log Files and Error Checks

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

1.3. Notes on the screen command

From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, the standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

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

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

The version of **screen** used in VOSS-4-UC 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

2 Standalone Upgrade

2.1. Upgrade a Standalone Environment with the Delta Bundle

Note:

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

From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, the standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

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

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

The version of **screen** used in VOSS-4-UC 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

2.1.1. Download Files and Check

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

2.1.2. Adaptations Check

Description and Steps	Notes and Status
Identify installed adaptations and determine any effect on the upgrade plan. If the release is accompanied by Upgrade Notes, refer to the details.	
Run template customization audits at the `sys` and `sys.hcs` hierarchy levels to identify template definitions and instances that were not delivered in the standard template packages during an installation or upgrade. The audit report includes custom model schema definitions as well as data, domain, and view instances created on the hierarchy node as a result of workflow execution. If the release is accompanied by Upgrade Notes, refer to the details. 1. Log in as an administrator above Provider level that has access to the hierarchies. 2. Choose **Administration Tools > Reports > Audit Template Customization**. 3. Choose the hierarchy node for which you want to audit customized templates. 4. Click **Save**. View the audit report: 5. Choose **Administration Tools > Reports > Template Customization Reports**. A list of template customization audit reports is displayed. 6. Click a report to view the details. The message field shows how many customized templates were found at the hierarchy node. The details fields lists the model type and instance of each customized template. Record and / or export the report details so that any adaptations to models can be restored during the post-upgrade steps.	

2.1.3. Schedules, Transactions and Version Check

Description and Steps	Notes and Status
Turn off any scheduled imports to prevent syncs triggering part way through the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box. Mass modify: 1. On the GUI, export scheduled syncs into a bulk load sheet. 2. Modify the schedule settings to de-activate scheduled syncs. 3. Import the sheet.	
Check for running imports. Either wait for them to complete or cancel them: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Transaction** menu to view transactions. 3. Filter the **Action** column: a. Choose **Status** as “Processing” and then choose each **Action** that starts with “Import”, for example, “Import Unity Connection”. b. Click **Search** and confirm there are no results. c. If there are transactions to cancel, select them and click **Cancel**.	
Record the current version information. This is required for upgrade troubleshooting. • Log in on the GUI and record the information contained in the **About > Extended Version**	

2.1.4. Pre-Upgrade, Security and Health Steps

Description and Steps	Notes and Status

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

Shutdown server and take snapshots from VMWare and then restart server: Use VMware snapshots. Consider the following; • VOSS cannot guarantee that a VMware snapshot can be used to successfully restore VOSS-4-UC or any Cisco HCS Management application. If you cannot restore the application from a snapshot, your only recourse is to reinstall the application. • When the backup is complete and you do not need the VMware snapshot for restore activities, delete the snapshot immediately to preserve LUN space. • **system shutdown** Log into VMWare and take a snapshot. After the snapshot, restart: • Power up the servers via VMWare. Optional: If a backup is required in addition to the snapshot, 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**	

2.1.5. Upgrade

Description and Steps	Notes and Status
From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, it is recommended that the upgrade steps are run in a terminal opened with the **screen** command. • **screen** Run (optionally with command parameters below): • **app install media/<script_file> delete-on-success yes –force** From release 19.1.2 and later, the `delete-on-success` parameter and `yes` or `no` value have been added to remove or keep the the patch file in the `media/` directory after successful installation.	

2.1.6. Post-Upgrade, Security and Health Steps

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

2.1.7. Database Filesystem Conversion

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:

1. Run **database config** and ensure that the storage engine shows as `storageEngine: WiredTiger`.
2. Run **drives list** and ensure that the LVM storage shows for the converted database node under `Volume Groups`.

The **database convert_drive** command provides parameters allows 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 standalone 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 VMWare snapshot so that the system can easily be reverted in the case of a conversion error. Boot the system in VMWare. Stop transactions from being scheduled. Run:
• **database convert_drive standalone**
Note: this step may take a while. 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 shows for the *database node* 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`	

2.1.8. Post Template Upgrade Tasks

Description and Steps	Notes and Status
Verify the upgrade: Log in on the GUI and check the information contained in the **About > Extended Version** menu. Confirm that versions have upgraded. • **Release** should show 19.3.2 • **Platform Version** should show 19.3.2 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	

2.1.9. Restore Adaptations

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

2.1.10. Restore Schedules

Description and Steps	Notes and Status
Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available: Individually for each job: 1. Log in on the GUI as a high level administrator above Provider level. 2. Select the **Scheduling** menu to view scheduled jobs. 3. Click each scheduled job. On the Base tab, check the **Activate** check box. Mass modify: 1. Modify the exported sheet of schedules to activate scheduled syncs. 2. Import the bulk load sheet.	

2.1.11. Log Files and Error Checks

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

Index