## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Preface</td>
<td>iv</td>
</tr>
<tr>
<td>1</td>
<td>12c Forms Provisioning New / Upgrade Requirements</td>
<td>1-1</td>
</tr>
<tr>
<td>2</td>
<td>Forms 12c Platform Clean / Upgrade Install via Command Line</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Accessing Platform Upgrade Utility</td>
<td>2-5</td>
</tr>
<tr>
<td></td>
<td>Running Platform Utility (Command Line): Upgrade Logs</td>
<td>2-6</td>
</tr>
<tr>
<td>3</td>
<td>Forms 12c Platform Clean / Upgrade Install via Upgrade Utility</td>
<td>3-1</td>
</tr>
<tr>
<td></td>
<td>OPERA Forms Upgrade Utility (UI)</td>
<td>3-1</td>
</tr>
<tr>
<td></td>
<td>OPERA Forms Upgrade</td>
<td>3-1</td>
</tr>
<tr>
<td></td>
<td>Logs</td>
<td>3-8</td>
</tr>
<tr>
<td>4</td>
<td>Expand an Existing Cluster by Adding New Node</td>
<td>4-9</td>
</tr>
<tr>
<td></td>
<td>Adding a New Node on AdminServer</td>
<td>4-10</td>
</tr>
<tr>
<td>5</td>
<td>Clean De-Install Of Installed Components (11g &amp; 12C)</td>
<td>5-14</td>
</tr>
<tr>
<td></td>
<td>Running Clean De-Install (Command Line):</td>
<td>5-14</td>
</tr>
<tr>
<td>6</td>
<td>Keystores and wallets on an 12c OPERA Application Server</td>
<td>6-19</td>
</tr>
<tr>
<td>7</td>
<td>Updating an 12c OPERA Application Server with New Certificates</td>
<td>7-20</td>
</tr>
<tr>
<td>8</td>
<td>Applying E-Patch Functionality</td>
<td>8-25</td>
</tr>
</tbody>
</table>
Preface

This document explains the platform utility to be used when building a new forms 12c or upgrading an existing forms 11g to a 12c platform on OPERA 5 Property Services and OPERA Property Cloud Services.

Audience

This document is intended for system administrators, support personnel, and users wanting to build or upgrade to a 12c platform.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>Initial publication.</td>
</tr>
<tr>
<td>August 2019</td>
<td>Added E-patch installation chapter.</td>
</tr>
</tbody>
</table>
12c Forms Provisioning New / Upgrade Requirements

**WARNING:**

OS Compatibility

- Windows 2012 R2 and 2016 servers

**WARNING:**

Make sure to back up any customized forms in OPERA V5 and have them manually converted to 12c so that they can be placed back after 12c server provisioning.

In the case of Pre-Build Application Server provisioning / upgrade (Installed and pre-configured app server from install media), please make sure to copy over entire "micros" folder from existing / old application server to new Pre-Build Application server before starting 12c provisioning.

**WARNING:**

OPERA artifacts must be downloaded and included into the utility before starting 12C server provisioning.

**NOTE:** Important Instructions on how to include OPERA artifacts into the utility

1. Download the required and compatible OPERA version artifacts from MOS (Doc ID 2577659.1).
2. Using "7-Zip", unzip and extract files from downloaded OPERA artifacts zip file.
3. Once extraction is completed, copy entire "opera" folder.
4. Overwrite copied "opera" folder into the following utility folder structure "Forms12CPlatformUpgrade\scripts\core\stage\MICROS\".
Important Instructions for retaining an existing Java KeyStore (JKS)/V5MACHINE

1. Copy the existing JKS file into the scripts/config/clustering/keystores folder. When clustering with multiple nodes, make sure all JKS files for all nodes are placed in this location before provisioning the AdminServer.

2. Once the JKS file is copied to the designated location, rename the existing JKS files with the appropriate computer name/s for all the nodes. Run echo %COMPUTERNAME% from the command line to get the computer name.
   a. Not adhering to the above naming standard will result in unsuccessful provisioning of the servers.
This utility is not supported for the 10G to 12c upgrade path.

Before provisioning 12c, the media will do a clean uninstall of any previously installed 11g installations. This only applies to the upgrade process.

The following components are provisioned as part of this utility.

Uninstalls (applies only to the upgrade process):

- Oracle HTTP Server (OHS)
- Forms and Reports
- Oracle Fusion Middleware
- Oracle SQL Client
- JDK

Installs (applies to both clean and upgrade process):

- JDK 1.8 (8u201-windows-x64)
- Oracle Fusion Middleware 12.2.1.3.0
- Oracle Forms & Reports 12.2.1.3.0
- Oracle OHS 12.2.1.3.0
- Oracle Database Client 32-bit 12.2.0.1
- Provisions and starts Managed Servers (WLS_HOME, WLS_FORMS, WLS_REPORTS)
- Provisions and starts Reports Server instance

---

**NOTE: Important Instructions for retaining the existing JKS / V5MACHINE**

1. Make sure to have all of the computer names for all of the nodes before provisioning the AdminServer. Run echo %COMPUTERNAME% from the command line to get the computer name.

2. Provision the AdminServer first. Do not start provisioning any other nodes until the AdminServer has been provisioned successfully.

3. Once the AdminServer is provisioned successfully, copy the entire Config folder from the AdminServer and paste/overwrite it to the same location on every node (For example, Node 2, Node 3 and so on.).
   
   a. All installation must be done on the same drive for all nodes. (Example: If "AdminServer" is installed on drive "D:\" then all subsequent nodes should also be installed on drive "D:\")

4. After successful provisioning of AdminServer, all remaining nodes can be provisioned simultaneously.
Figure 1 Provisioning Components (AdminServer Vs Node 2 Succeeding Nodes)

**Admin Server**
- **Applied CPU Patches:**
  - July 2019

**Node 2 ... Succeeding Nodes**
- **Applied CPU Patches:**
  - July 2019
Forms 12c Platform Clean / Upgrade Install via Command Line

The platform utility is used to build a new Forms 12c or upgrade an existing Forms 11g to a 12c platform.

Accessing Platform Upgrade Utility

Download the utility from the following location.

**NOTE:** Important 12c Documentation References

New 12c Directory Paths for Reports Configuration Files
https://support.oracle.com/epmos/faces/DocumentDisplay?id=1373210.1
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2071812.1
Running Platform Utility (Command Line):

Below are 2 ways to invoke command line utility:

A. Running "12C_Forms_Platform_Upgrade.CMD" from windows explorer by selecting "Run as administrator". This approach requires user to enter configuration data and password at the very first step of 12c provisioning (Please follow steps 1 through 7)

B. Invoking "12C_Forms_Platform_Upgrade.CMD" from command line with required arguments, which is then would be completely silent (Please follow steps 8 through 12)

1. In the 12CPlatformUpgrade folder, select 12C_Forms_Platform_Upgrade. CMD, then right click and select Run as administrator.
2. When prompted, press any key to continue.

Figure 2 Configuration File CMD Prompt

3. The config file opens and the following parameters must be entered and saved before continuing the upgrade.

The following parameters are mandatory for a Single Domain / Node install:

- OPERA_DB_HOST_NAME: Database Host Name. The RAC DB is only supported when the SCAN (Single Client Access Name) feature is configured. SCAN provides a single domain name via DNS, allowing end-users to address a RAC cluster as if it were a single IP address.
- OPERA_DB_LISTEN_PORT: Database listening port
- OPERA_DB_SERVICE_NAME: Database service name
- INFRA_DB_HOST_NAME: INFRA Database Server Name
- INFRA_DB_SERVICE_NAME: Infra DB service name
- INFRA_DB_LISTEN_PORT: Infra DB listening port
• INFRA_DB_SYSDBA_ROLE_USER: Database User can now be either a SYSDBA role user or a normal user who has been granted access to create schemas for RCU.

• INFRA_DB_USER_ROLE: Accepted values are “sysdba” for SYSDBA role user and “normal” or normal user who has granted access.

• OPERA_DB_USER: Database user name

• INFRA_RCU_PREFIX: RCU prefix for Infra Database. Make sure the value is unique within the DB server. The value provided should only be alphanumeric and should not be more than 12 characters.
  – While provisioning a Cluster with multiple nodes, INFRA schemas will be created only once at the time of the AdminServer provisioning.

• INSTALL_ON_DRIVE_LETTER: Enter the drive letter with no colon where 12c provisioning is to be executed (For example: D).

The following parameters are only required when setting up for a Cluster with Multiple Nodes. The Utility can support up to 30 nodes.

• COMPUTER_NAME_1: This computer will be the primary WebLogic node where the AdminServer resides. To find the computer name, logon to the computer and execute the following command from the command line: echo %COMPUTERNAME%

• COMPUTER_NAME_2: This will be WebLogic node 2

• COMPUTER_NAME_3: This will be WebLogic node 3

• COMPUTER_NAME_4: This will be WebLogic node 4

• COMPUTER_NAME_5: This will be WebLogic node 5

• COMPUTER_NAME_6: This will be WebLogic node 6

• COMPUTER_NAME_7: This will be WebLogic node 7

• COMPUTER_NAME_8: This will be WebLogic node 8

• COMPUTER_NAME_9: This will be WebLogic node 9

• COMPUTER_NAME_10: This will be WebLogic node 10

• COMPUTER_NAME_15: This will be WebLogic node 15

• COMPUTER_NAME_16: This will be WebLogic node 16

• COMPUTER_NAME_17: This will be WebLogic node 17

• COMPUTER_NAME_18: This will be WebLogic node 18

• COMPUTER_NAME_19: This will be WebLogic node 19

• COMPUTER_NAME_20: This will be WebLogic node 20

• COMPUTER_NAME_21: This will be WebLogic node 21

• COMPUTER_NAME_22: This will be WebLogic node 22

• COMPUTER_NAME_23: This will be WebLogic node 23

• COMPUTER_NAME_24: This will be WebLogic node 24
Chapter 2

Forms 12c Platform Clean / Upgrade Install via Command Line

- COMPUTER_NAME_25: This will be WebLogic node 25
- COMPUTER_NAME_26: This will be WebLogic node 26
- COMPUTER_NAME_27: This will be WebLogic node 27
- COMPUTER_NAME_28: This will be WebLogic node 28
- COMPUTER_NAME_29: This will be WebLogic node 29
- COMPUTER_NAME_30: This will be WebLogic node 30

- The Command window will display values entered in the config file for final user verification. Once everything is validated, enter the OPERA DB password when prompted and press Enter.

Figure 3 Schema Password Prompt

4. The Utility prompts the user to enter a single password, which will be used for login to the WebLogic console, Node Managers, JKS, cacerts, and wallet passwords. Type the password and press Enter.
NOTE:
When the JKS is being retained as part of provisioning, make sure that the current password for JKS is the same as the one that is being supplied. Not adhering to this standard will have will result in an unsuccessful upgrade.

Figure 4 INFRA SYSDBA Password Prompt

5. The Utility prompts for the INFRA SYSDBA role password. Enter the password and press Enter.

Figure 5 SYS DBA Role password For RCU / INFRA Schemas creation Prompt

6. The Utility prompts for the INFRA schemas password. Enter the password and press Enter.
7. Copy config.txt from the following location "Forms12CPlatformUpgrade\scripts\config\sample" and paste it in "Forms12CPlatformUpgrade\scripts\config"

8. Open the "config.txt" file from "Forms12CPlatformUpgrade\scripts\config", fill out all the required information, and then save the file.

9. Open Command Prompt by right clicking the program icon and selecting "Run as an administrator"

10. Run "12C_Forms_Platform_Upgrade.CMD" with the following arguments as shown below and press Enter. In case of OPERA DB and SYS DB passwords with an exclamation point (!) character, the exclamation point character must be prefaced by two carrot (^) characters. (Ex: If the password is "operadbpwd!" then it should be passed as "operadbpwd^^!") as shown below in Figure 7.1

   OPERA_DB_PASSWORD
   PROV_PASSWORD_FOR_ALL
   INFRA_RCU_SYSDBA_PASSWORD
   INFRA_RCU_PASSWORD

---

Figure 6 RCU Schemas Password Prompt

Figure 7 12c_Forms_Platform_Upgrade.CMD Arguments Order
11. Once message "Press any key to continue...." is displayed, press any key. The config.cmd file is then displayed with pre-populated information for final user verification. After everything is validated, close the Config file.

12. While installing Forms and Reports, the installation might take longer when it reaches 90% completion.

13. Once the installation is complete, press Ctrl + BREAK or Ctrl + C and answer N to the question Terminate batch job.
14. The WebLogic Console window will open after being successfully upgraded. Log in with username and password credentials.

15. After logging into the WebLogic console, click Environment under Domain Structure and then click on Servers.

16. Verify that the managed servers are up and running.
Upgrade Logs

Logs can be found in the following locations:

Utility Drive (for example: D):\Forms12CPlatformUpgrade\logs
\Users\\<<user name>>\AppData\Local\Temp
3

Forms 12c Platform Clean / Upgrade Install via Upgrade Utility

OPERA Forms Upgrade Utility (UI)

The OPERA Forms Upgrade Utility (OFUU) provides a seamless transition when provisioning new or from existing forms 11g to 12c platforms.

OPERA Forms Upgrade

In the 12CPlatformUpgrade folder, select OFUU.BAT, then right-click and click Run as administrator.

1. OPERA Forms Upgrade Utility should be displayed.

Figure 14 OPERA Forms Upgrade Utility

2. OPERA Database Details: Enter the OPERA DB and INFRA DB parameters. Successful connection is required before moving to the next step. Check your connection by clicking the Test Connection button.

The following lists the mandatory parameters that are required for Single Domain / Node install:

- OPERA DB Host Name: Database Host Name. RAC DB is only supported when the SCAN (Single Client Access Name) feature is configured. SCAN provides a single domain name via DNS, allowing you to address a RAC cluster as if it were a single IP address.
Chapter 3
Forms 12c Platform Clean / Upgrade Install via Upgrade Utility

- OPERA DB Listening Port: Database listening port.
- OPERA DB Service Name: Database service name.
- OPERA DB User Name: Opera Database user name.
- OPERA DB Password: Opera Database password.
- OPERA Host is the same as INFRA machine: Selecting this checkbox will auto-populate INFRA DB Host Name and INFRA DB Service Name.
- INFRA DB Host Name: INFRA Database Server Name.
- INFRA DB Service Name: Infra DB service name.
- INFRA DB SYS User: INFRA Database User with Sys DBA role.
- INFRA DB SYS Password: INFRA Database password.

3. Checklist Step: This screen validates certain prerequisites. After clicking the **Start** button click **Next** after a successful validation.

- Choose the drive to install: Select the drive from list of values where 12c provisioning is to be executed.
- Verify Hardware: Verifies hardware requirements. Required minimum of 2 core CPU and 12 GB RAM.
- Verify DB Version: Required DB of 11.2.0.4.0 or higher.
- Verify Invalid Objects in Database: Checks for any invalid objects in the DB and notifies the user about invalid objects before continuing 12c provisioning. The utility does not recompile existing invalid objects.
- Verify OPERA Version: Checks for underlying OPERA version. OPERA version 5.0.05.00 or higher is required for 12c provisioning.

Figure 15 OFUU Checklist Screen

4. Parameter Settings Step:
• Unified Password: User has to enter a single password, which will be used for the WebLogic console, Node Managers, JKS, cacerts, and wallet passwords.

NOTE:

If JKS is being retained as part of provisioning, make sure that the current password for JKS is the same as the one that is being supplied. Not adhering to this standard will result in unsuccessful provisioning of servers.

• RCU Schemas Password: Enter INFRA schemas password. The password that is going to be entered here will be used to access the newly created Infra schemas that gets created as part of 12c provisioning.

• INFRA RCU Prefix: RCU prefix for Infra Database. Make sure the value is unique within DB server. Value provided should only be alphanumeric and should not be more than 12 characters. While provisioning Cluster with multiple nodes, INFRA schemas will only get created once, at the time of the AdminServer provisioning.

• Node Specification:
  – Single Node: Selecting this option will create a cluster with single node. Click OK button and then Click Next.

  Figure 16 OFUU Parameter Settings Screen

  – Multiple Nodes: Selecting this option allows users to enter computer names for all nodes. The first computer name that is entered will be marked as the AdminServer and all other consecutive nodes will be marked in sequential order.
  – The Utility can support up to 30 nodes. Users can update existing computer names by double clicking on the computer name. Then Click the OK button and then Click Next.
5. Parameter Review: This step allows users to review the information that has been entered in previous steps and all information will be displayed in read-only mode. By clicking the **Back** button users can update existing parameters if required. Click the **Next** button once confirmed.
6. **Installation:** This step lists out all core components that will be provisioned and will display individual component progress and overall progress of the installation. Click the **Start** button to start 12c provisioning.

**NOTE:**

While 12c provisioning is running, users will see command windows and Oracle Universal Installers being opened and / or closed automatically. Refrain on taking any actions while the process completes.
Figure 20 OFUU Installation Screen
7. The WebLogic console window should be opened after the successful upgrade. If not, access the console and login with appropriate credentials.

Figure 21 WebLogic Login Screen

8. After logging into WebLogic console, click Environment under Domain Structure and then click Servers.
9. Verify that the managed servers are up and running.

**Figure 23 WebLogic Managed Servers Running Screen**

Logs

Logs can be found in the following locations:

- Utility Drive (for example, D):\Forms12CPlatformUpgrade\logs
- \Users\<<user name>>\AppData\Local\Temp
4

Expand an Existing Cluster by Adding New Node

**NOTE:** Important Instructions for retaining the existing JKS / V5MACHINE

1. Copy the existing JKS file into the scripts/config/clustering/keystores folder. When clustering with multiple nodes, make sure all JKS files for all nodes are placed in this location before provisioning the AdminServer.

2. Once the JKS file is copied to the designated location, rename the existing JKS files with the appropriate computer name/s for all the nodes. Run echo %COMPUTERNAME% from the command line to get the computer name.
   
   a. Not adhering to the above naming standard will result in unsuccessful provisioning of the servers.

**NOTE:** Important Instructions for expanding an existing cluster

1. Make sure to have all of the computer names for all of the nodes before provisioning the AdminServer. Run echo %COMPUTERNAME% from the command line to get the computer name.

2. Provision the AdminServer first. Do not start provisioning any other nodes until the AdminServer has been provisioned successfully.

3. Once the AdminServer is provisioned successfully, copy the entire Config folder from the AdminServer and paste/overwrite it to the same location on every node (For example, Node 2, Node 3 and so on.).

4. Multiple provisioning utilities should not be run simultaneously, so provisioning should be one node at a time.
   
   a. All installation must be done on the same drive for all nodes. (Example: If "AdminServer" is installed on drive "D:\" then all subsequent nodes should also be installed on drive "D:\")
Adding a New Node on AdminServer

1. Select "Expand_exiting_cluster.cmd" in the scripts folder, right click and select "Run as administrator" option.

   Figure 24 Expand Existing Cluster Command Prompt

   ![Command Prompt](image)

   Note: Configuration file will be opened in Notepad. Update and review accordingly. Afterwards, close the Notepad, and installation will continue automatically.

   **IMPORTANT:** This script can only be executed on the AdminServer machine.

   Press any key to continue . . .

2. Config.txt file will be opened, enter COMPUTER_NAME of the new nodes that are going to be added to existing cluster. Do not change any other configuration values from this file other than providing computer names for new nodes. Once completed, save the file and close.
3. Enter the password which will be used for Weblogic console, Node Managers, JKS, cacerts, and wallet passwords and press **Enter**.

**NOTE:**

If JKS is being retained as part of provisioning, make sure that the current password for JKS is the same as the one that is being supplied. In case of clustering, make sure to enter the same password when provisioning nodes that are part of the same cluster. Not adhering to this standard will have adverse impact and will result in unsuccessful upgrade.
4. The script will start executing and wait for the script to complete (as shown below).
Provisioning Platform on New Node

Make sure entire "config" folder is copied to new node before continuing provisioning. Users can provision new node by either running the command line or UI utility (OFUU).
5 Clean De-Install Of Installed Components (11g & 12C)

The utility can only perform permanent uninstallations of existing 11g and 12C installed components. However, running this utility will not re-install any 12C components. The components listed below will be uninstalled as part of this utility.

Components to be Uninstalled:
- Oracle HTTP Server (OHS)
- Forms and Reports
- Oracle Fusion Middleware
- Oracle SQL Client
- JDK

Running Clean De-Install (Command Line):

1. Run the “Deinstall_11g_and_12c.CMD” file as administrator. It can be found under the Scripts/deinstall folder
2. When prompted, press any key to continue.
3. After pressing any key, configuration file should be opened in notepad. Enter all required details in the config file, then save and close.

   Please refer to step 3 under Running Platform Utility (Command Line) in this document for further details.

4. The utility should continue un-installation of components. Below are few screenshots when utility is in-installing.
Figure 3 Random screenshots while un-installing
Chapter 5
Clean De-Install Of Installed Components (11g & 12C)

```
Checking if CPU speed is above 300 MHz. Actual 2196 - Passed
Checking swap space must be greater than 512 MB - Passed
Checking if this platform requires a 64-bit JVM. Actual 64 - Passed (64-bit not required)
Checking temp space must be greater than 300 MB. Actual 48271 MB - Passed
Log: C:\Users\linboard\AppData\Local\Temp\2019\08\04\19\oracle\install\190810-08-45-15-32336983697.log
Setting ORACLE_HOME to D:\ORACLE\APP\12c\omg
Copyright (c) 1999, 2019, Oracle and/or its affiliates. All rights reserved.
Reading response file...
Starting silent deinstallation...
Percent Complete: 10
Percent Complete: 20
Percent Complete: 30
Percent Complete: 40
```

```
Checking 12c JHS installation on drive C:

Checking 12c JHS installation on drive D:
```

```
Uninstalling Oracle Grid Control 13.0.4.0.0 from \ORACLE\OMG
Uninstalling Oracle HTTP Server 12213 from drive D:
```

```
The specified service does not exist as an installed service.
[SC] OpenService FAILED 1060:
The specified service does not exist as an installed service.
```

```
uninstall node_manager_ohs.cmd
exit Code: 0
Wed 06/19/2019
04:30 PM
```

```
stop_reports_server.cmd:start
The system cannot find the path specified.
```

```
stop_node_manager_ohs.cmd
exit Code: 0
Wed 06/19/2019
04:39 PM
```

```
delete_reports_server.cmd:start
The system cannot find the path specified.
```

```
```
```
5. Once the uninstallation is complete, press **Ctrl + BREAK** or **Ctrl + C** and answer **N** to the question Terminate batch job.
6 Keystores and wallets on an 12c OPERA Application Server

The OPERA 11g Application Server makes use of some JAVA keystores and Oracle wallets and each of the files involved has a specific role.

The files involved are:

- \micros\wallets\ewallet.p12 (and cwallet.sso) is the “identity store” for the OHS (Apache) server. It should always include the server cert for the web server and the CA certs used to sign that certificate. With a self-signed cert, the server cert and the CA cert are the same. The installation wizard generates this file by converting the next file

- \micros\opera\security\V5MACHINE.jks is the “identity store” for the WLS server. The managed servers use a certificate out of this keystore (accessed by alias) to act as the server cert for the WLS SSL ports. Details of the config are available via the WLS admin console. This file is basically the same as the previous file but used by a different server component.

- %JAVA_HOME%\jre\lib\security\cacerts is the “trust store” for the JDK. Any program running via the JDK will (by default) use the CA certs in this file as a trusted CA list. So things like the WLST scripting tool will use it to decide if the SSL connection it is making is trusted or not. Since we use SSL for deploying applications to WLS managed servers, the CA used to sign the WLS server cert (the previous file) must be in here as a trusted certificate. Any outbound calls from java applications running in the managed servers on the machine will do the same.

A couple other points:

- There is no harm in installing additional CA certs that are expected to be trusted in any of the files. Sometimes this is unnecessary but no harm done. The only required ones are ones used for connections out of components using that file.

- The way JKS files work is that when you first create a client certificate (-genkey) in a JKS keystore, the certificate will exist inside as a self-signed certificate. This is expected. The next steps are to export the certificate signing request, get it signed, and then import it back in overwriting the self-signed cert with a CA signed certificate. If you intend to use self-signed, then the export/import part are skipped.

- The wizard completes the installation using a self-signed certificate. This should be replaced by valid certificates once the wizard completes.

More information can be found at the below locations:

http://docs.oracle.com/cd/E29597_01/fusionapps.1111/e14496/securing.htm#CHDJGHC

http://docs.oracle.com/middleware/1212/webtier/HSADM/getstart.htm#HSADM860
Chapter 7: Updating an 12c OPERA Application Server with New Certificates

7 Updating an 12c OPERA Application Server with New Certificates

The wizard completes the installation using a self-signed certificate. You can replace them with valid certificates once the wizard completes.

You can use several methods to update the keystores and wallets with new certificates. This chapter documents recreating the wallets and keystores as a way of using new certificates. There are several other ways in which WebLogic administrators can replace the certificates and there is a good amount of Oracle documentation available on MOS and other sources in order to assist.

**NOTE:**

The keystore that is created when the certificate request is being created and the certificate that is obtained from that certificate request are a “pair”. You cannot create the keystore and create a certificate request / obtain the certificate separately, even if the same hostname is being used.

1. Take backups of and move the files in the below folders away:
   a. D:\MICROS\wallets
   b. D:\MICROS\opera\security
2. Create a copy of the file cacerts in D:\ORA\JDK\jre\lib\security
3. Create the new certificate request:
   In a CMD window type the below and validate the output/response:

   **WARNING:**
   
   Only change the entries that are bolded in the below command. It is important that the alias name of V5MACHINE is preserved.

   ```bash
   D:\ora\JDK\jre\bin\keytool.exe -genkey -keyalg RSA -dname "CN=servername, O=Oracle, C=US, ST=Florida, L=Naples" -alias V5MACHINE -keypass password -keystore D:\MICROS\opera\security\V5MACHINE.jks -storepass password -validity 1461 -keysize 2048
   ```
D:\ora\JDK\jre\bin\keytool.exe -certreq -v -alias V5MACHINE -file D:\MICROS\opera\security\servername.csr -keypass password -storepass password -keystore D:\MICROS\opera\security\V5MACHINE.jks

4. Submit the certificate request to your CA.

5. Once you receive the certificate and root certificate(s), navigate to D:\ORA\JDK\jre\lib\security and place the original cacerts file from the JDK media in this location.

6. Open a CMD window and run the commands below and validate the output/response:

D:\ora\JDK\jre\bin\keytool.exe -storepasswd -new password -keystore D:\ora\JDK\jre\lib\security\cacerts -storepass changeit

D:\ora\JDK\jre\bin\keytool.exe -delete -keystore D:\ora\JDK\jre\lib\security\cacerts -alias ttelesecglobalrootclass2ca -storepass password -noprompt

D:\ora\JDK\jre\bin\keytool.exe -delete -keystore D:\ora\JDK\jre\lib\security\cacerts -alias ttelesecglobalrootclass3ca -storepass password -noprompt
7. Copy the certificate and root certificate(s) to D:\MICROS\opera\security
8. Import the root certificate(s) and certificate by opening a CMD window and running the commands below (ftdevca2.crt is the root certificate in this example) and validate the output/response.

```bash
set java_home=D:\ORA\JDK

cd /d %JAVA_HOME%\jre\lib\security

%java_home%\jre\bin\keytool -importcert -file D:\micros\opera\security\rootCA.crt -alias rootCA -keystore D:\micros\opera\security\V5MACHINE.jks -storepass password -storetype JKS -noprompt

%java_home%\jre\bin\keytool -importcert -file D:\micros\opera\security\rootCA.crt -alias rootCA -keystore cacerts -storepass password -storetype JKS -noprompt

%java_home%\jre\bin\keytool -importcert -file D:\micros\opera\security\servername.cer -alias V5MACHINE -keystore D:\micros\opera\security\V5MACHINE.jks -storepass password -storetype JKS -noprompt

%java_home%\jre\bin\keytool -importcert -file D:\micros\opera\security\servername.cer -alias V5MACHINE -keystore cacerts -storepass password -storetype JKS -noprompt

%java_home%\jre\bin\keytool -importcert -file D:\micros\opera\security\rootCA.crt -alias rootCA -keystore
```
D:\ORA\12213ohs\wlserver\server\lib\DemoTrust.jks -storepass
"DemoTrustKeyStorePassPhrase" -storetype JKS -noprompt

%java_home%\jre\bin\keytool -importcert -file
D:\micros\opera\security\servername.cer -alias v5machine -keystore
D:\ORA\12213ohs\wlserver\server\lib\DemoTrust.jks -storepass
"DemoTrustKeyStorePassPhrase" -storetype JKS -noprompt

⚠️ WARNING:

If the output of the importcert command of the actual server certificate (3rd
command in the below screenshot) does not return with “Certificate reply
was installed in keystore”, the certificate was not correctly added to the
keystore. The most likely source of the issue would be the wrong files
were used.

9. Now that the root and server certificates have been installed in the keystore, you
need to recreate the Oracle wallet. Open a CMD window, run the commands below
and validate the output/response:

set JAVA_HOME=D:\ora\JDK

D:\ORA\MWFR\12cappr2\oracle_common\bin\orapki.BAT wallet create -
wallet D:\micros\opera\security -pwd password -auto_login

D:\ORA\MWFR\12cappr2\oracle_common\bin\orapki.BAT wallet
jks_to_pkcs12 -wallet D:\MICROS\opera\security -pwd password -
keystore D:/micros/opera/security/V5MACHINE.jks -jkspwd password
10. Now you must update the security on the wallet files. Open a CMD window, and run the commands below and validate the output/response:

```
echo 'Y'|CACLS D:\micros\opera\security\cwallet.sso /E /T /C /G "Everyone":F
```

11. Move cwallet.sso and ewallet.p12 from D:\MICROS\opera\security to D:\MICROS\wallets

12. Import any additional certificates that are needed into the Oracle wallet using the Oracle Wallet Manager GUI.

13. Reboot the server.

**NOTE:**

In order to obtain more information regarding commands being used in this document, please read the below documentation:

```
http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html
```
Chapter 8 Applying E-Patch Functionality

8 Applying E-Patch Functionality

E-Patch functionality has been implemented as of the 19.10.0.4 release. If the E-Patch functionality is being applied for the first time on a 19.10.x.x release, follow steps 1 through 3, otherwise the first 3 steps can be ignored.

1. Open the E-Patch Zip archive using 7-Zip and open the scripts folder as shown below.

   Figure 1 Opening “scripts” folder from E-Patch archive

2. Right click the “Utility_Patch.CMD” file, and click the **Copy To** option, then select the existing 12C Utility location and make sure that file is copied under the same scripts folder as shown below.

   Figure 2 Copying “Utility_Patch.CMD” to existing 12C utility under “\scripts” folder
3. From the E-Patch archive open the “\scripts\core\stage\” directory, right click the “7z1900-extra” folder, and click the **Copy To** option. Then select the existing 12C Utility and make sure that file is copied under the same folder (\scripts\core\stage) as shown below.

**Figure 3 Copying “7z1900-extra” folder to existing 12C utility under “\scripts\core\stage\”**
4. Open command line as administrator and run “Utility_Patch.CMD” from the existing 12C Utility location by passing E-Patch zip file location as an argument as shown below and press Enter.

Figure 4 Executing “Utility_Patch.CMD” in order to apply E-Patch
5. After pressing **Enter**, the utility will start extracting and will make sure that all E-Patch related files will be placed / overwritten in their respective locations under the existing 12C Utility as shown below.

**Figure 5 Extracting E-Patch related files to their respective locations**

![Extracting E-Patch related files to their respective locations](image)

6. Press any key to continue once patching of the utility is completed successfully as shown below.

**Figure 6 Utility Patch successful message**

![Utility Patch successful message](image)

7. Provisioning of 12C server can now be continued from either the command line or Upgrade Utility (OFUU).