



The TRELLIS™ Real-Time Infrastructure Optimization Platform

Administrator's Guide

For Microsoft Windows

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit <https://www.vertiv.com/en-us/support/> for additional assistance.

TABLE OF CONTENTS

1 Overview	1
2 TRELLIS™ Platform BackUp, Restore and Upgrade	3
2.1 Cold Backup	3
2.1.1 Back machine files and folder	4
2.1.2 Front machine files and folders	5
2.2 Cold Restore	7
2.3 License Server Reset and Reinstall Version 4.0 to 4.0.3	8
2.4 License Server Reset and Reinstall Version 5.0.1 to 5.06	10
2.5 RMAN Backup and Recovery Tool	12
2.5.1 Incremental backups	12
2.5.2 Oracle database configuration	12
2.5.3 Host server file backup	12
2.5.4 Tool configuration	13
2.5.5 Fast Recovery Area size	13
2.5.6 Fast Recovery Area location	14
2.5.7 Reports	14
2.5.8 Modify the backup schedule	15
2.5.9 Restore	16
2.5.10 Database threshold notification	16
2.5.11 Running an RMAN backup	17
2.6 Platform Upgrade	17
2.6.1 Version 4.0.0 upgrade	18
2.6.2 Version 4.0.2 upgrade	19
2.6.3 Version 4.0.3 upgrade	21
2.6.4 Version 5.0.1 upgrade	23
2.6.5 Version 5.0.1.2 upgrade	25
2.6.6 Version 5.0.2 upgrade	31
2.6.7 Version 5.0.3 upgrade	33
2.6.8 Version 5.0.4 and higher upgrade	36
3 TRELLIS™ Intelligence Engine BackUp, Restore and Upgrade	39
3.1 Back Up via the Platform	39
3.2 Back Up via Command Line	40
3.3 Restore	40
3.4 Trellis™ Intelligence Engine Upgrade	41
3.4.1 Upgrade history	42
4 Embedded Intelligence Engine BackUp and Restore	43
4.1 Manual Backup	43
4.2 Automated Backup	44

4.3 Appliance and Embedded Intelligence Engine Restore45

4.4 Embedded Intelligence Engine Restore45

5 Replacing Certificates47

1 OVERVIEW

The *Trellis*™ Real-Time Infrastructure Optimization Platform and the *Trellis*™ Intelligence Engine data collection engine may require a backup to restore a current or new system. This document provides procedures to back up, restore and upgrade the *Trellis*™ platform database and the Avocent® Intelligence Engine that is embedded in the Avocent® Universal Management Gateway appliance. Additional instructions are provided to restore the Avocent® Universal Management Gateway appliance.

An administrator who has experience with Microsoft® Windows® commands, can perform the backup and restore procedures. If you are restoring to a new system, the operating system (OS) and the *Trellis*™ platform version must be the same as in the existing system and the same internal files and directories must exist in both systems after the restoration is complete.

NOTE: This section describes how to back up and restore the *Trellis*™ platform software, version 3.4 and higher.

The following tools can be used to back up and restore the system:

- The *Trellis*™ platform cold backup and restore procedure enables you to create backups of all of the *Trellis*™ platform and the operating system files in order to restore all of the platform contents on a new server.
- The *Trellis*™ platform backup and recovery tool - RMAN provides a continuous incremental hot backup of the platform database, a backup of all schema, including *Trellis* platform users, and allows a platform restore to a point in time.

For information about upgrading the platform, see [Platform Upgrade](#) on page 17.

The following table defines the most common terms that are used in this document.

Table 1.1 Common Terms

TERM	DESCRIPTION
Fast Recovery Area (FRA)	Provides a centralized disk location for backup and recovery files; stores all of the files needed to completely recover a database.
Recovery Manager (RMAN)	Primary tool for the physical backup and recovery of an Oracle database.
Block Change Tracking (BCT)	When enabled, the database backup and recovery tool uses a tracking file to identify changed blocks for incremental backups. Using this file avoids the tool having to scan every block in the data file.
DB_RECOVERY_FILE_DEST	Backups are stored in this fully qualified path.
Archive log mode	Database mode enables archiving of the online redo log.
Online redo log	Includes two or more online redo log files that record all changes made to the Oracle database data and control files.

This page intentionally left blank

2 TRELLIS™ PLATFORM BACKUP, RESTORE AND UPGRADE

This section provides the backup, restore and upgrade procedures for the *Trellis*™ platform.

NOTE: Some entries in the following procedures apply for software versions 4.0 - 4.0.3 or version 5.0.1 and higher. Always identify which version you are upgrading prior to initiating a procedure.

2.1 Cold Backup

The cold backup process enables you to create backups of all the *Trellis*™ platform and Windows® operating system files in order to restore the platform onto a new server.

NOTE: Starting with *Trellis* platform version 5.0, the Vertiv™ license server is used instead of the Emerson license server.

To create a cold backup:

1. As administrator on the front and back machines, enter the following at the command prompt to stop the machine:

```
C:\u01\trellis\trellis.bat stop
```

2. On the front machine, enter the following to stop the Node Manager service:

```
sc stop "Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)"
```

NOTE: The service can also be stopped via Services.msc.

3. On the back machine, enter the following to stop the database:

```
sc stop "OracleServiceORCL"
```

NOTE: The service can also be stopped via Services.msc.

4. Enter one of the following to stop the license server on the back machine:
 - Version 4.0 to 4.0.3: **sc stop "ServedLicenseInterface"**
 - Versions 5.0.1 to 5.0.4: **Run Services.msc**, navigate to the Served License Interface Service and stop the service
 - For versions 5.1 and higher, the license server does not exist.
5. After the backup completes, enter the following to reboot the operating system servers for the back and front machines:

```
sc start "Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)"
```

NOTE: The Node Manager, License Server and Oracle database services are automatically started with the operating system.

NOTE: The service can also be started via Services.msc.

6. For versions 5.1 and higher, the back machine automatically starts. For versions prior to 5.1, on the back machine, enter **C:\u01\trellis\trellis.bat start** to start the platform.
7. On the front machine, enter **C:\u01\trellis\trellis.bat start** to start the platform.

2.1.1 Back machine files and folder

As administrator, back up and restore the following directories and files from the back machine. Because systems may have different configurations, test each instance.

NOTE: The following list is a guideline.

Table 2.1 Back Machine Files and Directories

DIRECTORIES	FILES
C:\u01	C:\users\Administrator\TrellisConfiguration.zip
C:\u02	C:\users\Administrator\TrellisScript.zip
C:\u03	N/A
C:\bea	N/A
C:\users\Administrator\oracle	N/A
C:\Program Files\Oracle	N/A
C:\Program Files\EmersonNetworkPower	N/A

To export registry files:

1. Select *Run* and enter **regedit** to open the Windows registry.
2. Export the following platform-related entries to create a separate .reg file for each export.
 - HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\ServedLicenseInterface
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\beasvc
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle.orcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle12
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleDBConsoleorcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\OracleDBConsoleorcl
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleJobSchedulerORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleMTSRecoveryService
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleOraDb12g_home1TNSListener
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleOraDb12g_home1ClrAgent
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleVssWriterORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_asinst_1
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle Services for MTS
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleServiceORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Oracle.VSSWriter.ORCL
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\beasvc
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleDBConsoleorcl

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle11
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleOraDb12g_home1ClrAgent
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleOraDb12g_home1TNSListener
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleJobSchedulerORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleMTSRecoveryService
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_asinst_1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleServiceORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleVssWriterORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SCM
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle.orcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle Services for MTS
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\Oracle.VSSWriter.ORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\beasvc
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
- HKEY_CURRENT_USER\Software\JavaSoft
- HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBCINST.INI\Oracle in OraDb12g_home1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle.orcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle12
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleOraDb12g_home1ClrAgent
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleOraDb12g_home1TNSListener
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\OracleDBConsoleorcl
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleJobSchedulerORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleMTSRecoveryService
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_asinst_1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle Services for MTS
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleVssWriterORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\eventlog\Application\Oracle.VSSWriter.ORCL
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleServiceORCL

2.1.2 Front machine files and folders

As administrator, back up and restore the following directories and files from the front machine. Because systems may have different configurations, test each instance.

NOTE: The Robocopy or Xcopy command-line tool can be used when replicating files.

Table 2.2 Front Machine Files and Directories

DIRECTORIES	FILES
C:\u01	C:\users\Administrator\TrellisConfiguration.zip
C:\u02	C:\users\Administrator\TrellisScript.zip
C:\u03	N/A
C:\bea	N/A
C:\users\Administrator\oracle	N/A
C:\Program Files\Oracle	N/A

The Administrator role must first be assigned ownership of the password in order to copy the command to a remote backup destination.

To set the Administrator as the owner of the jmxremote.password file:

1. As administrator, navigate to `C:\u02\domains\<Trellis domain>\config` and execute the following command:
takeown /f C:\u02\domains\<Trellis domain>\config\jmxremote.password
2. Wait for the response SUCCESS: The file (or folder): "C:\u02\domains\<Trellis domain>\config\jmxremote.password" is now owned by the user "HSV-STR-20207\Administrator."

NOTE: In this example, HSV-STR-20207 is the service account name you provide.

3. After `C:\u02\domains\<Trellis domain>\config`, execute the following command to grant the administrator access to the jmxremote.password file:

icacls C:\u02\domains\<Trellis domain>\config\jmxremote.password /grant administrator:F

NOTE: In this example, administrator:F is the service account name you provide.

4. Wait for one of the following responses:
 - Processed file: C:\u02\domains\<Trellis domain>\config\jmxremote.password
 - Successfully processed 1 files; Failed processing 0 files
5. Copy the C:\U02 directory to the remote backup location.

To export the registry files:

1. Select *Run* and enter **regedit** to open the Windows registry.
2. Export the following platform-related entries to create a separate .reg file for each export.
 - HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\Application\beasvc
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\Oracle WebLogic NodeManager
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_osbproxy01
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\services\OracleProcessManager_ui01
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_osbproxy01
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleProcessManager_ui01
 - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Oracle WebLogic NodeManager (C_u01_fm_11.1.1.7_wlserver_10.3)

- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_osbproxy01
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\OracleProcessManager_ui01

NOTE: If a permission error displays when copying the `c:\u02\domains\<DomainName>\config\jmxremort.password` file, make sure the file has administration privileges and re-copy the file. After copying the file remove all the privileges.

2.2 Cold Restore

After the cold backup process is complete, you can perform the following cold restore procedure. The new instance configuration is a replica of the original failed instance. Changing the IP addresses, hosts names or other configurations is not supported.



WARNING! The *Trellis™* platform must be re-licensed after a restore. Contact Technical Support for assistance.

To restore from a cold backup:

1. As administrator, provision the front and back machines using the appropriate Windows® OS version with all pre-requisites.
2. Configure the front and back machines with pre-installation steps as a replica of the original systems.
3. On the back machine, restore all the files and folders mentioned in [Cold Backup](#) on page 3.
4. On the front machine, restore all the files and folders mentioned in [Cold Backup](#) on page 3.
 - a. As administrator, execute the following command to set the SYSTEM as the owner of the `jmxremote.password` file:

```
icacls "C:\u02\domains\<Trellis domain>\config\jmxremote.password" /setowner "SYSTEM" /T /C
```

- b. Wait for one of the following responses:
 - Processed file: `jmxremote.password`
 - Successfully processed 1 files; Failed processing 0 files
- c. Execute the following command to revoke the administrator access to the `jmxremote.password` file:

```
C:\u02\domains\<Trellis domain>\config> icacls C:\u02\domains\<Trellis domain>\config\jmxremote.password /deny administrator:F
```

NOTE: In this example, `administrator:F` is the service account name you provide.

5. For restoring/importing the registry entries, double-click each exported registry and click Yes for the corresponding information on the front and back machines.
6. Reset the license server. See [License Server Reset and Reinstall Version 4.0 to 4.0.3](#) on page 8.
7. As administrator user on the back machine, enter the following to start the database:

```
c:\u01\trellis>sqlplus / as sysdba
```

```
SQL> startup
```

```
SQL>exit
```

8. Enter `lsnrctl start` to start the database listener.
9. Enter `lsnrctl status` to verify the db listener is up and running.
10. As administrator on the back machine, enter `\u01\trellis\trellis start` to start the platform.

11. As **oracle** on the front machine, enter `\u01\trellis\trellis` to start the platform.
12. If the front machine fails when starting, proceed as follows:
 - a. Remove all users and permissions from the `c:\u02\domains\<DomainName>\config\jmxremort.password` file.
 - b. On a Windows machine, create the **ora_dba** group and assign administrator user to the group to start the oracleORCL service.
 - c. Enter `C:\u01\trellis>trellis start` to start the back machine.

2.3 License Server Reset and Reinstall Version 4.0 to 4.0.3

After the restore is complete, the operating system license server detects the copy and breaks the trust store. You will need to reset the license server, reinstall the license server and then reissue a license. This process can take 30 minutes or more to complete.

NOTE: All licensing activation tasks are completed on the back machine.

NOTE: Starting with *Trellis*™ platform version 5.0.1, the Vertiv™ license server is used instead of the Emerson license server.

To reset the license server:

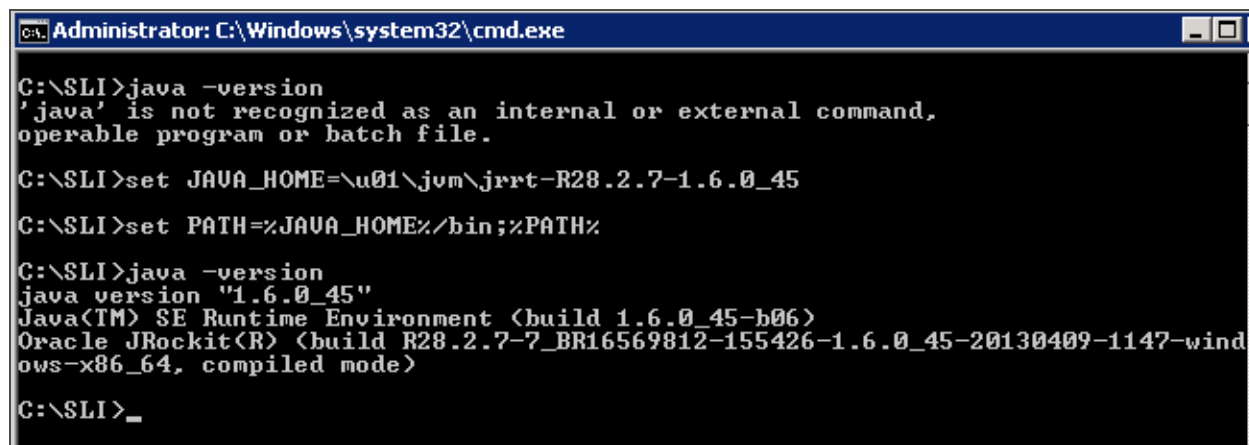
1. Before proceeding, ensure the platform software is not running.
2. As administrator, log into the back machine.
3. In Windows®, go to services and verify the license services are running.
4. If the services are not running, run **tsreset_svr.exe** to start the *Served License Interface* service.
5. From the command prompt, reset the license server in the `C:\Program Files\EmersonNetworkPower\ServedLicenseInterface` folder.
6. If the license server reset fails, follow the steps to reinstall the license server.

NOTE: If the license server reset is unsuccessful, you must reinstall the license server.

To reinstall the license server:

1. As administrator, go to the services and stop the Served License Interface service.
2. Create a directory on your C drive called `C:\SLI` and copy the license server **sli_windows_install64-1_0_1_50.exe** installer file to the back machine.
3. At a DOS prompt, go to the SLI directory and enter the following to set the correct Java version:
 - a. **set JAVA_HOME=\u01\jvm\jdk1.7.0_85**
 - b. **set PATH=%JAVA_HOME%\bin;%PATH%**
4. Enter **java -version** to verify the Java version. See the following screen.

Figure 2.1 Java Version Screen



```

Administrator: C:\Windows\system32\cmd.exe

C:\SLI>java -version
'java' is not recognized as an internal or external command,
operable program or batch file.

C:\SLI>set JAVA_HOME=\u01\jvm\jrrt-R28.2.7-1.6.0_45

C:\SLI>set PATH=%JAVA_HOME%\bin;%PATH%

C:\SLI>java -version
java version "1.6.0_45"
Java(TM) SE Runtime Environment (build 1.6.0_45-b06)
Oracle JRockit(R) (build R28.2.7-7_BR16569812-155426-1.6.0_45-20130409-1147-wind
ows-x86_64, compiled mode)

C:\SLI>_

```

5. From the DOS command prompt, in the SLI directory, run `sl_i_windows_install64-1_0_1_50.exe`.

-or-

Double-click the `SLI.exe` file to install the license server.

6. From the Windows services, verify the Served License Interface service is running.

-or-

If the service is not running, start it.

To reissue a license:

1. As administrator, generate the Request XML file from the following directory and save it to the request directory on the C drive. The following is an example of the command:

Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface):

```
serveractivationui.exe -activate a1a7-94e9-22a5-4867-8204 -quantity 10 -gen c:\requests\reqActivate_052302.xml
```

2. After the request.xml file is generated for all the files, send it to Technical Support. After you receive the Response XML files, save them to the response directory on C Drive.
3. Process the response files. For example,

Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface)

```
serveractivationui.exe -process c:\responses\response.xml
```

4. After the command is complete, the following message is displayed:

File activate_response.xml successfully processed

Refresh license client cache

Windows (C:\Program Files (x86)\EmersonNetworkPower\ServedLicenseInterface)

```
lmutil lmreread
```

5. After the command is complete, the following message is displayed:

Imutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved.

Imreread successful

NOTE: The licenses are returned during normal business hours. A 10-day emergency license can be provided and should be replaced with an official license within the 10-day period.

6. After the system is licensed, enter **serveractivationui.exe -showlocal** from
C:\ProgramFiles\EmersonNetworkPower\Served

LicenseInterface directory to verify the license is available through the license server.

2.4 License Server Reset and Reinstall Version 5.0.1 to 5.06

After the restore is complete, the operating system license server detects the copy and breaks the trust store. You will need to reset the license server, reinstall the license server and then reissue a license. This process can take 30 minutes or more to complete.

NOTE: All license activation tasks are completed on the back machine.

NOTE: Starting with *Trellis*™ platform version 5.0.1, the Vertiv™ license server is used instead of the Emerson license server.

NOTE: Starting with *Trellis*™ platform version 5.1, the Vertiv™ license server is no longer used.

To reset the license server:

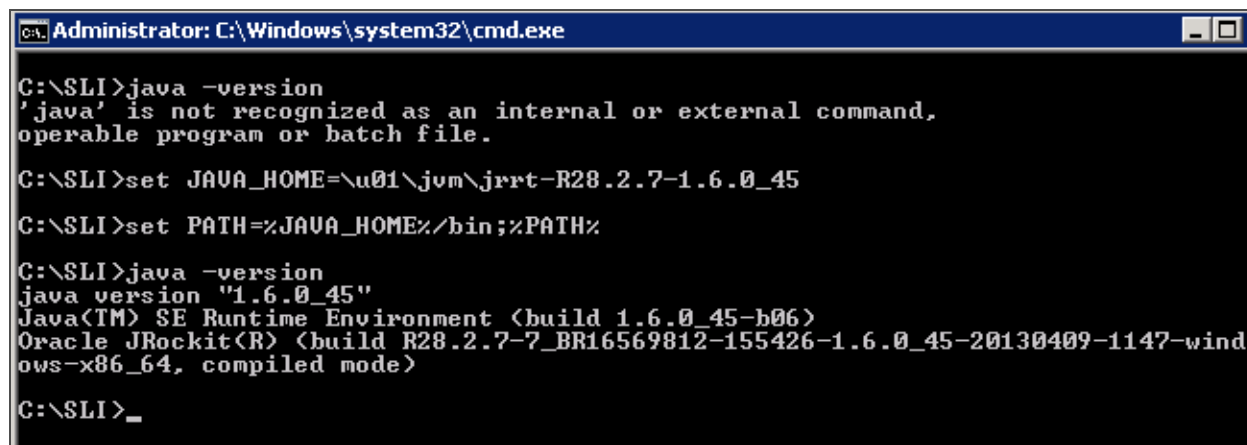
1. Before proceeding, ensure the platform software is not running.
2. As administrator, log into the back machine.
3. In Windows®, go to services and verify the license services are running.
4. If the services are not running, run **tsreset_svr.exe** to start the *Served License Interface* service.
5. From the command prompt, reset the license server in the **C:\Program Files\Vertiv\ServedLicenseInterface** folder.
6. If the license server reset fails, follow the steps to reinstall the license server.

NOTE: If the license server reset is unsuccessful, you must reinstall the license server.

To reinstall the license server:

1. As administrator, go to the services and stop the Served License Interface service.
2. Create a directory on your C drive called **C:\SLI** and copy the license server **sli_windows_install64-1_0_1_50.exe** installer file to the back machine.
3. At a DOS prompt, go to the SLI directory and enter the following to set the correct Java version:
 - a. **set JAVA_HOME=\u01jvm\jdk1.7.0_85**
 - b. **set PATH=%JAVA_HOME%\bin;%PATH%**
4. Enter **java -version** to verify the Java version. See the following screen.

Figure 2.2 Java Version Screen



```
Administrator: C:\Windows\system32\cmd.exe

C:\SLI>java -version
'java' is not recognized as an internal or external command,
operable program or batch file.

C:\SLI>set JAVA_HOME=\u01\jvm\jrrt-R28.2.7-1.6.0_45

C:\SLI>set PATH=%JAVA_HOME%\bin;%PATH%

C:\SLI>java -version
java version "1.6.0_45"
Java(TM) SE Runtime Environment (build 1.6.0_45-b06)
Oracle JRockit(R) (build R28.2.7-7_BR16569812-155426-1.6.0_45-20130409-1147-wind
ows-x86_64, compiled mode)

C:\SLI>_
```

5. From the DOS command prompt, in the SLI directory, run `sl_i_windows_install64-1_0_1_50.exe`.

-or-

Double-click the `SLI.exe` file to install the license server.

6. From the Windows services, verify the Served License Interface service is running.

-or-

If the service is not running, start it.

To reissue a license:

1. As administrator, generate the Request XML file from the following directory and save it to the request directory on the C drive. The following is an example of the command:

Windows (C:\Program Files (x86)\Vertiv\ServedLicenseInterface):

```
Serveractivationui.exe -activate a1a7-94e9-22a5-4867-8204 -quantity 10 -gen c:\requests\reqActivate_052302.xml
```

2. After the request.xml file is generated for all the files, send it to Technical Support. After you receive the Response XML files, save them to the response directory on C Drive.

3. Process the response files. For example,

Windows (C:\Program Files (x86)\Vertiv\ServedLicenseInterface)

```
Serveractivationui.exe -process c:\responses\response.xml
```

4. After the command is complete, the following message is displayed:

File activate_response.xml successfully processed

Refresh license client cache

Windows (C:\Program Files (x86)\Vertiv\ServedLicenseInterface)

```
lmutil lmreread
```

5. After the command is complete, the following message is displayed:

Imutil - Copyright (c) 1989-2010 Flexera Software, Inc. All Rights Reserved.

Imreread successful

NOTE: The licenses are returned during normal business hours. A 10-day emergency license can be provided and should be replaced with an official license within the 10-day period.

6. After the system is licensed, enter `serveractivationui.exe -showlocal` from C:\Program Files\Vertiv\ServedLicenseInterface directory to verify the license is available through the license server.

2.5 RMAN Backup and Recovery Tool

An administrator can use the *Trellis*™ platform database backup and recovery tool to perform the following tasks:

- Set up the database to perform online incremental backups
- Modify the backup retention policy
- Change the Fast Recovery Area size
- Change the location of the Fast Recovery Area
- Change the database backup job schedule
- Report the status of the recovery manager incremental backups
- Restore the database to a point in time within the retention policy

When enabled, RMAN runs an initial full backup, then an incremental backup each day. A new full backup is created each day, merging the incremental with the full, if the retention policy is set to one day.

2.5.1 Incremental backups

The *Trellis*™ platform provides a command-line interface tool to protect the data in your Oracle database. The tool enables database incremental backups without server downtime. Each incremental backup contains the database blocks that have changed since the previous backup. The incremental backups are saved for recovery, based on the days set in your retention policy.

2.5.2 Oracle database configuration

The database must be configured before the backup and recovery tool can be used. The platform installer configures the database and dependencies.

The following pre-configuration is applied by the installer:

- The *Trellis*™ platform database is in archive log mode.
- The default location c:\u03\backup is configured for the FRA.
- BCT is enabled.

2.5.3 Host server file backup

The backup and recovery tool depends on a host server backup of the file system (described in the [Incremental backups](#) on page 12). The file system backup must be able to recover and restore the operating system to a working state. After the operating system is restored, the tool can restore the latest database backup.

2.5.4 Tool configuration

The database backup and recovery tool, RMAN, is installed automatically on the database server in the c:\u01\trellis directory. The factory default setting for tool functionality is disabled. After the RMAN tool is enabled, you can configure the default values for the Fast Recovery Area location and size, enable Block Change Tracking and schedule the daily backup job.

To configure the tool:

1. As the Windows administrator user that installed the *Trellis™* platform, log into the database host server.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. At the prompt, enter **c:\u01\trellis\configure**.
4. Enter option **1** RMAN Configuration, then option **1** Enable RMAN and press **Enter** to enable the RMAN tool.
5. Accept the default FRA location and press **Enter** or enter a new location.
6. Enter **YES** to enable the RMAN tool, execute the first database backup and schedule the backup to the default value at midnight. Full backups of the database include the complete contents of all data files, the control file, archived redo log files and the server parameter file. With these files, you can perform a complete recovery.
7. Verify the first database backup has been created. See [To view database backup and recovery reports](#) on page 14.

NOTE: The default backups run daily at midnight.

8. Enter option **0** one or more times to exit the Configuration menu.

2.5.5 Fast Recovery Area size

The FRA stores the backups and other critical files. With database size fluctuations, retention policy changes and the increase of backups, the space allocated to the FRA must be adjusted. As you approach the limit, a notification is sent to the platform administrator until the issue is resolved. See [Database threshold notification](#) on page 16. If you exceed the allocated space, the database ceases to function.

The FRA should be large enough for copies of the data files, control files, online redo log files and archived redo log files, which are needed to recover the database. The copies of these backup files are kept based on the retention policy. See [Modify the backup schedule](#) on page 15.

The FRA needs to be sized for your environment. FRA size is calculated based on your database size and usage. For a new installation of the *Trellis™* platform, the default/recommended minimum is 23355MB. To calculate your FRA size, multiply the 23355MB by three. In this example, your FRA size is 70065MB.

To change the FRA size:

1. As the Windows administrator user that installed the *Trellis™* platform, log into the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter **c:\u01\trellis\configure**.
4. Enter option **1** RMAN Configuration, then option **2** Modify FRA Settings in the Configuration Menu and press **Enter**.
5. Enter the FRA size and press **Enter**.
6. Press **Enter** to accept the default location.
7. At the confirmation prompt, type **YES** to accept the changes.
8. Enter option **0** one or more times to exit the Configuration menu.

2.5.6 Fast Recovery Area location

The new FRA Location directory should exist prior to setting a new location. Before setting a new FRA location, review the following:

- Place the FRA on a separate disk from your database files to prevent losing your files if a media failure occurs.
- The permanent files and transient files can be left in the previous FRA location.
- The database deletes transient files from the previous FRA location as they become eligible for deletion.

To change the FRA location:

1. As the Windows administrator user that installed the *Trellis™* platform, log into the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter **c:\u01\trellis\configure**.
4. Enter option **1** RMAN Configuration, then option **2** Modify FRA Settings and press **Enter**.
5. Enter the recommended FRA size and press the **Enter** key. Alternatively, you can enter the current FRA size, including the last character **M** and press the **Enter** key.
6. Press the **Enter** key to accept the default FRA location. Alternatively, you can enter the full path of a different FRA location.
7. At the confirmation prompt, type **YES** to accept the changes.
8. Enter option **0** one or more times to exit the Configuration menu.

2.5.7 Reports

Backup reports contain summary and detailed information about previous backup jobs run by the tool. They also include information about the health of the database files.

To view database backup and recovery reports:

1. As **oracle**, log into the database host server.
2. At the prompt, enter **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration.
3. On the Configuration menu, enter option **4** Reports and press **Enter**.
4. Enter option **2** Backup History.
5. Enter a filename to save the report in a file in your current directory.
6. Enter option **0** one or more times to exit the Configuration menu.

To view a database health status report:

1. As **oracle**, log into the database host server.
2. At the prompt, enter **/u01/trellis/configure.sh** and enter option **1** RMAN Configuration.
3. On the Configuration menu, enter option **4** Reports and press **Enter**.
4. Enter option **1** Data files status to view a report about the health of the database files.

NOTE: This operation will take some time to execute, depending on the size of the database. When the operation is completed, verify there is a message indicating the backup data files are in good condition.

5. Press any key to return to the Reports Menu.
6. Enter option **0** one or more times to exit the Configuration menu.

2.5.8 Modify the backup schedule

By default, the start date/time schedule for a backup is daily at midnight. After this, the backup runs on a fixed configurable interval based on this date. The RMAN backup schedule displays the next five scheduled backups.

The start time and interval for the backups can be modified. With a small interval, the backup schedule is more frequent and may require re-evaluating the FRA size. When modifying the backup interval, enter a value between 1 and 99 hours. The value should be less than the retention policy. For example, if the retention policy is one day, use an interval between 1 and 24 hours.

To modify the backup schedule:

```
Trellis RMAN Backup Schedule
=====
Started backups on: 29-10-2014 00:00:00 America/New_York
Back up intervals (in hours): 24
Next 5 backup starts are:
29-10-2014 00:00:00 America/New_York
30-10-2014 00:00:00 America/New_York
31-10-2014 00:00:00 America/New_York
01-11-2014 00:00:00 America/New_York
02-11-2014 00:00:00 America/New_York
Modifying the backup interval may require re-evaluating the FRA size
=====
New Interval (hours, default: 24):
```

1. As the Windows administrator user that installed the *Trellis™* platform, log into the database host server.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. At the prompt, enter `c:\u01\trellis\configure`.
4. Enter option **1** RMAN Configuration, then option **3** Modify Backup Schedule and press **Enter**.
5. Press the **Enter** key to accept the default backup interval value (for example, 24 hours). Alternatively, you can enter a different backup interval value.

```
New Interval (hours, default: 24): 20
dd-MM-yyyy HH:mm:ss z
default: 29-10-2014 00:00:00 America/New_York):
```

6. Enter the backup start date and time in the format `DD-MM-YYYY HH:MM:SS Z` (for example, 27-08-2018 00:00:00 UTC-04:00).

```
New Interval (hours, default: 24): 20
dd-MM-yyyy HH:mm:ss z
default: 29-10-2014 00:00:00 America/New_York):
29-10-2014 14:14:00
New Scheduled Start date is: 2014-10-29T14:14-04:00[America/New_York]
New Interval (hours) is: 20
Next five run date are:
2014-10-29T14:14-04:00[America/New_York]
2014-10-30T10:14-04:00[America/New_York]
2014-10-31T06:14-04:00[America/New_York]
2014-11-01T02:14-04:00[America/New_York]
2014-11-01T22:14-04:00[America/New_York]
Is this correct (Type : YES to accept, NO to abort):
```

7. At the confirmation prompt, type **YES** to accept the changes.

8. Enter option **0** one or more times to exit the Configuration menu.

2.5.9 Restore

The platform restore feature allows you to restore the platform from a previous backup to a point in time. All current data in the database is overwritten with the backup files for the given date.

To restore the platform:

1. Stop the front machine.
2. Stop the back machine.
3. If necessary, restore the operating system files from an operating system backup.
4. As the Windows administrator user that installed the *Trellis™* platform, log into the database host server.
5. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
6. At the prompt, enter `c:\u01\trellis\configure`.
7. Enter option **1** RMAN Configuration.
8. On the Configuration Menu, enter option **5** Restore Database.
9. The tool presents a range of available dates to restore the database backups. Enter a date and time for the restore in the DD/MM/YYYY HH:MM:SS format. For example, you can enter the date and time for the newest backup to restore the latest database changes. You can also copy the date and time (for example, 27/07/2016 03:30:42) from one of the available database backups to restore, paste the text after the Restore to date prompt and press **Enter**.

NOTE: If you are outside the range of the available backups, the nearest date is automatically selected.

10. At the restore database confirmation prompt, type **YES** and press **Enter**.

NOTE: This operation will take time depending on the size of the database.

11. Open another session (also as **oracle** on the back machine) and enter `tail -400f /u02/app/oracle/diag/rdbms/orcl/orcl/trace/alert_orcl.log` to see the restore operation in progress.
12. To verify the restore operation completed successfully, enter `vi /u02/app/oracle/diag/rdbms/orcl/orcl/trace/alert_orcl.log`, verify the message "alter database open resetlogs" is displayed and verify there are no errors logged after this message. The Configuration Menu appears when the restore operation is complete.
13. Enter option **0** one or more times to exit the Configuration menu.
14. After the database has been restored successfully, perform the following:
 - a. Start the back machine.
 - b. Start the front machine.

2.5.10 Database threshold notification

The platform runs a disk space check in the FRA every 15 minutes, updates the Alarm and Event Viewer and sends an email to notify the administrator and RMAN tool users. When the available space in the database is less than 15%, a notification is sent. When reclaimable space is less than 3%, a critical alert notification is sent to the platform administrator and an entry is added to the Event Viewer of the *Trellis™* platform scheduler.

IMPORTANT! The email notification will have an address containing the following text: support@trellis.com. When this occurs, perform the following recommended procedure to correct the problem.

To correct the problem:

1. Increase the FRA size to the recommended size. See [To change the FRA size](#): on page 13.

2. Open the alert log file called `/u02/app/oracle/diag/rdbms/orcl/orcl/trace/alert_orcl.log` and search for the following ALTER database message: ALTER SYSTEM SET db_recovery_file_dest_size={NEW_FRA_SIZE}..
3. Every 15 minutes or more, open the same alert log file and verify the following error does NOT appear AFTER the ALTER database message:

ORA-19815: WARNING: db_recovery_file_dest_size of {FRA_SIZE} bytes is 100.00% used, and has 0 remaining bytes available.

4. Clear the CRITICAL active alarm as follows:
 - Log into the Trellis UI as a Trellis Administrator.
 - From the Active Alarms window, search for a CRITICAL Alarm called “Database Backup Area Threshold exceeded”.
 - Acknowledge and clear the active critical alarm. From this point on, a critical alert notification will no longer be sent to the Trellis Administrator.

NOTE: The original email notification will continue to be sent every 15 minutes until the CRITICAL active alarm is ACKNOWLEDGED and CLEARED by the Trellis Administrator.

NOTE: The database continues to consume space in the flash recovery area until there is no reclaimable space left.

To add users to receive a notification alert:

For version 4.0 to 4.0.3, click the *Administration* menu in the platform software, select *User* and add a new user with the name **rmannotificationX**, where X is a number between 0 and 9.

NOTE: You must add each user in sequential order starting with rmannotification0. For example, rmannotification0 must be added before rmannotification1, rmannotification1 must be added before rmannotification2 and so on.

FRA files are auto managed. When available space is low, Oracle automatically deletes files that are out of the retention policy. If no files are eligible for automatic deletion, the following steps are required:

- Increase the FRA size.
- Move backups from the FRA to tertiary storage.

2.5.11 Running an RMAN backup

An administrator can run an RMAN backup manually by selecting Option 5 - Run RMAN Backup from the RMAN Configuration Menu.

When run outside the retention period, a full and incremental backup is executed. When run within the retention period, only an incremental backup from the last backup is executed.

2.6 Platform Upgrade

Upgrading the *Trellis*™ Real-Time Infrastructure Optimization platform on a Microsoft® Windows® operating system does not change the functionality available. The platform software is available from a web browser after installation is complete on the front and back machines.

All *Trellis*™ platform startups, shutdowns, installations, patches and upgrades must be performed using a Service Account with local Administrator privileges or by using the Administrator account.

You should run any precheck scripts for installing any patches. Results should be analyzed before attempting to install any patch.

Before applying a patch, you should stop the *Trellis* platform and the database and reboot. Performing this via snapshot will ensure the machines are rebooted before applying a patch.

NOTE: Always upgrade or patch the *Trellis*™ platform using the same Service Account or the Administrator account that was used originally to install the platform.

NOTE: The front and back machine's operating system must have regional settings set to US English and the location set to United States.

Prior to running the upgrade installer, the *TrellisConfiguration.zip* file must be present on both the front and back machines. The file is located on the following path:

`%systemdrive%\users\[service_account]\TrellisConfiguration.zip`

NOTE: Throughout this document, terms enclosed in brackets (<...>) must be replaced with the actual value. Folder names cannot contain spaces.

2.6.1 Version 4.0.0 upgrade

When upgrading to version 4.0.0, your current *Trellis*™ platform version (`c:\u01\trellis\trellis.version`) should be 3.4.0 or 3.4.1. For assistance, contact Technical Support.

Prior to upgrading the *Trellis*™ platform to version 4.0.2, complete the following prerequisites.

Prerequisites

Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot to cover the duration of the upgrade. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.

NOTE: The front and back machine's operating system must have regional settings set to US English and the location set to United States.

NOTE: To confirm memory or storage requirements on the front and back machines or get need additional information about the upgrade prerequisites, see The TRELLIS™ Real-Time Infrastructure Optimization Platform Pre-Installation Installer/User Guide.

To prepare for upgrading to version 4.0.0:

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

1. Download the following installation upgrade files on the front and back machines:
 - *TrellisPatch-4.0.0.zip*
 - *TrellisPatch-4.0.0.zip.md5sum*
2. Verify the md5 checksum for the zip file in step 2 and unzip it.
3. Create and name a directory **TrellisPatch-4.0.0**.

NOTE: This directory is referred to as <TRELLIS_PATCH_DIR> in this document.

NOTE: If you do not know how to use an MD5SUM program to validate your files, contact Technical Support.

4. Open the `c:\u01\trellis\trellis.version` file to verify the *Trellis*™ platform version.

Upgrade procedures

Now that you have verified the version and copied the installation upgrade files to the front and back machines, you must stop the front machine, then the back machine.

To stop the machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. Enter `\u01\trellis\trellis stop` to stop the front machine, and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.



WARNING! Closing the command prompt window during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at `\u03\installer\logs`) and contact Technical Support.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `cd <TRELLIS_PATCH_DIR>` to access the *Trellis*™ platform install patch directory.
4. Enter `installPatch` to run the patch.
5. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 8-45 minutes.

NOTE: The upgrade process migrates data during the `cdmr-sql-patch` process. The duration of the migration is relative to the amount of data in the system and performance of the hardware. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

To upgrade the front machine:

NOTE: If you recently downloaded symbols from the *Trellis* platform portal and they are newer than those available in the 4.0.0 upgrade package, an `Unmarshal Exception` error occurs. If this error occurs, go to <https://www.vertiv.com/Trellis-Platform> for additional information.

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `cd <TRELLIS_PATCH_DIR>` to access the install patch directory.
4. Enter `installPatch` to run the patch.
5. At the platform install patch prompt, enter the DomainDir directory location and press **Enter**.
6. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 120-200 minutes.

2.6.2 Version 4.0.2 upgrade

When upgrading to version 4.0.2, your current *Trellis* platform version (`c:\u01\trellis\trellis.version`) should be 4.0.0 or 4.0.1. For assistance, contact Technical Support.

NOTE: In *Trellis* platform 4.0.2 and higher, SSLv3 is disabled and Transport Layer Security (TLS) 1.0 is enabled.

Prior to upgrading the *Trellis* platform to version 4.0.2, complete the following prerequisites.

Prerequisites

Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot to cover the duration of the upgrade. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.

NOTE: To confirm memory or storage requirements on the front and back machines or get additional information about the upgrade prerequisites, see The TRELLIS™ Real-Time Infrastructure Optimization Platform Pre-Installation Installer/User Guide.

To prepare for upgrading to version 4.0.2:

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

1. Download the following installation upgrade files on the front and back machines:
 - TrellisPatch-4.0.2.zip
 - TrellisPatch-4.0.2.zip.md5sum
2. Verify the md5 checksum for the zip file in step 2 and unzip it.
3. Create and name a directory **TrellisPatch-4.0.2**.

NOTE: This directory is referred to as <TRELLIS_PATCH_DIR> in this document.

NOTE: If you do not know how to use an MD5SUM program to validate your files, contact Technical Support.

4. Open the `c:\u01\trellis\trellis.version` file to verify the *Trellis* platform version.

Upgrade procedures

Now that you have verified the version and copied the installation upgrade files to the front and back machines, you must stop the front machine, then the back machine.

To stop the machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `\u01\trellis\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.



WARNING! Closing the command prompt window during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at `/u03/installer/logs`) and contact Technical Support.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.

3. Enter `cd <TRELLIS_PATCH_DIR>` to access the *Trellis* platform install patch directory.
4. Enter `installPatch` to run the patch.
5. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 8-45 minutes.

NOTE: The upgrade process migrates data during the `cdmr-sql-patch` process. The duration of the migration is relative to the amount of data in the system and performance of the hardware. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

To upgrade the front machine:

NOTE: If you recently downloaded symbols from the *Trellis* platform portal and they are newer than those available in the 4.0.2 upgrade package, an Unmarshal Exception error occurs. If this error occurs, go to <https://www.vertiv.com/Trellis-Platform> for additional information.

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `cd <TRELLIS_PATCH_DIR>` to access the install patch directory.
4. Enter `installPatch` to run the patch.
5. At the platform install patch prompt, enter the DomainDir directory location and press **Enter**.
6. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 120-200 minutes.

2.6.3 Version 4.0.3 upgrade

When upgrading to version 4.0.3, your current *Trellis*™ platform version (c:\u01\trellis\trellis.version) should be 4.0.2. For assistance, contact Technical Support.

NOTE: In the *Trellis*™ platform version 4.0.3 and higher, SSLv3 is disabled and Transport Layer Security (TLS) 1.0 is enabled.

Prior to upgrading the *Trellis*™ platform to version 4.0.3, complete the following prerequisites.

Prerequisites

Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot to cover the duration of the upgrade. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.

NOTE: To confirm memory or storage requirements on the front and back machines or get need additional information about upgrade prerequisites, see [The TRELLIS™ Real-Time Infrastructure Optimization Platform Pre-Installation Installer/User Guide](#).

To prepare for upgrading to version 4.0.3:

NOTE: The *Trellis*™ platform upgrade must be must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis* platform.

1. Download the following installation upgrade files on the front and back machines:
 - TrellisPatch-4.0.3.zip

- TrellisPatch-4.0.3.zip.md5sum
2. Verify the md5 checksum for the zip file in step 2 and unzip it.
 3. Create and name a directory **TrellisPatch-4.0.3**.

NOTE: This directory is referred to as <TRELLIS_PATCH_DIR> in this document.

NOTE: If you do not know how to use an MD5SUM program to validate your files, contact Professional Services.

4. Open the `c:\u01\trellis\trellis.version` file to verify the *Trellis* platform version.

Upgrade procedures

Now that you have verified the version and copied the installation upgrade files to the front and back machines, you must stop the front machine, then the back machine.

To stop the machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. Enter `\u01\trellis\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.



WARNING! Closing the command prompt window during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `cd <TRELLIS_PATCH_DIR>` to access the *Trellis*™ platform install patch directory.
4. Enter `installPatch` to run the patch.
5. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 8-45 minutes.

NOTE: The upgrade process migrates data during the cdmr-sql-patch process. The duration of the migration is relative to the amount of data in the system and performance of the hardware. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

To upgrade the front machine:

NOTE: If you recently downloaded symbols from the *Trellis* platform portal and they are newer than those available in the 4.0.3 upgrade package, an Unmarshal Exception error occurs. If this error occurs, go to <https://www.vertiv.com/Trellis-Platform> for additional information.

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `cd <TRELLIS_PATCH_DIR>` to access the install patch directory.
4. Enter `installPatch` to run the patch.

5. At the platform install patch prompt, enter the DomainDir directory location and press **Enter**.
6. Wait for the BUILD SUCCESSFUL message to appear when the process is complete, which can take 120-200 minutes.

2.6.4 Version 5.0.1 upgrade

Notes and Special Instructions:

NOTE: Starting with *Trellis*™ platform version 5.0.1, the Vertiv™ license server is used instead of the Emerson license server.

- For more information and detailed instructions on using the *Trellis*™ platform, visit <https://www.vertiv.com/Trellis-Platform> for accompanying user documentation.
- Version 5.0.1 of the *Trellis*™ platform supports *Trellis*™ Intelligence Engine version 4.6.15 and higher, as well as the Avocent® Universal Management Gateway appliance firmware version 4.0.0.15 and higher, containing the embedded *Trellis* Intelligence Engine version 4.0.3.6.
- Prior to upgrading to Version 5.0.1, you must stop the WMI service on the back server.

NOTE: Element Library versions 4.0.0.x and lower are supported by these versions listed.

You must perform the following steps in the order provided to upgrade the *Trellis*™ platform from version 4.0.3 to 5.0.1:

- Verify that the existing *Trellis*™ platform version is 4.0.3.
- Stop the *Trellis*™ platform on the front and back machines.
- Upgrade the back machine to version 5.0.1 and wait until the upgrade has completed successfully.
- Upgrade the front machine to version 5.0.1.

Prerequisites IMPORTANT!

Prior to upgrading the *Trellis*™ platform to version 5.0.1, you must complete the following prerequisites:

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

- Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.
- Perform a full backup of the front and back machines. If the front and back machines are running in virtual machines, you can create a virtual machine snapshot of both machines as follows:
 - a. Gracefully stop the *Trellis*™ platform on the front machine.
 - b. Gracefully stop the *Trellis*™ platform on the back machine.
 - c. Gracefully shut down the operating system on the front machine.
 - d. Gracefully shut down the operating system on the back machine.
 - e. Create a snapshot on the front machine.
 - f. Create a snapshot on the back machine.
 - g. Start the operating system on the front machine.
 - h. Start the operation system on the back machine.

- i. Start the *Trellis*™ platform on the back machine.
 - j. Start the *Trellis*™ platform on the front machine.
 - k. Log into *Trellis* application and verify functionality.
- The front and back machine's operating system must have regional settings set to US English and the location set to United States.
- You need to have at least 50 GB free space on the front and back machines.

The details of each step are provided in the following sections.

Upgrade procedures

NOTE: It is critical that there is no interruption during the upgrade process. Disconnecting from the session while the upgrade is in progress aborts the upgrade prematurely. Make sure that you have a stable and reliable connection to the front and back machine.

To verify the *Trellis* platform version:

1. Log into the front machine as the local administrator.
2. Enter `notepad %windir%\trellis\trellis.version` to display the current *Trellis*™ platform version.
3. Verify the *Trellis*™ platform version is 4.0.3.

To stop the *Trellis* platform front and back machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. Enter `%windir%\trellis\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir <TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.1 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd <TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis* Patch 5.0.1 ZIP file to the installation patch directory.
6. Right-click the *Trellis* Patch 5.0.1 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis* platform on the back machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

NOTE: The upgrade process migrates data in the *Trellis*™ database on the back machine. The duration of the migration is relative to the amount of data in the system and performance of the hardware during the upgrade process. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

8. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
9. Open the *Trellis* patch log file which starts with `patch.trellis.version.5.0.0.<ID>.log` where `<ID>` is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 150-250 minutes, has been successful. During the upgrade process, the back machine has been automatically started.

To upgrade the front machine:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir <TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.1 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd <TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis*™ Patch 5.0.1 ZIP file to the installation patch directory.
6. Right-click the *Trellis*™ Patch 5.0.1 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis*™ platform on the front machine and wait until the operation has been completed.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at `C: \u03\installer\logs`) and contact Technical Support.

8. After the platform install patch prompt, enter the location for the domain directory and press **Enter**.
9. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
10. Open the *Trellis*™ patch log file which starts with `patch.trellis.version 5.0.0.<ID>.log`, where `<ID>` is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 250-350 minutes, has been successful.

NOTE: The front machine is automatically started during the upgrade process.

2.6.5 Version 5.0.1.2 upgrade

Your current *Trellis*™ platform version (`/u01/trellis/trellis.version`) must be 5.0.1 or 5.0.1.1 when upgrading to version 5.0.1.2. The following is the upgrade process, which must be performed in the listed order.

NOTE: If you are considering upgrading the Windows® 2008 host that supports the *Trellis*™ platform, please contact your Engagement Manager or Technical Support to facilitate the upgrade.

To upgrade a *Trellis*™ platform system from version 5.0.1 to 5.0.1.2:

The following is a list of the procedures to be performed to upgrade your *Trellis*™ platform system from version 5.0.1 or 5.0.1.1 to 5.0.1.2.

1. Copy the version 5.0.12 hotfix to the version 5.0.1 or 5.0.1.1 system.
2. Stop the *Trellis*™ platform and proceed as follows:
 - a. Update the Time Series Domain (TSD) schema.
 - b. Update the *Trellis*™ platform database schema.
3. Start the *Trellis*™ platform and proceed as follows:
 - a. Apply the version 5.0.12 mini patch on the back machine.
 - b. Apply the version 5.0.12 mini patch on the front machine.
4. Perform the final verification procedure.

Proceed to perform the procedures in the following Prerequisites section and [Upgrade procedures](#) on page 27. For assistance, contact Technical Support.

Prerequisites

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

An operating system level backup of the *Trellis*™ platform version 5.0.1 or 5.0.1.1 front and back machines must be performed in case there is a failure during the execution of the following procedures. If using virtual machines, shut them down and take a snapshot of each machine. If there is no snapshot capability, create a cold backup of the *Trellis*™ database.

After the machines are backed up, you must copy the *Trellis*™ 5.0.12 hotfix to the *Trellis*™ 5.0.1 or 5.0.1.1 system.

To copy the *Trellis*™ hotfix zip file to the *Trellis*™ 5.0.1 or 5.0.1.1 system:

1. Download the *Trellis*™ hotfix zip file (for example, **trellis-hotfix-5.0.1-to-5.0.1.2.zip**) to the local machine.
2. As **Windows Administrator**, log into the *Trellis*™ back machine as follows:
 - a. Click the Start icon located in the left corner of the taskbar.
 - b. Right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
3. Enter **mkdir C:\tmp\hotfix** to create the temporary directory for the *Trellis*™ 5.0.12 files.

NOTE: If this directory already exists, delete any files and sub-directories in this directory.

4. Enter **cd C:\tmp\hotfix** to access the temporary directory.
5. Use a file transfer application (for example, WinSCP) to copy the *Trellis*™ hotfix zip file from the local machine to this temporary directory.
6. Enter **dir** to verify the *Trellis*™ hotfix zip file exists in the temporary directory.
7. Select the following to unzip the zip file in the temporary directory:
 - a. From Windows® Explorer®, access the C:\tmp\hotfix folder.
 - b. Right-click the *trellis-hotfix-5.0.1-to-5.0.1.2.zip* file.
 - c. Select *7-Zip - Extract Here*.

8. After unzipping the files, enter the following:

```
cd trellis-hotfix-5.0.12
```

```
dir
```

9. Verify the following directories and files exist in the top level trellis-hotfix-5.0.12 directory:
 - db: This directory contains the *Trellis*™ database schema files to execute.
 - tsd: This directory contains the SQL scripts to apply to the *Trellis*™ Time Series Database (TSD).
 - dbpatch5011.sql: This SQL script is used by the command script to update both the *Trellis*™ database and *Trellis*™ TSD.
 - trellis-patcher-0.0.0.28.exe: This executable file is the application used to apply the *Trellis*™ 5.0.12 patch.
10. As **Windows Administrator**, log into the *Trellis*™ front machine as follows:
 - a. Click the Start icon located in the lower left corner of the taskbar.
 - b. Right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
11. Enter **mkdir C:\tmp\hotfix** to create the temporary directory to store the *Trellis*™ platform version 5.0.12 files.

NOTE: If this directory already exists, delete any files and sub-directories in this directory.

12. Enter **cd C:\tmp\hotfix** to access the temporary directory.
13. Use a file transfer application (for example, WinSCP) to copy the *Trellis*™ hotfix zip file to the temporary directory on the *Trellis*™ platform front machine.
14. Enter **dir** to verify the *Trellis*™ hotfix zip file exists in this temporary directory.
15. Select the following to unzip the zip file from the temporary directory on the *Trellis*™ platform front machine:
 - a. From Windows® Explorer®, access the C:\tmp\hotfix folder.
 - b. Right-click the *trellis-hotfix-5.0.1-to-5.0.12.zip* file.
 - c. Select *7-Zip - Extract Here*.
16. After unzipping the files, enter the following:

```
cd trellis-hotfix-5.0.12
```

```
dir
```

17. Verify the following directories and files exist in the top level trellis-hotfix-5.0.12 directory:
 - db: This directory contains the *Trellis*™ database schema files to execute.
 - tsd: This directory contains the SQL scripts to apply to the *Trellis*™ TSD.
 - dbpatch5011.sql: This SQL script is used by the command script to update both the *Trellis*™ database and *Trellis*™ TSD.
 - trellis-patcher-0.0.0.28.exe: This executable file is the application to apply the *Trellis*™ 5.0.12 patch.

Upgrade procedures

Now that you have verified the platform version and copied the installation upgrade files to the front and back machines, you must stop the front machine and then stop the back machine prior to updating the *Trellis*™ platform database and TSD. The following procedures are used for this process: to log in, perform the updates, start the platform and apply the patch to the front and back machine.

Stopping the *Trellis*™ platform

To stop the *Trellis*™ platform on the front and back machine:

1. Verify the *Trellis*™ platform is up and running.
2. Stop the *Trellis*™ platform on the front machine. Refer to [Stopping the TRELLIS™ platform on the front machine](#) on page 30.
3. Stop the *Trellis*™ platform on the back machine. Refer to [Stopping the TRELLIS™ platform on the back machine](#) on page 30.

To update the *Trellis*™ platform environment variables:

1. Verify the back machine is stopped.
2. As **Windows Administrator**, log into the *Trellis*™ platform back machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter the `C:\u01\trellis\setTrellisEnv.cmd` command to configure the required environment variables for the SQL *Plus utility.

To update the *Trellis*™ database and TSD:

1. As **Windows Administrator**, log into the *Trellis*™ platform back machine.
2. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
3. Enter `cd C:\tmp\hotfix\trellis-hotfix-5.0.1.2` to access the temporary directory where the script to update the *Trellis*™ database and TSD is stored.
4. Execute the `dbpatch501.cmd` script to update the *Trellis*™ database and TSD and wait until the script is completed successfully. This script uses the SQL *Plus utility to execute database script files.

NOTE: This operation takes several minutes to execute, depending on the size of the *Trellis*™ database.

5. Enter `notepad C:\u03\logs\minipatch501.log` to check the log file and verify there are no errors.

Starting the *Trellis*™ platform

To start the *Trellis*™ platform on the back machine and then on the front machine:

1. Verify the *Trellis*™ platform is stopped on the front and back machines.
2. Start the *Trellis*™ platform on the back machine. Refer to [Starting the TRELLIS™ platform on the back machine](#) on page 30.
3. Start the *Trellis*™ platform on the front machine. Refer to [Starting the TRELLIS™ platform on the front machine](#) on page 30.
4. Log into the *Trellis*™ application and verify the functionality.

Applying the *Trellis*™ 5.0.1.2 mini patch on the *Trellis*™ platform

To apply the *Trellis*™ 5.0.1.2 mini patch to the *Trellis*™ platform back machine:

1. Verify the *Trellis*™ software has been started on the back machine and the *Trellis*™ database is up and running.
2. As **Windows Administrator**, log into the *Trellis*™ platform back machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.

4. Enter `cd C:\tmp\hotfix\trellis-hotfix-5.0.12` to access the directory where the *Trellis*™ mini patch files are stored.
5. Execute the *Trellis*™ mini patch `trellis-patcher-0.0.0.28.exe` application to apply changes to the *Trellis*™ platform.
6. Select the location for the extracted files that are needed for the *Trellis*™ mini patch installation, and at the prompt, click *OK* to accept the default directory.
7. Wait until the *Trellis*™ mini patch is complete. A blank Command Prompt window appears and closes automatically.
8. Enter the following to make sure there are no errors in the *Trellis*™ Patch log file.
 - a. From Windows® Explorer®, access `C:\u03\logs\trellis-patcher`.
 - b. Right-click the `trellis-patcher.0.log` file and select *Edit with Notepad++*.

To apply the *Trellis*™ platform release 5.0.1.2 mini patch to the *Trellis*™ platform front machine:

1. Verify the *Trellis*™ software has been started on the front machine and the *Trellis*™ database is up and running to apply the *Trellis*™ 5.0.1.2 mini patch to the *Trellis*™ front machine.
2. As **Windows Administrator**, log into the *Trellis*™ platform front machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter `cd C:\tmp\hotfix\trellis-hotfix-5.0.12` to access the directory where the *Trellis*™ mini patch files are stored.
5. Execute the *Trellis*™ mini patch `trellis-patcher-0.0.0.28.exe` application to apply changes to the *Trellis*™ platform.
6. Select the location for the extracted files that are needed for the *Trellis*™ mini patch installation, and at the prompt, click *OK* to accept the default directory.

NOTE: During version 5.0.1 to 5.0.1.2 patch execution, the *Trellis*™ front machine restarts two times and can take approximately one hour or more, depending on the hardware speed.

NOTE: During version 5.0.1.1 to 5.0.1.2 patch execution, the *Trellis*™ front machine restarts one time and can take approximately one half hour, depending on the hardware speed.

7. After the patch is complete and the blank Command Prompt window opens and closes, verify there are no errors in the *Trellis*™ Patch log file as follows:
 - a. From Windows® Explorer®, access `C:\u03\logs\trellis-patcher`.
 - b. Right-click the `trellis-patcher.0.log` file and select *Edit with Notepad++*.

Final Verification

To verify the *Trellis*™ platform has been upgraded to 5.0.1.2:

1. Log into the *Trellis*™ platform application.
2. In the upper right corner, click the logged in username and select *About*.
3. Click *MORE DETAILS* and verify the *Trellis*™ Patch 5.0.1.2 is displayed.

General procedures

This section describes general procedures to execute on a *Trellis*™ platform environment.

Stopping the TRELLIS™ platform on the back machine

To stop the *Trellis*™ platform on the back machine:

1. Verify the Administrator has installed the *Trellis*™ platform on the back machine.
2. As **Windows Administrator**, log into the *Trellis*™ platform back machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter the `C:\u01\trellis\trellis stop` command to stop the *Trellis*™ software on the back machine.
5. Verify a message indicates the *Trellis*™ software components are stopped successfully.

Starting the TRELLIS™ platform on the back machine

To start *Trellis*™ on the back machine:

1. Verify the Administrator has installed the *Trellis*™ platform on the back machine.
2. As **Windows Administrator**, log into the *Trellis*™ platform back machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter the `C:\u01\trellis\trellis start` command to start the *Trellis*™ platform software on the back machine.
5. Verify a message indicates the *Trellis*™ software components are started successfully.
6. Wait a few minutes and enter the `C:\u02\domains\IDMDomain\idm.status.cmd` command to verify the status of each IDM domain component is Alive.

Stopping the TRELLIS™ platform on the front machine

To stop the *Trellis*™ platform on the front machine:

1. Verify the Administrator has installed the *Trellis*™ platform on the front machine.
2. As **Windows Administrator**, log into the *Trellis*™ platform front machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter the `C:\u01\trellis\trellis stop` command to stop the *Trellis*™ platform software on the front machine.
5. Verify a message indicates the *Trellis*™ software components are stopped successfully.

Starting the TRELLIS™ platform on the front machine

To start the *Trellis*™ platform on the front machine:

1. Verify the Administrator has installed the *Trellis*™ platform on the front machine.
2. As **Windows Administrator**, log into the *Trellis*™ platform front machine.
3. Click *Start*, right-click the *Command Prompt* application and select *Run as administrator* to open the command prompt window.
4. Enter the `C:\u01\trellis\trellis start` command to start the *Trellis*™ software on the front machine.
5. Verify the *Trellis*™ software components (for example, Admin, Coherence, OSB, SOA, ADF and Jasper servers) start successfully.

NOTE: This operation may take approximately one half hour, depending on the hardware speed.

2.6.6 Version 5.0.2 upgrade

Notes and Special Instructions:

- For more information and detailed instructions on using the *Trellis™* platform, visit <https://www.vertiv.com/Trellis-Platform> for accompanying user documentation.
- Version 5.0.2 of the *Trellis™* platform supports *Trellis™* Intelligence Engine version 4.6.1.31, as well as the Avocent® Universal Management Gateway appliance firmware version 4.1.2.12 and higher, containing the embedded *Trellis™* Intelligence Engine version 4.0.3.23.

NOTE: Element Library versions 4.0.0.x and lower are supported by these versions listed. The *Trellis™* platform version 5.0.2 release supports the Microsoft Windows 2012 R2 Standard operating system.

You must perform the following steps in the order provided to upgrade the *Trellis™* platform from version 5.0.1.x to 5.0.2:

- Verify that the existing *Trellis™* platform version is 5.0.1.x.
- Stop the *Trellis™* platform on the front and back machines.
- Upgrade the back machine to version 5.0.2 and wait until the upgrade has completed successfully.
- Upgrade the front machine to version 5.0.2.

Prerequisites IMPORTANT!

Prior to upgrading the *Trellis™* platform to version 5.0.2, you must complete the following prerequisites:

NOTE: The *Trellis™* platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis™* platform.

- Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.
- Perform a full backup of the front and back machines. If the front and back machines are running in virtual machines, you can create a virtual machine snapshot of both machines as follows:
 - a. Gracefully stop the *Trellis™* platform on the front machine.
 - b. Gracefully stop the *Trellis™* platform on the back machine.
 - c. Gracefully shut down the operating system on the front machine.
 - d. Gracefully shut down the operating system on the back machine.
 - e. Create a snapshot on the front machine.
 - f. Create a snapshot on the back machine.
 - g. Start the operating system on the front machine.
 - h. Start the operation system on the back machine.
 - i. Start the *Trellis™* platform on the back machine.
 - j. Start the *Trellis™* platform on the front machine.
 - k. Log into *Trellis™* application and verify functionality.
- The front and back machine's operating system must have regional settings set to US English and the location set to United States.
- You need to have at least 50 GB free space on the front and back machines.

The details of each step are provided in the following sections.

Upgrade procedures

NOTE: It is critical that there is no interruption during the upgrade process. Disconnecting from the session while the upgrade is in progress aborts the upgrade prematurely. Make sure that you have a stable and reliable connection to the front and back machine.

To verify the *Trellis* platform version:

1. Log into the front machine as the local administrator.
2. Enter `notepad %trellis%\trellis.version` to display the current *Trellis*™ platform version.
3. Verify the *Trellis*™ platform version is 5.0.1.x.

To stop the *Trellis* platform front and back machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. Enter `%trellis%\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.2 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis* Patch 5.0.2 ZIP file to the installation patch directory.
6. Right-click the *Trellis* Patch 5.0.2 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis* platform on the back machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at `C:\u03\installer\logs`) and contact Technical Support.

NOTE: The upgrade process migrates data in the *Trellis*™ database on the back machine. The duration of the migration is relative to the amount of data in the system and performance of the hardware during the upgrade process. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

8. Enter `cd %u03%\logs\installer` to access the *Trellis*™ installer log directory.

9. Open the *Trellis* patch log file which starts with `patch.trellis.version.5.0.2.<ID>.log` where `<ID>` is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 150-250 minutes, has been successful. During the upgrade process, the back machine is automatically started.

To upgrade the front machine:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.2 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis*™ Patch 5.0.2 ZIP file to the installation patch directory.
6. Right-click the *Trellis*™ Patch 5.0.2 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis*™ platform on the front machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

8. After the platform install patch prompt, enter the location for the domain directory and press **Enter**.
9. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
10. Open the *Trellis*™ patch log file which starts with `patch.trellis.version 5.0.2.<ID>.log`, where `<ID>` is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 250-350 minutes, has been successful.

NOTE: The front machine is automatically started during the upgrade process.

2.6.7 Version 5.0.3 upgrade

Notes and Special Instructions:

- For more information and detailed instructions on using the *Trellis*™ platform, visit <https://www.vertiv.com/Trellis-Platform> for accompanying user documentation.
- Version 5.0.3 of the *Trellis*™ platform supports *Trellis*™ Intelligence Engine version 4.6.131, as well as the Avocent® Universal Management Gateway appliance firmware version 4.12.12 and higher, containing the embedded *Trellis*™ Intelligence Engine version 4.0.3.23.

NOTE: Element Library versions 4.0.0.x and lower are supported by these versions listed. The *Trellis*™ platform version 5.0.3 release supports the Microsoft Windows 2012 R2 Standard operating system.

You must perform the following steps in the order provided to upgrade the *Trellis*™ platform from version 5.0.2 to 5.0.3:

- Verify that the existing *Trellis*™ platform version is 5.0.2.
- Stop the *Trellis*™ platform on the front and back machines.
- Upgrade the back machine to version 5.0.3 and wait until the upgrade has completed successfully.

- Upgrade the front machine to version 5.0.3.

Prerequisites IMPORTANT!

Prior to upgrading the *Trellis*™ platform to version 5.0.3, you must complete the following prerequisites:

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

- Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.
- Perform a full backup of the front and back machines. If the front and back machines are running in virtual machines, you can create a virtual machine snapshot of both machines as follows:
 - a. Gracefully stop the *Trellis*™ platform on the front machine.
 - b. Gracefully stop the *Trellis*™ platform on the back machine.
 - c. Gracefully shut down the operating system on the front machine.
 - d. Gracefully shut down the operating system on the back machine.
 - e. Create a snapshot on the front machine.
 - f. Create a snapshot on the back machine.
 - g. Start the operating system on the front machine.
 - h. Start the operation system on the back machine.
 - i. Start the *Trellis*™ platform on the back machine.
 - j. Start the *Trellis*™ platform on the front machine.
 - k. Log into *Trellis*™ application and verify functionality.
- The front and back machine's operating system must have regional settings set to US English and the location set to United States.
- You need to have at least 50 GB free space on the front and back machines.

The details of each step are provided in the following sections.

Upgrade procedures

NOTE: It is critical that there is no interruption during the upgrade process. Disconnecting from the session while the upgrade is in progress aborts the upgrade prematurely. Make sure that you have a stable and reliable connection to the front and back machine.

To verify the *Trellis* platform version:

1. Log into the front machine as the local administrator.
2. Enter `notepad %userprofile%\trellis\trellis.version` to display the current *Trellis*™ platform version.
3. Verify the *Trellis*™ platform version is 5.0.2.

To stop the *Trellis* platform front and back machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.

3. Enter `\u01\trellis\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis™* Patch 5.0.3 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis* Patch 5.0.3 ZIP file to the installation patch directory.
6. Right-click the *Trellis* Patch 5.0.3 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis* platform on the back machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at `C:\u03\installer\logs`) and contact Technical Support.

NOTE: The upgrade process migrates data in the *Trellis™* database on the back machine. The duration of the migration is relative to the amount of data in the system and performance of the hardware during the upgrade process. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

8. Enter `cd \u03\logs\installer` to access the *Trellis™* installer log directory.
9. Open the *Trellis* patch log file which starts with `patch.trellis.version.5.0.3.<ID>.log` where `<ID>` is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 150-250 minutes, has been successful. During the upgrade process, the back machine is automatically started.

To upgrade the front machine:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis™* Patch 5.0.3 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis™* Patch 5.0.3 ZIP file to the installation patch directory.
6. Right-click the *Trellis™* Patch 5.0.3 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis™* platform on the front machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

8. After the platform install patch prompt, enter the location for the domain directory and press **Enter**.
9. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
10. Open the *Trellis*™ patch log file which starts with patch.trellis.version 5.0.3.<ID>.log, where <ID> is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 250-350 minutes, has been successful.

NOTE: The front machine is automatically started during the upgrade process.

2.6.8 Version 5.0.4 and higher upgrade

Notes and Special Instructions:

- For more information and detailed instructions on using the *Trellis*™ platform, visit <https://www.vertiv.com/Trellis-Platform> for accompanying user documentation.
- Version 5.0.4 of the *Trellis*™ platform supports *Trellis*™ Intelligence Engine version 4.6.131, as well as the Avocent® Universal Management Gateway appliance firmware version 4.1.2.12 and higher, containing the embedded *Trellis*™ Intelligence Engine version 4.0.3.23.

NOTE: Element Library versions 4.0.0.x and lower are supported by these versions listed. The *Trellis*™ platform version 5.0.4 release supports the Microsoft Windows 2012 R2 Standard operating system.

You must perform the following steps in the order provided to upgrade the *Trellis*™ platform from version 5.0.3 to 5.0.4:

- Verify that the existing *Trellis*™ platform version is 5.0.3.
- Stop the *Trellis*™ platform on the front and back machines.
- Upgrade the back machine to version 5.0.4 and wait until the upgrade has completed successfully.
- Upgrade the front machine to version 5.0.4.

Prerequisites IMPORTANT!

Prior to upgrading the *Trellis*™ platform to version 5.0.4, you must complete the following prerequisites:

NOTE: The *Trellis*™ platform upgrade must be executed from C: drive.



CAUTION: Disable any antivirus software running on the front and back machines. You can enable the antivirus software after completing the upgrade of the *Trellis*™ platform.

- Perform an operating system level backup of the front and back machines. If using virtual machines, shut them down and take a snapshot. After completing the backup, start the platform software to verify functionality. See [TRELLIS™ Platform BackUp, Restore and Upgrade](#) on page 3 for more information.
- Perform a full backup of the front and back machines. If the front and back machines are running in virtual machines, you can create a virtual machine snapshot of both machines as follows:
 - a. Gracefully stop the *Trellis*™ platform on the front machine.
 - b. Gracefully stop the *Trellis*™ platform on the back machine.
 - c. Gracefully shut down the operating system on the front machine.

- d. Gracefully shut down the operating system on the back machine.
 - e. Create a snapshot on the front machine.
 - f. Create a snapshot on the back machine.
 - g. Start the operating system on the front machine.
 - h. Start the operation system on the back machine.
 - i. Start the *Trellis*™ platform on the back machine.
 - j. Start the *Trellis*™ platform on the front machine.
 - k. Log into *Trellis*™ application and verify functionality.
- The front and back machine's operating system must have regional settings set to US English and the location set to United States.
 - You need to have at least 50 GB free space on the front and back machines.

The details of each step are provided in the following sections.

Upgrade procedures

NOTE: It is critical that there is no interruption during the upgrade process. Disconnecting from the session while the upgrade is in progress aborts the upgrade prematurely. Make sure that you have a stable and reliable connection to the front and back machine.

To verify the *Trellis* platform version:

1. Log into the front machine as the local administrator.
2. Enter `notepad %userprofile%\trellis\trellis.version` to display the current *Trellis*™ platform version.
3. Verify the *Trellis*™ platform version is 5.0.3.

To stop the *Trellis* platform front and back machines:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, right-click and select *Run as Administrator*.
3. Enter `%userprofile%\trellis\trellis stop` to stop the front machine and wait for the machine to stop.
4. Repeat steps 1-3 for the back machine.
5. Complete the upgrades on the back and front machine by running the installer patch on each.

To upgrade the back machine:

1. Log into the back machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.4 ZIP file will be stored and then extracted. Replace `<TRELLIS_PATCH_DIR>` with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis* Patch 5.0.4 ZIP file to the installation patch directory.
6. Right-click the *Trellis* Patch 5.0.4 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis* platform on the back machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

NOTE: The upgrade process migrates data in the *Trellis*™ database on the back machine. The duration of the migration is relative to the amount of data in the system and performance of the hardware during the upgrade process. No further action is required on the back machine after the upgrade is complete. However, do not proceed to the front machine upgrade until everything is fully complete on the back machine.

8. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
9. Open the *Trellis* patch log file which starts with `patch.trellis.version.5.0.4.<ID>.log` where <ID> is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 150-250 minutes, has been successful. During the upgrade process, the back machine is automatically started.

To upgrade the front machine:

1. Log into the front machine as the local administrator.
2. Click *Start - Command Prompt*, then right-click and select *Run as Administrator*.
3. Enter `mkdir<TRELLIS_PATCH_DIR>` to create an installation patch directory where the *Trellis*™ Patch 5.0.4 ZIP file will be stored and then extracted. Replace <TRELLIS_PATCH_DIR> with a meaningful name for this directory.
4. Enter `cd<TRELLIS_PATCH_DIR>` to access the installation patch directory.
5. Copy the *Trellis*™ Patch 5.0.4 ZIP file to the installation patch directory.
6. Right-click the *Trellis*™ Patch 5.0.4 ZIP file, select the 7-Zip item and click the *Extract Here* menu item to extract the contents of this file on the installation patch directory.
7. Enter `installPatch` to run the installer patch to upgrade the *Trellis*™ platform on the front machine and wait until the operation is complete.



WARNING! Closing the command prompt window or dropping the network connection to the machine during an upgrade causes the installation to fail. If the installer patch fails on either machine for any reason, do not run the installer again. Collect the patch log (located at C: \u03\installer\logs) and contact Technical Support.

8. After the platform install patch prompt, enter the location for the domain directory and press **Enter**.
9. Enter `cd \u03\logs\installer` to access the *Trellis*™ installer log directory.
10. Open the *Trellis*™ patch log file which starts with `patch.trellis.version 5.0.4.<ID>.log`, where <ID> is a unique number associated with the log file. Look for the BUILD SUCCESSFUL message at the end of this file. This indicates that the upgrade process, which can take 250-350 minutes, has been successful.

NOTE: The front machine is automatically started during the upgrade process.

3 TRELLIS™ INTELLIGENCE ENGINE BACKUP, RESTORE AND UPGRADE

The following procedures are provided to back up, restore and upgrade the *Trellis* Intelligence Engine that is available with the *Trellis*™ Site Manager module.

NOTE: The *Trellis* Intelligence Engine is only supported on a machine running Red Hat® Enterprise Linux® (RHEL)/Ubuntu. If your *Trellis* platform is running on a Windows OS machine, you must run the *Trellis* Intelligence Engine on a separate Red Hat® Enterprise Linux®/Ubuntu machine.

NOTE: The preferred method to back up the engine is via the *Trellis* platform. The engine can also be backed up via command line, however, if you use command line, the backup is not displayed in the *Trellis* platform user interface.

If you are using the embedded *Trellis* Intelligence Engine data collection engine that is available with the appliance firmware version 4.2.0.34 and lower, see Embedded Intelligence Engine Backup, Restore and Upgrade.

For Universal Management Gateway appliance firmware version 4.3.0.23 and higher that contains the *Trellis* Intelligence Engine 5.1, see the following guidelines.

3.1 Back Up via the Platform

The data collection engine's data is backed up from the *Trellis*™ platform UI. The backup file is encrypted and contains the Intelligence Engine configuration and a database backup. The backup file is located in the <BackupLocation>/tmpdir folder with the filename format: **intelligence_engine_backup.<BackupTimeStamp>.bin**.

To back up one or more data collection engines using the platform:

1. As an administrator user, log into the platform UI.
2. For version 4.0 to 4.0.3, click the Administration icon and under System Configuration, click *Data Collection Engine*.

-or-

For version 5.0.1 to 5.0.6, click the Monitoring icon and select *Data Collection Engine*.

-or-

For version 5.1 or later, click the Administration icon and then click *Data Collection Engine - Select Intelligence Engine with OS*.
3. In the Data Collection Engine window, select one or more data collection engines and click *Backup Engine*.

NOTE: After the data collection engine is successfully backed up, the data collection engine publishes the status event which can be seen in the platform's event viewer.

To locate the backup history:

1. For version 4.0 to 4.0.3, click the Administration icon and under System Configuration, click *Data Collection Engine - Select Intelligence Engine with OS*.

-or-

For version 5.0.1 to 5.0.6, click the Monitoring icon and select *Data Collection Engine*.

-or-

For version 5.1 or later, click the Administration icon and click *Data Collection Engine - Select Intelligence Engine with OS*.

2. Select *RedHat* and click *Details - Backup History*.

3.2 Back Up via Command Line

The backup is stored in the BackupLocation file, which is configured in the install-prop.ini file. See more about the BackupLocation file in The TRELLIS™ Real-Time Infrastructure Optimization Platform User Guide in the Default Install Options section.

To back up the data collection engine using command line:

1. In PuTTY or a similar program, enter **SSH** to host where the data collection engine is installed.
2. Log in as the user with sudo permissions.
3. Enter **cd /etc/mss/utility** to go to the */etc/mss/utility/* folder.
4. Execute the **sudo nohup ./BackUp_Restore.sh** backup command.
5. Enter credentials for sudo permission.
6. Verify the backup file is stored in the <BackupLocation>/tmpdir directory folder which was selected during installation of the Intelligence Engine. The backup history includes the backup executed from command line.
7. Back up the filename format: intelligence_engine_backup.<BackupTimeStamp>.bin

3.3 Restore

The *Trellis* platform communicates with the *Trellis*™ Intelligence Engine via IP address or FQDN address. The IP address and FQDN address must match the restored *Trellis* Intelligence Engine.

NOTE: The IP address of the new Red Hat® Enterprise Linux®/Ubuntu installation must match the IP address of the previous installation.

The Intelligence Engine can be backed up via command line to the same virtual machine (VM) or physical server. The entire VM can be backed up and restored on the same virtualization host. A back up of a registered and active Intelligence Engine can also be restored to a clean install of the Intelligence Engine on a new VM/server.

NOTE: Restoring old backup files may introduce complexity because the backed up engine may not contain the monitored devices and element libraries that were added after the backup was created.

NOTE: The entire Virtual Machine can be backed up and restored on the same virtualization host. The Intelligence Engine does not support restoring an engine backup on a different IP.

To restore existing backup files:

1. In PuTTY, enter **SSH** to host where the data collection engine is installed.
2. As a user with sudo permission, log into the platform.
3. Enter **cd /iebackup/tmpdir** to navigate to the backup location. For example, the default location for backup files is in the */iebackup* folder.

NOTE: This folder contains the backup .bin file with the UTC timestamp in the filename. The timestamp, located immediately prior to the .bin extension, indicates the time the backup was created.

4. Enter **cd /etc/mss/utility** and navigate to the */etc/mss/utility* folder.
5. Run the Restore command using **sudo** and **./BackUp_Restore.sh restore <Backup .bin file>**. For example, **sudo nohup./BackUp_Restore.sh restore intelligence_engine_backup.1463510452.bin**.

6. After a successful restore, verify the engine services restart and re-establish communication with the platform and the end devices that are monitored and managed by the data collection engine.

To restore the backup files to a new Red Hat® Enterprise Linux®/Ubuntu installation:

1. Install the Intelligence Engine in the Red Hat® Enterprise Linux®/Ubuntu operating system. See the Installing the Intelligence Engine section in The TRELLIS™ Real-Time Infrastructure Optimization Platform Pre-Installation Installer/User Guide.
2. Copy the Intelligence Engine backup file `<intelligence_engine_backup.{UTCtimestamp}.bin>` to `<BackupLocation>/tmpdir`.
3. Enter `cd /etc/mss/utility` to navigate to the `/etc/mss/utility` folder.
4. Enter `sudo ./BackUp_Restore.sh restore <Backup .bin file>` to run the Restore command. For example, enter `sudo ./BackUp_Restore.sh restore intelligence_engine_backup.1463510452.bin`.
5. After a successful restore is complete, verify the engine services restart and they re-establish communication with the *Trellis*™ platform and the end devices that are monitored and managed by the data collection engine.

3.4 *Trellis*™ Intelligence Engine Upgrade

The *Trellis*™ Intelligence Engine can be downloaded from the <http://www.vertiv.com/TrellisDownloads> URL. It can be installed or uninstalled using PuTTY or a similar program. The data collection engine can also be upgraded from the *Trellis*™ platform UI using the following applicable tar.gz installer:

- RHEL: `ieupgrade_package-<version>-RELEASE-RHEL.tar.gz`
- Ubuntu: `ie_upgrade_package_UBUNTU-<version>.tar.gz`

To upgrade one or more data collection engines:

1. From www.vertiv.com, download the Intelligence Engine upgrade software package for your operating system.
2. As administrator user with access to the data collection engine upgrade, log into the platform UI.
3. For version 4.0.2 and 4.0.3, click the Administration icon, select *System Configuration* and click *Device Installation* to upload the Intelligence Engine upgrade file.

-or-

For version 5.0.1 or later, click the Administration icon, select *System Settings* and go to the Firmware Settings section to upload the Intelligence Engine upgrade file.

4. For version 4.0.2 and higher, click the Administration icon and select *Data Collection Engine*.

-or-

For version 5.0.1 to 5.0.6, click the Monitoring icon and select *Data Collection Engine*.

-or-

For version 5.1 or later, click the Administration icon and then click *Data Collection Engine - Select Intelligence Engine with OS*.

5. Select the data collection engine to be upgraded and click the *Upgrade Engine* button.
6. Select the *Data Collection Engine* software file from the list and select to schedule the date and/or time to initiate the upgrade.
7. After the data collection engine is successfully upgraded, the schedule task status is updated and can be viewed from the Scheduler window. The upgrade status event is also published and can be seen in the Event Viewer.

NOTE: During the upgrade process, the engine temporarily stops communicating with the platform.

To delete the engine upgrade package:

1. In the Device Installation window, highlight the engine upgrade package and click *Remove*.
2. In the confirmation message, click *OK*.

3.4.1 Upgrade history

A list of the completed upgrades performed on the Intelligence Engine can be accessed.

To view the upgrade history:

1. For version 4.0.2 and 4.0.3, click the Administration icon and under System Configuration, click *Data Collection Engine* and select the data collection engine from the list.

-or-

For version 5.0.1 and higher, click the Monitoring icon, click *Data Collection Engine* and select the data collection engine from the list.

2. Click the *Details* button and click the *Upgrade History* link.

4 EMBEDDED INTELLIGENCE ENGINE BACKUP AND RESTORE

The Avocent® Universal Management Gateway appliance can be used to provide additional functionality to the *Trellis*™ platform. The appliance includes the embedded *Trellis*™ Intelligence Engine data collection engine, which provides the ability to monitor devices and perform other associated functions. The following procedures allow you to back up and restore the embedded *Trellis* Intelligence Engine, as well as restore the appliance and engine after a system failure.

The Avocent Universal Management Gateway appliance firmware is backed up separately from its embedded Intelligence Engine. Instructions to back up and restore the appliance firmware can be found in the Avocent Universal Management Gateway Appliance Installer/User Guide.

NOTE: For instructions to back up and restore the data collected from the *Trellis* Intelligence Engine that is available with the *Trellis*™ Site Manager module, see [TRELLIS™ Intelligence Engine Backup, Restore and Upgrade](#) on page 1.

4.1 Manual Backup

To manually back up the embedded Intelligence Engine version 4.6.2 or earlier:

1. As **admin**, open an **ssh** connection into the appliance.
2. Select option **2** in the login menu to access the shell command line interface.
3. Enter **sh /mss/engine/version.sh** to identify the Intelligence Engine version.
4. Enter **cd /mss/engine/bin** to navigate to the directory that contains the backup and restore tool.
5. Enter **./mss-run BackUp_Restore.sh backup** to perform the backup. The backup time varies depending on the size of the embedded Intelligence Engine database.
6. After the backup is complete, enter the following commands to verify that the embedded Intelligence Engine's files have been backed up:

For embedded Intelligence Engine versions lower than 3.0:

```
cd /var/home
```

```
ll ./db_backup_TODAY/
```

For embedded Intelligence Engine version 3.0 and higher:

```
cd /mss-db/tmpdir
```

```
ll ./db_backup_TODAY/
```

7. Verify the directory `db_backup_TODAY` has been created with all of the files associated with the Intelligence Engine backup.

Example: Backup Directory

```
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 conf
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 elementlibrary
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 mssengine
-rw-r--r-- 1 admin admin 1933121 Oct 17 12:24 mssengine_backup.gz
```

8. Enter **tar -zcvf ./db_backup_TODAY.tar.gz ./db_backup_TODAY/** to tar zip the folder.
9. Enter **md5sum ./db_backup_TODAY.tar.gz > ./db_backup_TODAY.tar.gz.md5** to create an md5sum of the tar.gz file and save the output.
10. Enter the following commands to back up the tar zip file and the md5 sum file to a backup location:

- `scp db_backup_TODAY.tar.gz oracle@<backup_server>:<backup_location><appliance Name>_<Date>`
- `scp db_backup_TODAY.tar.gz.md5 oracle@<backup_server>:<backup_location><appliance Name>_<Date>`

4.2 Automated Backup

A script can be created and copied to the appliance to automatically run a backup. A cronjob runs daily, creates a backup for the embedded Intelligence Engine and then copies the backup to a backup location.

Example: Sample Contents of an MSSbackup.sh File

NOTE: This example assumes the backup location provides an ssh interface and allows for the exchange of SSH keys.

```
cd /mss/engine/bin
./mss-run BackUp_Restore.sh backup
cd /mss-db/tmpdir
tar -zcvf ./db_backup_TODAY.tar.gz ./db_backup_TODAY/
md5sum ./db_backup_TODAY.tar.gz > ./db_backup_TODAY.tar.gz.md5
/usr/bin/scp -r ./db_backup_TODAY.tar.gz oracle@<backup_server>:<backup_location>/db_backup_
TODAY.`date +%F`.tar.gz
/usr/bin/scp -r ./db_backup_TODAY.tar.gz.md5 oracle@<backup_server>:<backup_location>/db_backup_
TODAY.`date +%F`.tar.gz.md5
```

To schedule an automated backup:

1. As **admin**, open an **ssh** connection into the appliance.
2. Select option **2** in the login menu to drop to the shell.
3. Enter **ssh-keygen -t rsa** to generate ssh keys for the admin user.
4. Transfer the public key to the backup server location to the backup user.
 - a. Enter **scp <backupuser>@<backup_location>:~/.ssh/authorized_keys ~/.ssh** to copy the original authorized_keys to the appliance.
 - b. Enter **cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys** to append the new key to authorized_keys.
 - c. Enter **~/.ssh/authorized_keys <backup_user>@<backup_location>:~/.ssh/authorized_keys** to copy the authorized_keys back to the server.
5. As the **root** user, **ssh** to the backup location server and create the backup folder. Enter **backend # mkdir <backup location>**.
6. Change the ownership of the folder to the backup user.
7. Enter **ssh <backup_user>@<backup_location>:~/** to test the automatic log in from the appliance to the backup location.
8. Edit or create the **mssbackup.sh** file and ensure that the last line points to the correct server and appropriate location.
9. As **admin**, use **scp** to copy the file into the **/var/home** folder of the appliance.
10. Navigate to **/var/home** and make the script executable. Enter **chmod +x ./mssbackup.sh**.
11. From the ssh console session to the appliance, set up a cronjob using **crontab -e** to copy the backup file to the back machine every X minutes.

Example: Cronjob for 1:05 AM


```
# Minute Hour Day of Month Month Day of Week Command
# (0-59) (0-23) (1-31) (1-12 or Jan-Dec) (0-6 or Sun-Sat)
5 1 * * * /var/home/mssbackup.sh
```

4.3 Appliance and Embedded Intelligence Engine Restore

In the case of a disaster, the failed appliance is replaced by a new appliance. The appliance should be restored from a full backup to ensure that the new appliance has the same configurations, firmware and patch level. After the appliance is restored, the embedded Intelligence Engine should be restored. Restoring the embedded Intelligence Engine ensures the appliance has the same monitoring configuration and settings as the failed appliance. Any SSL certificates required for communication with the *Trellis™* platform are also restored.

After restoring the appliance, see Restore to restore the embedded Intelligence Engine.

To restore the appliance:

1. From a laptop or similar system, set up an FTP server and verify the appliance backup image is available.
2. Connect the appliance to the FTP server.
3. Using a keyboard and mouse, open the console to the appliance.
4. Reboot the appliance.
5. On the boot prompt, select **nboot recovery**.
6. Enter the following commands to configure the appliance:
 - a. **ifconfig eth0 up**
 - b. **ifconfig eth0 <Appliance IP> netmask <NETMASK>**
7. If required, enter **route add default gateway <GATEWAY IP>** to define the gateway.
8. Enter the following commands to start the netboot process.
 - a. If there is no user on the FTP server, enter the **nboot ftp://<FTP IP>/<Location and filename of the img file>** command.
 - b. Enter the username and password of the FTP server using the **nboot ftp://<FTPusername>:<FTP Password>@<FTP IP>/<Location and filename of the img file>** command. No special characters are allowed.
9. Press **Enter** and wait approximately 45 minutes. During the process, the appliance downloads the image from the FTP server, recreates the required partitions and boot menus and then reboots to complete the process.

4.4 Embedded Intelligence Engine Restore

The file must be extracted before the backup can be restored.

NOTE: The embedded Intelligence Engine can only be restored to the same version as the backup.

To restore the embedded Intelligence Engine:

1. As **admin**, open an **ssh** connection to the appliance.
 2. Select option **2** in the login menu to drop to the shell.
 3. Navigate to the directory for the backup file.
 4. For embedded Intelligence Engine versions lower than 3.0, enter **cd /var/home**.
- or-
- For embedded Intelligence Engine versions higher than 3.0, enter **cd /mss-db/tmpdir**.

-or-

If the directory does not exist, enter **mkdir -p /mss-db/tmpdir** to create the directory.

5. Enter **rm -rf ./db_backup_TODAY/** to remove the folder `./db_backup_TODAY/`, if it exists. Be sure you are in the correct folder.
6. Use `scp` to copy the latest mss-engine backup file and md5 sum file into the appliance folder as follows:

For embedded Intelligence Engine versions lower than 3.0, enter `cd /var/home`.

-or-

For embedded Intelligence Engine version 3.0 and higher, enter `cd /mss-db/tmpdir`.

7. Enter **md5sum ./<backup file name>** and **cat ./<backup file name>.md5** to confirm both outputs match.
8. Enter **tar -zxvf ./<backupfile name>** to extract the files. The `db_backup_TODAY` folder should now exist under the `/var/home/` folder for the Intelligence Engine version 3.0 or lower and `/mss-db/tmpdir/` for Intelligence Engine version 3.0 and higher.
9. Make sure there are no error messages during the extraction. The folder structure in `db_backup_TODAY` appears as follows:

Example: Folder structure in `db_backup_TODAY`

```
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 conf
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 elementlibrary
drwxr-xr-x 3 admin admin 4096 Oct 17 12:24 mssengine
-rw-r--r-- 1 admin admin 1933121 Oct 17 12:24 mssengine_backup.gz
```

10. If the folder structure does not contain the same folders and files, navigate to `/mss/engine/bin` and enter the following: **./mss-run BackUp_Restore.sh restore** to restore the Intelligence Engine. The restore time depends on the size of the Intelligence Engine database.
11. When the restore is complete, enter **/mss/engine/MSScont.sh status** and verify the Oracle Complex Event Processing, Intelligence Engine, ELF, Exporter and node processes are running.

5 REPLACING CERTIFICATES

A certificate replacement procedure must be used to replace expired certificates. Contact Technical Support or Professional Services for the Certificate (SSL/TLS) replacement procedure.

If you need to replace only the *Trellis*™ platform's UI self-signed certificate on the front machine with a new certificate that includes a customized *Trellis*™ published URL, contact Technical Support or Professional Services.

This page intentionally left blank





Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2020 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice

590-1464-501G