



Codar

Software Version: 1.7

Upgrade Guide

Document Release Date: July 2016

Software Release Date: July 2016



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© 2015 - 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

The OpenStack® Word Mark and the Square O Design, together or apart, are trademarks or registered trademarks marks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the Software Support site or click **Create an Account** on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your sales representative for details.

Support

Visit the software support site at: <https://softwaresupport.hpe.com>.

Hewlett Packard Enterprise software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

Contents

Overview	5
Directories affected by upgrade	5
New directories and content	6
Preserved directories and content	6
Backed up directories and content	6
Customized files affected by upgrade	6
Customized files by location	7
Initial setup	12
Export HPE Operations Orchestration certificate	18
Run upgrade installer	19
Run upgrade installer on Windows	19
Run upgrade installer on Linux	26
Applying the Codar license	33
Update Codar	34
Customize SSL/Security	34
Files, actions, and locations	35
Import certificates into Codar's truststore	37
Customize manually configured files	39
Remount shared file systems on Linux	39
Restart Codar services	39
Restart Codar service on Windows:	39
Restart Codar service on Linux	39
Customize Codar	40
Configure Codar Console properties	40
Customize Codar Console dashboard	41
Configure Codar Console to import large archives	43
Customize Codar Console session timeout	43
Customize Codar Console dashboard title	44
Add custom graphic files or dynamic query scripts	45
Customize Codar tools	46

Customize Codar database user	48
Customize Codar seeded users	49
Integrate Codar with common access card	50
Configure Identity Management component	55
Configure IPv6	57
Configure JBoss password vault	57
Configure Oracle RAC	58
Configure Codar to use a single sign-on	58
Integrate Codar with SiteMinder	62
Upgrade shortcuts on Windows	67
Deploy content pack for topology designs	69
Verify deployed content packs	69
Deploy Operations Orchestration and component tool content packs	70
Import service designs	72
Upgrade resource providers	73
Clear web browser cache	74
Restart Codar service	75
Restart Codar service on Windows:	75
Restart Codar service on Linux	75
Package deployment behavior post upgrade	76
Appendix A: Cross-product upgrade between Codar and Cloud	
Service Automation	77
Send documentation feedback	78

Overview

This guide provides information necessary to upgrade your HPE Codar application from version 1.50 and 1.60 to 1.7. Successful implementation requires knowledge of the integrated products, as well as Codar.

Information in this guide augments information provided in the integrated products documentation but is not intended to replace that documentation. Primary product documentation contains the most up-to-date information. Cross references are provided to those documents where appropriate.

For information about Codar, see the *Codar Concepts Guide*. Review the *Codar System and Software Support Matrix* for version requirements.

You must perform the following steps. It is recommended that you perform each step in the following order:

1. Review the ["Directories affected by upgrade" below](#) and ["Customized files affected by upgrade" on the next page](#).
2. Perform ["Initial setup" on page 12](#).
3. ["Run upgrade installer" on page 19](#).
4. ["Update Codar" on page 34](#)
5. ["Customize Codar" on page 40](#)
6. ["Deploy content pack for topology designs" on page 69](#)
7. ["Import service designs" on page 72](#)
8. ["Upgrade resource providers" on page 73](#)
9. ["Clear web browser cache" on page 74](#)
10. ["Restart Codar service" on page 75](#)

Directories affected by upgrade

When Codar is upgraded, new directories and content are added and existing directories and content are preserved, backed up, or updated. The following is a list of the affected directories where `CSA_HOME` is the directory in which Codar is installed: on Windows, `C:\Program Files\HPE\Codar` or on Linux, `/usr/local/hpe/codar`.

New directories and content

- CSA_HOME\Codar_1_70_0_installation

Preserved directories and content

Preserved directories and content are not affected by the upgrade. If these directories existed before the upgrade, they are preserved during the upgrade, and remain on your system after the upgrade.

- CSA_HOME\CSAKit-4.6

Backed up directories and content

- CSA_HOME\node.js
(backed up to CSA_HOME\Codar_1_70_0_installation\Backup\node.js)
- CSA_HOME\portal
(backed up to CSA_HOME\Codar_1_70_0_installation\Backup\portal)
- CSA_HOME\jboss-as\standalone\deployments*.war
(backed up to CSA_HOME\Codar_1_70_0_installation\Backup\standalone*.war)
- CSA_HOME\jboss-as\domain.*
(backed up to CSA_HOME\Codar_1_70_0_installation\Backup\domain\)

Customized files affected by upgrade

Before Codar is upgraded (now called Codar, you may need to back up customized files if they are not automatically restored or backed up by the upgrade installer. Automatically restored files retain their customizations after the upgrade. Automatically backed up files have been saved to the backup directory but must be manually restored after the upgrade.

This section lists customized files by location. The customized files listed are based on the features that you selected as being configured, customized, or used prior to the upgrade.

If you want to configure, customize, or use any of these features for the first time, see the following guides for more information: *Codar Configuration Guide* and *Codar Console Help*.

For files listed by feature and the actions to perform, see "[Customize Codar](#)" on page 40. For a list of customized files that must be manually backed up, see "[Initial setup](#)" on page 12.

Caution: If you customized a file that is not listed here, you must manually back up this file (to a directory outside of `CSA_HOME`) before running the upgrade installer and then manually restore the file after running the upgrade installer. If you do not back up this file, the customizations will be lost after running the upgrade installer.

Customized files by location

`CSA_HOME\jboss-as\bin\`

Field	Action
<code>standalone.bat</code> (Windows)	Automatically restored
<code>vault.bat</code> (Windows)	Automatically restored
<code>standalone.conf</code> (Linux)	Automatically restored
<code>vault.sh</code> (Linux)	Automatically restored

`CSA_HOME\jboss-as\standalone\configuration\`

Field	Action
<code>*.cer</code>	Automatically restored
<code>.keystore</code>	Automatically restored
<code>standalone.xml</code>	Automatically backed up, manually restore (for common access card) Automatically restored (for all other features)

`CSA_HOME\jboss-as\standalone\deployments\csa.war\custom\`

Field	Action
<code>message.properties</code>	Automatically restored

CSA_HOME\jboss-as\standalone\deployments\csa.war\custom-content\

Field	Action
index.jsp	Automatically restored

CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\

Field	Action
config.json	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\messages\common\

Field	Action
message.properties	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\deployments\csa.war\images\

Field	Action
*.gif, *.jpeg, *.jpg, *.png	Automatically restored

CSA_HOME\jboss-as\standalone\deployments\csa.war\propertysources\

Field	Action
*.jsp	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\

Field	Action
applicationContext.xml	Automatically backed up, manually restore
applicationContext-security.xml	Automatically restored (for SiteMinder only) Automatically backed up, manually restore (for the following feature(s): single sign-on, common access)

Field	Action
	card, Codar seeded users)
ssologout.jsp	Automatically backed up, manually restore
web.xml	Automatically backed up, manually restore (for the following feature(s): Codar Console: session timeout, SiteMinder)

CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\

Field	Action
csa.properties	Automatically restored
log4j.properties	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\

Field	Action
csa-consumer-users.properties	Automatically backed up, manually restore
web.xml	Automatically backed up, manually restore
hpssoConfig.xml	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\

Field	Action
applicationContext.properties	Automatically restored
applicationContext.xml	Automatically backed up, manually restore
applicationContext-common.xml	Automatically restored
applicationContext-security.xml	Automatically backed up, manually restore
applicationContext-v0.xml	Automatically backed up, manually restore

CSA_HOME\jboss-as\standalone\logs\

Field	Action
* all	Automatically backed up, manually restore

CSA_HOME\portal\conf\

Field	Action
* all	Automatically restored

CSA_HOME\portal\node_modules\mpp-ui\dist\locales*\

Field	Action
rb.json	Automatically backed up, manually restore

CSA_HOME\portal\node_modules\mpp-ui\dist\themes*<theme_directory>*\styles\

Field	Action
main.css	Automatically backed up, manually restore

CSA_HOME\portal\node_modules\mpp-ui\dist\themes\default\styles\

Field	Action
main.css	Automatically backed up, manually restore

CSA_HOME\portal\node_modules\mpp-ui\dist\themes\pilot\styles\

Field	Action
main.css	Automatically backed up, manually restore

CSA_HOME\Tools\db-purge-tool\

Field	Action
config.properties	Automatically backed up, manually restore

CSA_HOME\Tools\ProcessDefinitionTool\

Field	Action
db.properties	Automatically backed up, manually restore
HP00InfoInput.xml	Automatically backed up, manually restore

CSA_HOME\Tools\ProviderTool\

Field	Action
config.properties	Automatically backed up, manually restore
provider.xml	Automatically backed up, manually restore

CSA_HOME\Tools\SchemaInstallationTool\

Field	Action
config.properties	Automatically backed up, manually restore

CSA_HOME\openjre\lib\security\

Field	Action
cacerts	Manually back up, manually restore
java.security	Manually back up, manually restore

<user-specified location>

Field	Action
*.jar (for dynamic queries)	Manually back up, manually restore
*.jsp (custom for the Codar dashboard defined in the CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json configuration file)	Manually back up, manually restore

Field	Action
keystore file (defined by the certificate-key-file property of the connector attribute in CSA_HOME\jboss-as\standalone\configuration\standalone.xml)	Manually back up, manually restore

Initial setup

Before you run the upgrade installer, the following steps must be completed.

- The following files must be manually backed up outside of CSA_HOME (these files are not automatically restored nor backed up by the upgrade installer):
 - CSA_HOME\openjre\lib\security\cacerts
 - CSA_HOME\openjre\lib\security\java.security
 - The keystore file defined by the certificate-key-file property of the connector attribute in CSA_HOME\jboss-as\standalone\configuration\standalone.xml if you are not using the default keystore file (the default keystore file is automatically backed up and restored)
 - Any .jar files used by dynamic query scripts. Any Java server page (.jsp) files created for the Codar dashboard and saved in a directory within the Codar 1.50 or 1.60 installation but not in a directory whose content is backed up by the upgrade installer (the directory where the Codar Console expects to find these files is defined in the CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json configuration file.
- You **MUST** back up all files that you have created, customized, or manually installed in the CSA_HOME installation directory that are not automatically restored or backed up by the upgrade installer. See ["Customized files affected by upgrade" on page 6](#) for a list of customized files and the action performed during the upgrade. These files should be backed up outside of CSA_HOME.

You must back up these files to preserve them. While the upgrade installer will back up some files and directories, it does not back up all files and directories. If the upgrade installer fails before it backs up the selected files and directories, these files and directories may be deleted or corrupted.

Examples of files that you may have created, customized, or manually installed that may not be automatically backed up include custom graphic files, Oracle JDBC drivers, and jar files used by custom widgets or dynamic query scripts.

Note: If you are not sure which files may have been created, customized, or manually installed in the Codar installation directory, back up the entire `CSA_HOME` directory.

Caution: Back up files outside of `CSA_HOME`. The existing Codar installation directory and all of its contents are deleted during upgrade.

Caution: Do not remove any directories in `CSA_HOME`. Doing so may cause the upgrade to fail.

3. Back up the database.

Caution: If the upgrade installer fails, the database may be corrupted.

4. If it exists, back up the registry file (outside of `CSA_HOME`).

Windows

The registry file name and location is `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`.

Linux

The registry file name and location is `/home/codaruser/.com.zerog.registry.xml` or `/var/.com.zerog.registry.xml`.

Caution: If the upgrade installer fails, the registry file may be corrupted or deleted.

5. On Linux, if you mounted a file system within the Codar installation directory (for example, within `CSA_HOME`), you must unmount the file system. The upgrade installer cannot remove the mounted file system during the upgrade.

Caution: The upgrade will fail if you do not unmount the file system.

6. Create a database instance, user, and schema for the Identity Management component. Work with the database administrator to do the following (or refer to the manufacturer's documentation for more information):

Caution: On Windows, the database name and user name cannot contain more than one dollar sign symbol (\$). For example, `c$adb` is a valid name but `c$$adb` and `cadb` are not valid names.

- a. Create a database instance that is used by the Identity Management component.
- b. Create a schema for the Identity Management component by creating a database user (for example, `codaridmdbuser`).

- c. Create a role for this Codar database user (for example, `codaridmdbrole`) and grant the following privileges to the role:
 - `CREATE SESSION`
 - `CREATE TABLE`
 - `CREATE VIEW`
 - `CREATE SEQUENCE`
 - `CREATE ANY SYNONYM`
 - `UNLIMITED TABLESPACE`
- d. Grant the role to the database user.
- e. Alter the database user by setting this role as the user's default role.

For example, run the following commands to create the `codaridmdbrole` role and `codaridmbuser` user:

```
Create user codaridmbuser identified by codaridmbuser;  
Create role codaridmdbrole;  
Grant CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE SEQUENCE,  
CREATE ANY SYNONYM, UNLIMITED TABLESPACE to codaridmbuser;  
Grant codaridmdbrole to codaridmbuser;  
Alter user codaridmbuser default role codaridmdbrole;
```

You must provide this database's SID, database user name and, user's password when prompted for the Identity Management component database information during the upgrade of Codar.

7. Stop Codar:

Windows

- a. Open a command prompt and navigate to `CSA_HOME\jboss-as\bin`.
- b. Run the following command:

```
jbosscli.bat connectcommand=:shutdown
```
- c. Close the command prompt.
- d. Navigate to **Start > Administrative Tools > Services**.
- e. Close the Control Panel.

Linux

- a. Open a command prompt.
- b. Run the following command:

```
service codar stop
```

- c. Close the command prompt.
8. Verify that you have upgraded to the latest versions of software components required for Codar version 1.7. For example, for some resource providers, you may need to install a hotfix or service pack. See the Codar System and Software Support Matrix for the latest versions of software components required for Codar version 1.7.
9. If you are integrating with an existing external HPE Operations Orchestration, do the following:
 - a. Install Operations Orchestration to the correct version and patch level. See *Codar System and Software Support Matrix* for version requirements.
 - b. If you have upgraded Operations Orchestration, you may need to upgrade your content packs. See the *Operations Orchestration Release Notes* for more information.
 - c. Export Operations Orchestration's certificate from Operations Orchestration's truststore and, if Operations Orchestration and Codar are not installed on the same system, copy the certificate to the Codar system. This certificate will be imported into Codar's truststore by the Codar installer. TLS must be configured between Codar and Operations Orchestration.

For example, complete the following steps:

- i. On the system running Operations Orchestration, open a command prompt and change to the directory where Operations Orchestration is installed.
- ii. Run the appropriate command shown below. This command will generate a certificate file in the path shown in the command based on the platform (Windows/Linux).

C:\oo.cer (Windows) and /tmp/oo.cer (Linux) are examples of file names and locations used to store the exported root certificate (you can choose a different file name and location). *<password>* is the password you create. Be sure to store it in a secure location that you can access.

Windows

```
.\java\bin\keytool -export -alias tomcat -file C:\oo.cer -keystore  
.\Central\var\security\key.store -storepass <password>
```

Linux

```
./java/bin/keytool -export -alias tomcat -file /tmp/oo.cer -keystore  
./Central/var/security/key.store -storepass <password>
```

- iii. If Operations Orchestration is not running on the same system as Codar, copy oo.cer from the Operations Orchestration system to the system running Codar.
10. If you had installed the embedded Operations Orchestration, export the certificate from the

truststore of Operations Orchestration as it is needed during the upgrade process. Do the following:

- a. Open a command prompt and navigate to a directory outside of `CSA_HOME` and the embedded Operations Orchestration installation (for example, the embedded Operations Orchestration may be installed in `C:\Program Files\HPE\HPE Operations Orchestration\`) in which you will store the certificate file (for example, create the directory `C:\tmp` and store the certificate file in this directory).

- b. Run the following command:

```
"CSA_HOME\openjre\bin\keytool" -exportcert -keystore  
"C:\ProgramFiles\Hewlett Packard\HPE Operations Orchestration\central\var\  
security\key.store" -alias tomcat -file .\<filename> storepass <password>
```

where `CSA_HOME\openjre` is the directory in which the JRE that is used by Codar is installed and `<filename>` is a unique file name given to the certificate file that will be imported into Codar version 1.7 later during the upgrade process.

11. Because the JRE has been upgraded in this release, you must export the certificate from the truststore of Codar version 1.50 or 1.60 so that you may import it (at a later time during the upgrade process) into the truststore of Codar version 1.7.

To export the certificate, do the following:

- a. Open a command prompt and navigate to a directory outside of `CSA_HOME` in which you will store the certificate file.

- b. Run the following command:

```
CSA_HOME\openjre\bin\keytool -exportcert -keystore  
CSA_HOME\jboss-as\standalone\configuration\keystore -alias <alias> -file  
.\<filename>
```

`CSA_HOME\openjre\` is the directory in which the JRE that is used by Codar is installed.

`keystore` is the keystore file defined by the `certificate-key-file` property of the `connector` attribute in `CSA_HOME\openjre\jboss-as\standalone\configuration\standalone.xml`.

`<alias>` is the name used by the Codar server keystore to identify the SSL certificate.

`<file_name>` is a unique file name given to the certificate file that will be imported into Codar version 1.7 later during the upgrade process:

For example, run the following command if the JRE used by Codar version 1.50 is located in `CSA_HOME`, the alias used to identify the certificate is `codar`, and the file the certificate is saved to is `codar.cert`:


```
CSA_HOME\openjre\bin\keytool -exportcert -keystore  
CSA_HOME\jboss-as\standalone\configuration\keystore -alias codar -file  
.\codar.cert
```

12. Close all command prompts (for Windows, close all instances of Windows Explorer) and exit all programs that are running on the system.

Caution: The upgrade will fail if any program is accessing an Codar file or directory.

Export HPE Operations Orchestration certificate

You must export the Operations Orchestration certificate to Codar, when upgrading Codar 1.50 or 1.6 to Codar 1.7.

To export the Operations Orchestration certificate, complete the following steps:

1. Open the Chrome browser and launch the embedded Operations Orchestration (<https://localhost:8445/oo>).

Note: If you launch embedded Operations Orchestration version 10.20 or 10.21.0001, a validation message will be displayed informing you that 10.20 or 10.21.0001 will be upgraded to Operations Orchestration 10.50.

2. Click the **lock** icon in the address bar to open the drop-down dialog.
3. Click **Certificate information** to open the Certificate dialog.
4. Click the **Details** tab, then **Copy to file** to open the Certificate Export Wizard.
5. Click **Next** to open the Export File Format dialog.
6. Select the file format **Base-64 encoded X.509(.CER)** and click **Next**.
7. Specify a name for the certificate and click **Next**, then **Finish**.

Run upgrade installer

Note: Upgrade log files are written to the `CSA_HOME_Codar_1_70_0_installation\Logs` directory.

The memory requirements for any Codar installation are as follows:

- A Codar installation with the External Operations Orchestration option requires a minimum of 4.5 GB of available RAM.
 - A Codar with the Embedded Operations Orchestration option requires a minimum of 6 GB of available RAM.
 - HPE strongly recommends installing Codar on a system with 16 GB of RAM.
-
- ["Run upgrade installer on Windows " below](#)
 - ["Run upgrade installer on Linux" on page 26](#)

Run upgrade installer on Windows

Note: Upgrade log files are written to the `CSA_HOME_Codar_1_70_0_installation\Logs` directory.

To run the upgrade installer on Windows, complete the following steps:

1. Close all instances of Windows Explorer and command prompts and exit all programs that are running on the system.
2. Unzip the `setup-codar.zip` upgrade file. Go to the directory to which the files have been extracted and run the `setup.bat` installation file.
3. On the Introduction screen, read the information and click **Next**.
4. Read the license agreement and select **I accept the terms of the License Agreement**. Click **Next** to continue with the installation.

Note:

When you upgrade Codar 1.5 patch 1 to Codar 1.7, the following message is displayed in the license Agreement Screen:

HPE Codar Reporting Database Username was not provided during installation of HPE Codar 04.50.00000.1.

You can ignore the Codar version number displayed in the message and continue with the upgrade.

5. Verify that you want to upgrade to Codar version 1.7 and click **OK**.
6. Select the JRE used by Codar.
 - Use the existing JRE to continue using the JRE that was used with Codar version 1.50 or 1.60. No additional configuration is required if you use the existing JRE.
 - Use Open JRE if you want to use the JRE that is installed with Codar version 1.7. You must manually export the Codar certificate from the existing truststore and import it into the truststore that is installed with the upgrade.
 - Use Oracle JRE if you want to use an Oracle JRE and it is a different JRE from the one used with Codar version 1.50 or 1.60. If you used Oracle JRE with Codar version 1.50 or 1.60 and want to continue using this same JRE, select **Existing JRE**. You must manually export the Codar certificate from the existing truststore and import it into the Oracle JRE truststore.

In this documentation, the directory in which the JRE is installed will be referred to as `CSA_HOME\openjre\`.

For a list of supported JREs, see the *Codar System and Software Support Matrix*,

Click **Next** after you have selected a JRE option.

7. Verify that you have stopped the following services and click **OK**:
 - HPE Codar
 - HPE Search Services
 - Elasticsearch
 - HPE Marketplace Portal
8. Select the environment in which Codar is running and click **Next**.
 - Select **Standalone** if Codar is running in a non-clustered environment.

This selection determines the file from which the database instance information is read. For example, if you select standalone, the database instance information is read from the JBoss server's standalone.xml file (`CSA_HOME\jboss-as\standalone\configuration\standalone.xml`).

- Select **Cluster** if Codar is running in a clustered environment.

If you select cluster, the database instance information is read from the JBoss server's domain.xml file (CSA_HOME\jboss-as\domain\configuration\domain.xml).

9. Set passwords for the following system accounts used for administration and integrations between CSA components and other products:

Account	Description
Admin	Main administrator
consumerAdmin	Administrator account in sample consumer organization
consumer	End-user account in sample consumer organization
csaTransportUser	Used for CSA IDM to CSA communication
oolInboundUser	Used for HPE OO to CSA communication
csaReportingUser	Used internally for dynamic list properties
codarIntegrationUser	Used in Jenkins for Codar communication
csaCatalogAggregationTransportUser	Used for aggregation
securityEncryptedSigningKey	Used for encryption of SSO cookie

You can set passwords in any of the following methods:

- **Use generated passwords or set custom passwords:** Use passwords that are automatically generated by the Codar installer software. You can also edit the generated passwords.
- **Load passwords from a file and review:** Load a text file in which the passwords for all system accounts are saved. You can also edit the loaded passwords from the system account password fields.

```
Example:  
#HPE CSA passwords of system users  
#Mon Nov 16 01:38:04 PST 2015  
oolInboundUser=p0s7f1tbmlse18v2  
consumer=23tdvbntir6thmf3  
csaTransportUser=jjcigu4k16a989km  
codarIntegrationUser=m16c2de8gaqqcc7c  
securityEncryptedSigningKey=2surchgk13lsk711
```

```
csaCatalogAggregationTransportUser=cubouc8ptjnemesn  
csaReportingUser=3l31d1nhsb3dqts9  
admin=5q0mjmv7uckip5d3  
consumerAdmin=gkemt4accuqiajeb
```

- **Set a single password for all accounts (Not recommended):** Set a single password for all system accounts. HPE do not recommend to use a single for all system accounts.

Note: You must enter your passwords twice for password confirmation.

You can also edit the passwords by enabling **Edit generated passwords**.

10. Select any of the following options to save passwords in your system and click **Next**:
 - **Save to file**
 - **Copy to clipboard**

If you do not want to save your passwords, enable **Do not save the passwords. I can remember them all** and click **Next**.

11. Install the Codar database components onto the database instance to create the database schema, if it does not exist.

Click **Yes** to install Codar database components and create the database schema. When you select this option, the Codar service automatically starts when you exit the installer.

Click **No** if you are using an existing Codar database schema that was created as part of a prior successful installation of Codar version 1.7. When you select this option, the Codar service does not start when you exit the installer. See the end of this section for information on how to start the Codar service.

12. Verify the database instance information and click **Next**.

If the upgrade installer could not find the database instance information, a message is displayed and you will need to reenter the database information again. Continue to the next screen to reenter the database information again and click **Next** to continue.

13. Enter the Codar database user password and click **Next**.
14. If you configured a reporting database user, enter the reporting database user and password and click **Next**. If you did not configure a reporting database user, click **Next**.
15. Select **Yes** to install Codar database components and upgrade the schema then click **Next**.

16. The Single Sign-On configuration used during the previous installation (enabled or disabled), must be the same configuration used during the upgrade. The Single Sign-On that is included with Codar can only be used when launching an application, such as Operations Orchestration from the Codar Console. See the *Codar Configuration Guide* and Single Sign-On documentation for more information on integrating Single Sign-On with the application.

If you do not want to use Single Sign-On, you can disable it.

If enabled, enter the domain name of the network to which the server on which you are installing Codar belongs and click **Next**.

Applications launched from the Codar Console with which you want to use Single Sign-On must be installed on systems that belong to this domain.

17. Specify your integration with Operations Orchestration.

If you are integrating with Operations Orchestration 10.5, click **Configure connection to a running OO server** and click **Next** to proceed to step 18. The upgrade installer requires additional information to complete the integration.

Operations Orchestration 10.5 must be installed and running in order to complete the upgrade of Codar.

Caution: If you are upgrading your existing Embedded Operations Orchestration, before you begin using the Codar Upgrade Installer, make sure the Embedded Operations Orchestration is using the codaruser. If the Embedded Operations Orchestration Upgrade Service starts using the root user, then the installer will not function properly and the Operations Orchestration upgrade will fail.

Note: If you have chosen to upgrade the embedded Operations Orchestration from the previous Codar installation, and the upgrade has failed, you will need to delete the CODAR home folder that includes the unfinished installation, then restart the installer and resume the installation.

Note: If you have chosen to install a new version of Embedded OO during Codar upgrade, and the upgrade fails, do the following:

- Stop the Operations Orchestration Central service (Windows)
- Clear the database schema used for the Operations Orchestration installation;
- Finally, restart the installer and resume installation.

18. Define the Operations Orchestration 10.5 instance with which Codar is to be integrated. Enter the

following information and click **Next**.

Field Name	Description
Operations Orchestration Hostname	The fully-qualified domain name or IP address of the server where Operations Orchestration is located. Specify the hostname that was used to generate the Operations Orchestration's certificate. The hostname is used for TLS validation and to build the URL that the Codar Console uses to interact with Operations Orchestration (for example, in the subscription event overview section of the Operations area in the Codar Console, selecting the Process ID opens Operations Orchestration to the detailed page of the selected process when these properties are configured).
Operations Orchestration Port	The port number used to communicate with Operations Orchestration, such as 8445. The port number is used to build the URL that the Codar Console uses to interact with Operations Orchestration. By default, Operations Orchestration uses this port and port 8080. Applications running on the system on which Operations Orchestration is installed should not be using these ports.
Operations Orchestration User	The name of the user who logs in to Operations Orchestration Central. This is the user that was configured for provisioning topology designs.
Operations Orchestration Password	The password used by the Operations Orchestration user to log in to Operations Orchestration Central.
Operations Orchestration Certificate File	The file name and location of Operations Orchestration's certificate from Operations Orchestration's truststore on the Codar system. If you have not already done so, export the Operations Orchestration's certificate and copy it to the Codar system (see the section in this guide for more information).

Note: This information is used to set the Operations Orchestration properties in the `csa.properties` file and import Operations Orchestration's certificate into Codar's truststore. See the *Codar Configuration Guide* for more information about these properties.

19. By default, sample content (service designs and the components and Operations Orchestration flows required by the designs) are installed with Codar. You can choose to deploy this content during installation (making the sample service designs available in the Designs area of the Codar Console) or deploy the content at a later time.

To deploy the sample content during the Codar installation process, select any or all of the following sample contents and click **Next**.

Account	Description
CC-Vcentre-Topology-15.12.0000	This topology model integration demonstrates how to deploy virtual machine using VMWare vCentre server and flex resources such as the number of processors or memory.
CC-Openstack-Topology-15.12.0000	This topology model integration demonstrates how to provision multiple instances of server, volume, and swift container in an OpenStack based environment.
CC-Amazon-EC2-Topology-15.12.0000	This topology model integration demonstrates how to provision a classic Amazon EC2 instance using AWS interface.
ICSP-Topology-Integration-15.12.0000	This topology model integration demonstrates how to deploy physical infrastructure (servers, storage, and networking) and operating systems as a part of laas or Saas offerings using HPE OneView and HPE Insight Control server provisioning.
OneView-Topology-Integration-15.12.0000	This topology model integration demonstrates how to utilize HPE OneView to deploy physical infrastructure (servers, storage, and networking) as a part of laas or Saas offerings.
Helion-Development-Platform	Helion development platform
HPE-CODAR-1.70.0000	This topology model integration demonstrates how to provision instances of MySQL, PetClinic Application, Open Stack components, Tomcat Server.
Docker	This topology model integration demonstrates how to use OOT Docker components to deploy applications.

To deploy the sample content at a later time, click **Next** without selecting any of the sample contents.

If you choose to skip content installation, you can install the content at a later time, by running the Content Capsule Installer. For details, see the *Cloud Service Automation Content Pack User Guide*.

Note: If you chose not to install the database components, this dialog will not display.

20. Review your selections and click **Install** to complete the upgrade.
21. Click **Done** to exit the installer.

Run upgrade installer on Linux

Note: Upgrade log files are written to the `CSA_HOME\Codar_1_70_0_installation\Logs` directory.

To run the upgrade installer on Linux, complete the following steps:

1. Log in to the system as the root user.
2. Check the owner and group of `CSA_HOME/opencv/lib/security/cacerts`, where `CSA_HOME/opencv` is the directory in which the JRE that is used by Codar is installed.

If the owner is not **codaruser** or the group is not **codargrp**, reset the owner or group. For example, enter the following:

```
chown codaruser:codargrp CSA_HOME/opencv/lib/security/cacerts
```

3. Log out as the root user and log in as **codaruser**.
4. Check the values of the `CSA_HOME` environment variables. If they are set, verify that they do not contain any escape sequences. If any of these variables contain an escape sequence, the variable will cause the installer to fail. The variable must either be reset to a value that does not contain an escape sequence or must be unset.
5. Source the startup file in which you set the `CSA_HOME` and `PATH` environment variables.

On Linux Red Hat Enterprise, if you edited `.bash_profile`, enter the following:

```
source .bash_profile
```

On Linux Ubuntu, if you edited if you edited `.bashrc`, enter the following:

```
source .bashrc
```

6. Copy the Codar upgrade file, `setup-codar.bin`, to the system and go to the directory where it was copied.
7. Verify that `setup-codar.bin` is owned by `codaruser`, and that `codaruser` has full permissions to the file. If necessary, do the following:
 - a. Log in as the root user.
 - b. Enter the following commands:

```
chown codaruser setup-codar.bin
```

```
chmod 755 setup-codar.bin
```

- c. Log out as the root user and log in as codaruser.
8. Run the setup-codar.bin upgrade file as the codaruser.

Note: You must run the fixed setup-codar.bin as the codaruser. If you install Codar as another user, you may not be able to run Codar.

As the codaruser, enter the following:

```
./setup-codar.bin
```

9. Read the Introduction and press **Enter** to continue with the installation.
10. Read the license agreement. Press **Enter** after reading each page to scroll through the entire agreement.
11. Select **Y** and **Enter** to accept the license agreement and continue with the installation. Type **N** and **Enter** if you do not accept the license agreement and to exit the installation.

Note:

When you upgrade Codar 1.5 patch 1 to Codar 1.7, the following message is displayed in the license Agreement Screen:

```
HPE Codar Reporting Database Username was not provided during installation  
of HPE C0dar 04.50.00000.1.
```

You can ignore the Codar version number displayed in the message and continue with the upgrade.

12. Verify that you have stopped Codar version 1.50 or 1.60 and press **Enter**.
13. Verify that you have stopped the following services and press **Enter**:
 - o HPE Codar
 - o HPE Search Services
 - o Elasticsearch
 - o HPE Marketplace Portal
14. Select the environment in which Codar is running. Based on the options you selected in this guide, select **1** for standalone (Codar is running in a non-clustered environment), or select **2** for cluster mode, and press **Enter**.

This selection determines the file from which the database instance information is read.

- If you select **standalone**, the database instance information is read from the JBoss server's `standalone.xml` file (`CSA_HOME/jboss-as/standalone/configuration/standalone.xml`).
- If you select **cluster**, the database instance information is read from the JBoss server's `domain.xml` file (`CSA_HOME/jboss-as/domain/configuration/domain.xml`).

15. Select the appropriate JRE used by Codar and press **Enter**.

Use the existing JRE to continue using the JRE that was used with Codar version 1.50 or 1.60. No additional configuration is required if you use the existing JRE.

Select Open JRE if you want to use the JRE that is installed with Codar version 1.7. You must manually export the Codar certificate from the existing truststore and import it into the truststore that is installed with Codar.

Select Oracle JRE if you want to use an Oracle JRE and it is a different JRE from the one used with Codar version 1.50 or 1.60 (if you used Oracle JRE with Codar version 1.50 or 1.60 and want to continue using this same JRE, select Existing JRE). Then, select the location in which you installed this JRE. You must manually export the Codar certificate from the existing truststore and import it into the Oracle JRE truststore.

In this documentation, the directory in which the JRE is installed will be referred to as `CSA_HOME\openjre`.

For a list of supported JREs, see the *Codar System and Software Support Matrix*, available on the HPE Software Support Web site at <https://softwaresupport.hpe.com/> (this site requires that you register with an HPE Passport).

Based on the options you selected in this guide, select **2** (Open JRE) and press **Enter**.

16. Set passwords for the following system accounts used for administration and integrations between CSA components and other products:

You can set passwords in any of the following methods:

- **Use generated passwords or set custom passwords:** Use passwords that are automatically generated by the Codar installer software. You can also edit the generated passwords.
- **Load passwords from a file and review:** Load a text file in which the passwords for all system accounts are saved. You can also edit the loaded passwords from the system account password fields.

Example:

```
#HPE CSA passwords of system users  
#Mon Nov 16 01:38:04 PST 2015
```

```
ooInboundUser=p0s7f1tbm1se18v2
consumer=23tdvbntir6thmf3
csaTransportUser=jjcigu4k16a989km
codarIntegrationUser=m16c2de8gaqqcc7c
securityEncryptedSigningKey=2surchgk131sk711
csaCatalogAggregationTransportUser=cubouc8ptjnemesn
csaReportingUser=3131d1nhsb3dqts9
admin=5q0mjmv7uckip5d3
consumerAdmin=gkemt4accuqiajeb
```

- **Set a single password for all accounts (Not recommended):** Set a single password for all system accounts. HPE does not recommend the use of a single password for all system accounts.

Note: You must enter your passwords twice for password confirmation.

You can also edit the passwords by enabling **Edit generated passwords**

17. Select any of the following options to save passwords in your system and press **Enter**:

- **Save to file**
- **Copy to clipboard**

If you do not want to save your passwords, enable **Do not save the passwords. I can remember them all** and press **Enter**.

18. Acknowledge that you will manually export the Codar certificate from the existing truststore and import it into the truststore that is installed with Codar version 1.7. Select **1** and press **Enter**.

19. Verify the database instance information and press **Enter**.

If the upgrade installer could not find the database instance information, a message is displayed and you will need to re-enter the database information. Continue to the next screen to re-enter the database information and press **Enter** to continue.

20. Enter the Codar database user password and press **Enter**.

21. Enter the Codar reporting database user and press **Enter**. If you did not configure a reporting database user, press **Enter** to continue.

If you entered a reporting database user, enter the Codar reporting database user password and press **Enter**. If you did not enter a reporting database user, this option is not available.

22. Install Database Components?

Type **1** (Yes) to install Codar database components and upgrade the Codar database schema then press **Enter**.

23. The Single Sign-On configuration used during the previous installation (enabled or disabled), must be the same configuration used during the upgrade. The Single Sign-On that is included with Codar can only be used when launching an application, such as Operations Orchestration from the Codar Console. See the *Codar Configuration Guide* and Single Sign-On documentation for more information on integrating Single Sign-On with the application.

If you do not want to use Single Sign-On, you can disable it.

To enable Single Sign-On, type **1** and press **Enter**. To disable Single Sign-On, type **2** and press **Enter**.

24. If Single Sign-On is enabled, enter the domain name of the network to which the server on which you are installing Codar belongs and press **Enter**.

Applications launched from the Codar Console with which you want to use Single Sign-On must be installed on systems that belong to this domain.

25. Specify your integration with Operations Orchestration.

If you are integrating with Operations Orchestration 10.5, enter **1** (Configure the connection to a running Operations Orchestration server) and select **Enter**. The upgrade installer requires additional information to complete the integration.

Operations Orchestration 10.5 must be installed and running in order to complete the upgrade of Codar.

26. Define the Operations Orchestration 10.5 instance with which Codar is to be integrated. Enter the following information (select **Enter** after each entry).

- a. Enter the Operations Orchestration hostname. This is the fully-qualified domain name or IP address of the server where Operations Orchestration is located. Specify the hostname that was used to generate Operations Orchestration's certificate. The hostname is used for TLS validation and to build the URL that the Codar Console uses to interact with Operations Orchestration.
- b. Enter the Operations Orchestration port. This is the port number used to communicate with Operations Orchestration, such as 8445. The port number is used to build the URL that the *Codar* Console uses to interact with Operations Orchestration. By default, Operations Orchestration uses this port and port 8080. Applications running on the system on which Operations Orchestration is installed should not be using these ports.
- c. Enter the Operations Orchestration user. This is the name of the user who logs in to

- Operations Orchestration Central. This is the user that was configured for provisioning topology designs.
- d. Enter the Operations Orchestration password. This is the password used by the OO user to log in to Operations Orchestration Central.
 - e. Enter the Operations Orchestration certificate file. This is the filename and location of Operations Orchestration's certificate from Operations Orchestration's truststore on the Codar system. If you have not already done so, export the Operations Orchestration certificate and copy it to the Codar system (see ["Initial setup" on page 12](#) for more information).
27. By default, sample content (service designs and the components and Operations Orchestration flows required by the designs) are installed with Codar. You can choose to deploy this content during installation (making the sample service designs available in the Designs are of the Codar Console) or deploy the content at a later time.

To deploy the sample content during the Codar installation process, select any or all of the following sample contents and press **Enter**.

Account	Description
CC-Vcentre-Topology-15.12.0000	This topology model integration demonstrates how to deploy virtual machine using VMWare vCentre server and flex resources such as the number of processors or memory.
CC-Openstack-Topology-15.12.0000	This topology model integration demonstrates how to provision multiple instances of server, volume, and swift container in an OpenStack based environment.
CC-Amazon-EC2-Topology-15.12.0000	This topology model integration demonstrates how to provision a classic Amazon EC2 instance using AWS interface.
ICSP-Topology-Integration-15.12.0000	This topology model integration demonstrates how to deploy physical infrastructure (servers, storage, and networking) and operating systems as a part of laas or Saas offerings using HPE OneView and HPE Insight Control server provisioning.
OneView-Topology-Integration-15.12.0000	This topology model integration demonstrates how to utilize HPE OneView to deploy physical infrastructure (servers, storage, and networking) as a part of laas or Saas offerings.

Helion-Development-Platform	Helion development platform
HPE-CODAR-1.70.0000	This topology model integration demonstrates how to provision instances of MySQL, PetClinic Application, Open Stack components, Tomcat Server.
Docker	This topology model integration demonstrates how to use OOT Docker components to deploy applications.

To deploy the sample content at a later time, press **Enter** without selecting any of the sample contents.

If you choose to skip content installation, you can install the content at a later time, by running the Content Capsule Installer. For details, see the *Cloud Service Automation Content Pack User Guide*.

Note: If you chose not to install the database components, this dialog will not display.

28. Review your selections and press **Enter** to complete the installation or press **CTRL+C** to exit the installation.
29. When the installation is complete, press **Enter** to exit the installer.
30. Upgrade the Codar services to start and stop the Codar process.
 - a. Log in as the root user.
 - b. Remove the old version of the Codar script. Enter the following:

```
rm /etc/init.d/codar
```
 - c. Go to the directory in which Codar is installed. For example

```
cd /usr/local/hpe/codar
```
 - d. Copy the new `codar` script to the `/etc/init.d` directory. Enter the following:

```
cp ./scripts/codar/etc/init.d
```
 - e. Change permissions of the script. Enter the following:

```
chmod 755 /etc/init.d/codar
```


Applying the Codar license

When you upgrade Codar version 1.50 or 1.60 to 1.70, the Codar license expires. You must manually remove the old license and apply the new Codar 1.70 license.

You must contact HPE Customer Support to acquire the new license.

To apply the Codar license, perform the following steps:

1. Log on to Codar Console.
2. Click the admin icon.
3. Click **Licensing**.
The Manage Software License window is displayed.
4. Click the **Add** button.
5. In the **License Key** field, provide the new license and click **Add**.
The Codar license is applied.

To delete the old license, select the old license from the Manage Software License window and click **Delete**.

Update Codar

The following tasks must be completed before Codar can be restarted.

- ["Customize SSL/Security" below](#)
- ["Import certificates into Codar's truststore" on page 37](#)
- ["Customize manually configured files" on page 39](#)
- ["Remount shared file systems on Linux" on page 39](#)
- ["Restart Codar services" on page 39](#)

Customize SSL/Security

If you generated or copied SSL certificates that are used by Codar, you must copy these files to the appropriate directory in Codar 1.7.

The following is a list of files that you may have customized for SSL/security and the actions required when you upgrade Codar.

File	Action
certificate files	Required. Manually copy certificate files that do not use the .cer extension that are used by Codar from the backup directory to the Codar 1.7 directory (see the table below for more information).
.cacerts	Required. Because the JRE has been upgraded, you should not re-use the truststore from the old version of the JRE (it may contain public Certificate Authority certificates that are no longer trusted). Instead, you must export any root and/or self-signed certificates from the old truststore (certificates that you had manually imported into the old truststore) and import them into the new JRE truststore. You should have backed up the old version of the truststore prior to running the upgrade installer (see "Initial setup" on page 12).
Keystore file defined by the <code>certificate-key-file</code> property of the connector attribute in <code>standalone.xml</code>	Required (if not using the default keystore file). Manually copy the custom keystore file back from the location outside of the <code>CSA_HOME</code> installation directory

File	Action
	where you manually backed it up.
standalone.xml	No action required.

Files, actions, and locations

certificate files	
Action	Required. Manually copy certificate files that do not use the .cer extension that are used by Codar from the backup directory to the Codar 1.7 directory. Files that use the .cer extension are automatically restored. If you saved .cer files in a different directory, you must manually copy these files back after upgrade.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\security\

cacerts	
Action	Required. Because the JRE has been upgraded, you should not re-use the truststore from the old version of the JRE (it may contain public Certificate Authority certificates that are no longer trusted). Instead, you must export any root and/or self-signed certificates from the old truststore (certificates that you had manually imported into the old truststore) and import them into the new JRE truststore. You should have backed up the old version of the truststore prior to running the upgrade installer (see " Initial setup " on page 12).
File location in Codar 1.7	CSA_HOME\openjre\lib\security\ where CSA_HOME\openjre is the directory in which the JRE (used exclusively by Codar) is installed.
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	This file is not backed up.

Keystore file defined by the certificate-key-file property of the connector attribute in standalone.xml	
Action	<p>Required (if not using the default keystore file). Manually copy the keystore file back from the location outside of the CSA_HOME installation directory where you manually backed it up. If you are using the default keystore file, no action is required (the default keystore file is automatically backed up and restored).</p> <ul style="list-style-type: none"> • Windows default keystore file: C:\Program Files\Hewlett-Packard\Codar\jboss-as\standalone\configuration\.keystore • Linux default keystore file: ult value: /usr/local/hpe/codar/jboss-as/standalone/configuration/.keystore
File location in Codar 1.7	<p>The file and its location are determined by the value defined by the certificate-key-file.</p> <ul style="list-style-type: none"> • Windows default value: C:\Program Files\HPE\Codar\jboss-as\standalone\configuration\.keystore • Linux default value: /usr/local/hpe/codar/jboss-as/standalone/configuration/.keystore
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>If you are using a custom keystore file, this file is not backed up.</p> <p>The default keystore file is backed up to CSA_HOME_Codar_1_70_0_installation\Backup\security\kestores\</p>

standalone.xml	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\standalone\configuration\

Import certificates into Codar's truststore

Prior to running the upgrade installer, you should have exported the SSL certificate from the truststore for Codar. Import this certificate and other application's certificates into the truststore for the new version.

To import the certificates into Codar's truststore, complete the following steps:

1. If you did not export the SSL certificate from the truststore of Codar version 1.50 or 1.60, the truststore has been backed up to the `CSA_HOME_Codar_1_70_0_installation\Backup\security\keystores\` directory. Follow the instructions in ["Initial setup" on page 12](#) to export the Codar SSL certificate from the backed up truststore (you will need to modify the location of the truststore in the command).
2. Import the Codar certificate into the new Codar truststore. Complete the following steps:

- a. Run the following command:

```
CSA_HOME\openjre\bin\keytool -importcert -keystore  
CSA_HOME\openjre\lib\security\cacerts -alias <alias> -file <file_name> -  
storepass <password>
```

<alias> is the name used by the Codar server keystore to identify the SSL certificate.

<file_name> is the filename given to the certificate file to be imported.

<password> is the password you create. Be sure to store it in a secure location that you can access.

For example, run the following command where the alias used to identify the certificate is `codar`, and the file the certificate is named `codar.cert` and is saved in the current directory:

```
CSA_HOME\openjre\bin\keytool -importcert -keystore  
CSA_HOME\openjre\lib\security\cacerts -alias  
codar -file .\codar.cert -storepass <your-password>
```

- b. At the prompt to import the certificate, type **yes**.
3. Import the Operations Orchestration certificate into the new Codar truststore. Complete the following steps:
 - a. If the root certificate of the Operations Orchestration Certificate Authority is stored in a file on this system, import that file. Otherwise, export the Operations Orchestration certificate from Operations Orchestration's truststore:

- i. On the system running Operations Orchestration, open a command prompt and change the directory to `ICONCLUDE_HOME`.
- ii. Run the following command:

Windows

```
\java\bin\keytool -exportcert -alias pas -file C:\oo.cer -keystore  
.\Central\conf\rc_keystore -storepass bran507025
```

Linux

```
/java/bin/keytool -exportcert -alias pas -file /tmp/oo.cer -keystore  
./Central/conf/rc_keystore -storepass bran507025
```

Note: `C:\oo.cer` and `/tmp/oo.cer` are examples of file names and locations used to store the exported root certificate.

- iii. If Operations Orchestration is not running on the same system as Codar, copy `oo.cer` from the Operations Orchestration system to the system running Codar
- b. On the system running Codar, run the following command:

Windows

```
CSA_HOME\openjre\bin\keytool -importcert -alias pas -file  
C:\oo.cer -keystore CSA_HOME\openjre\lib\security\cacerts -storepass  
<password>
```

Linux

```
CSA_HOME\openjre/bin/keytool -importcert -alias pas -file /tmp/oo.cer  
-keystore  
CSA_HOME\openjre/lib/security/cacerts -storepass <password>
```

<password> is the password you create. Be sure to store it in a secure location that you can access.

- c. When prompted to trust the certificate, type **yes**.
4. If other applications, such as the database, LDAP, SMTP, Operations Orchestration Load Balancer, or Continuous Delivery Automation require SSL, you must import these applications' certificates into the truststore of Codar version 1.7.

Customize manually configured files

If you customized Codar files that are not documented as being customizable, you will need to manually customize those files again. Files that have been documented as being customizable are listed in the following sections in this guide:

- ["Customized files affected by upgrade" on page 6](#)
- ["Customize Codar" on page 40](#)

Remount shared file systems on Linux

If you unmounted one or more shared file systems within the Codar installation directory before running the upgrade installer, remount these file systems after the upgrade installer has completed.

Restart Codar services

Restart Codar service on Windows:

To restart the Codar service on Windows, complete the following steps:

1. On the server that hosts Codar, navigate to **Start > Administrative Tools > Services**.
2. Right-click on the **Codar service** and select **Restart**.

Restart Codar service on Linux

To restart the Codar service on Linux, complete the following steps:

1. On the server that hosts Codar, log in as **codaruser**.
2. Enter the following:

```
service codar restart
```

Customize Codar

You must customize Codar again for the features configured, customized, or used prior to the upgrade only. Complete only the tasks for features that were configured, customized, or used prior to upgrade.

If you want to configure, customize, or use any of these features for the first time, see the following guides for more information: *Codar Configuration Guide*, *Codar Console Help*.

- ["Configure Codar Console properties" below](#)
- ["Customize Codar Console dashboard" on the next page](#)
- ["Configure Codar Console to import large archives" on page 43](#)
- ["Customize Codar Console session timeout" on page 43](#)
- ["Customize Codar Console dashboard title" on page 44](#)
- ["Add custom graphic files or dynamic query scripts" on page 45](#)
- ["Customize Codar tools" on page 46](#)
- ["Customize Codar database user" on page 48](#)
- ["Customize Codar seeded users" on page 49](#)
- ["Integrate Codar with common access card" on page 50](#)
- ["Configure Identity Management component" on page 55](#)
- ["Configure IPv6" on page 57](#)
- ["Configure JBoss password vault" on page 57](#)
- ["Configure Oracle RAC" on page 58](#)
- ["Configure Codar to use a single sign-on" on page 58](#)
- ["Integrate Codar with SiteMinder" on page 62](#)
- ["Upgrade shortcuts on Windows" on page 67](#)

Configure Codar Console properties

The following is the file that you may have customized for the Codar Console and the actions required when you upgrade Codar:

File	Action
csa.properties	No action required.

File, action, and locations

csa.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME\Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\classes\

Customize Codar Console dashboard

The following is a list of files that you may have customized for the Codar Console dashboard and the actions required when you upgrade Codar:

File	Action
*.jsp	Required. Manually copy the JSP files from the backup directory to the appropriate directory in the Codar 1.7 directory (see the table below for more information).
config.json	Required. Manually copy the file from the backup directory to the Codar 1.7 directory (see the table below for more information).
messages.properties	Required. Manually copy the file from the backup directory to the Codar 1.7 directory (see the table below for more information).
index.jsp	No action required.

Files, actions, and locations

*jsp	
Action	Required. If you created custom Java server page (JSP) files for the Codar dashboard and saved them in a directory within the Codar 1.50 or 1.60 installation but not in a directory whose content is backed up by the upgrade installer, you should have backed up these files to preserve them. Otherwise, they will be deleted by the upgrade installer. Manually copy the JSP files from the backup directory to the appropriate directory in the Codar 1.7 directory.
File location in Codar 1.7	The directory where the Codar Console expects to find these files, defined in the <code>config.json</code> dashboard configuration file.
Backed up Codar1.50 or 1.60 file location in Codar 1.7	The directory to which the JSP files were backed up, either manually or by the upgrade installer, depending on where the files were located in Codar 1.50 or 1.60.

config.json	
Action	Required. Manually copy the file from the backup directory to the Codar 1.7 directory.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	Windows: CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\dashboard\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/csa.war/dashboard/

messages.properties	
Action	Required. Manually copy the file from the backup directory to the Codar1.7 directory.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	Windows: CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\dashboard\messages\dashboard\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/csa.war/dashboard/messages/dashboard/

index.jsp	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\operations\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\deployments\csa.war\custom-content

Configure Codar Console to import large archives

The following is the file that you customized to import large archives using the Codar Console or REST API and the actions required when you upgrade Codar.

File	Action
standalone.conf.bat	No action required.

Files, actions, and locations

standalone.conf.bat	
Action	No action required.
File location in Codar 1.7	CSA_HOME\jboss-as\bin\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\

Customize Codar Console session timeout

The following file may have been customized if you updated the Codar Console session:

File	Action
web.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).

Files, actions, and locations

web.xml	
Action	Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

Customize Codar Console dashboard title

The following file may have been customized if you updated the Codar Console dashboard title:

File	Action
message.properties	Required. Manually copy the file from the backup directory to the Codar 1.7 directory (see the table below for more information).

Files, actions, and locations

messages.properties	
Action	Required. Manually copy the file from the backup directory to the Codar 1.7 directory.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\custom\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	Windows: CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\custom\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/csa.war/custom/

Add custom graphic files or dynamic query scripts

The following is a list of custom files that you may have added and the actions required when you upgrade Codar:

File	Action
*.jsp (dynamic query scripts)	Required. Manually copy any custom dynamic query scripts from the backup directory to the Codar 1.7 directory (see the table below for more information).
*.jar (dynamic query scripts)	Required. Manually copy any custom dynamic query scripts from the manual backup copies you made before running the upgrade installer.
*.jpg, *.jpeg, *.gif, *.png	No action required.

Files, actions, and locations

*jsp (dynamic query scripts)	
Action	Required. Manually copy any custom dynamic query scripts from the backup directory to the Codar 1.7 directory.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\propertysources\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	Windows: CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\propertysources\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/csa.war/propertysources/

*.jar (dynamic query scripts)	
Action	Required. Manually copy any custom dynamic query scripts from the manual backup copies you made before running the upgrade installer.
File location in Codar 1.7	<user-specified location>

*.jar (dynamic query scripts)	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<user-specified location>

*.jpg, *.jpeg, *.gif, *.png	
Action	No action required. All custom graphics of the listed types in the associated directory are automatically restored.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\images\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	Windows: CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\images Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/csa.war/images/

Customize Codar tools

The following is a list of files that you may have customized if you ran any of the Codar tools and the actions required when you upgrade Codar:

File	Action
config.properties (content archive tool, purge tool, provider configuration tool)	Required. Manually copy any custom configuration files from the backup directory to the Codar 1.7 directory (see the table below for more information).
db.properties (process definition tool, schema installation tool)	Required. Manually copy any custom configuration files from the backup directory to the Codar 1.7 directory (see the table below for more information).
HP00InfoInput.xml (process definition tool)	Required. Manually copy any custom input files from the backup directory to the Codar 1.7 directory (see the table below for more information).
provider.xml (provider configuration tool)	Required. Manually copy any custom input files from the backup directory to the Codar 1.7 directory (see the table below for more information).

Files, actions, and locations

config.properties	
Action	Required. Manually copy any custom configuration files from the backup directory to the Codar1.7 directory. This is the generic name of the configuration file used in some examples for the content archive tool, purge tool, and provider configuration tool. If you used a different name for the configuration file, copy that file instead.
File location in Codar 1.7	CSA_HOME\Tools\ContentArchiveTool\ CSA_HOME\Tools\DBPurgeTool\ CSA_HOME\Tools\ProviderTool\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\ContentArchiveTool\ CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\DBPurgeTool\ CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\ProviderTool\

db.properties	
Action	Required. Manually copy any custom configuration files from the backup directory to the Codar1.7 directory. This is the generic name of the configuration file used in some examples for the process definition tool and schema installation tool. If you used a different name for the configuration file, copy that file instead.
File location in Codar 1.7	CSA_HOME\Tools\ProcessDefinitionTool\ CSA_HOME\Tools\SchemaInstallationTool\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\ProcessDefinitionTo ol\ CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\SchemaInstallationT ool\

HPOOInfoInput.xml	
Action	Required. Manually copy any custom input files from the backup directory to the Codar1.7 directory. This is the generic name of the input file used in some examples for the process definition tool. If you used a

HPOOInfoInput.xml	
	different name for the input file, copy that file instead.
File location in Codar 1.7	CSA_HOME\Tools\ProcessDefinitionTool
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\ProcessDefinitionTo ol\

provider.xml	
Action	Required. Manually copy any custom provider input files from the backup directory to the Codar1.7 directory. This is the generic name of the input file used in some examples for the provider configuration tool. If you used a different name for the provider input file, copy that file instead.
File location in Codar 1.7	CSA_HOME\Tools\ProviderTool\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\Tools\ProviderTool\

Customize Codar database user

The following is the file that you may have customized if you updated the password of the Codar database user and the actions required when you upgrade Codar:

File	Action
standalone.xml	No action required.

Files, actions, and locations

messages.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\standalone\configuration\

Customize Codar seeded users

The following is a list of files that you may have customized if you updated the password of one or more seeded users and the actions required when you upgrade Codar:

File	Action
applicationContext-security.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).
codar-consumer-users.properties	Required. Manually copy the file from the backup directory to the Codar 1.7 directory (see the table below for more information).
applicationContext.properties	No action required.

Files, actions, and locations

applicationContext-security.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

codar-consumer-users.properties	
Action	Required. Manually copy the file from the backup directory to the Codar 1.7.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\

codar-consumer-users.properties	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\classes\

applicationContext.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

Integrate Codar with common access card

The following is a list of files that you customized when integrating Codar with a common access card (CAC) and the actions required when you upgrade Codar:

File	Action
applicationContext-security.xml (Codar Console)	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext.xml (HPE Identity Management component)	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext.xml (Identity Management component)	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext-security.xml (Codar Console)	Required. If this file was customized, you must customize this file again (see the table below for more information).
rb.json	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (default)	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (pilot)	Required. If this file was customized, you must customize this file again (see the table below for more information).

File	Action
main.css (custom theme)	Required. If this file was customized, you must customize this file again (see the table below for more information).
java.security	Required. If this file was customized, you must customize this file again (see the table below for more information).
standalone.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).

Files, actions, and locations

applicationContext.xml (Codar Console)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

applicationContext-security.xml (Codar Console)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\

applicationContext-security.xml (Codar Console)	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

applicationContext.xml (Identity Management component)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

applicationContext-security.xml (Identity Management component)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

rb.json	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\locales\ <i><Locale></i> \
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\dist\locales\ <i><Locale></i> \

main.css (default)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\default\styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\default\styles\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/default/styles/</p>

main.css (pilot)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\pilot\styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\pilot\styles\</p> <p>Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/pilot/styles/</p>

main.css (<theme_directory>)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\<theme_directory>\styles\
Backed up Codar 1.60 or 1.70 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\<theme_directory>\styles\</p> <p>Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/<theme_directory>/styles/</p>

java.security	
Action	Required. Manually copy this file from the manual backup copy you made before running the upgrade installer.
File location in Codar 1.7	CSA_JRE_HOME\lib\security\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	This file is not backed up. You should have manually backed this file up prior to running the upgrade installer.

standalone.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\configuration\

Configure Identity Management component

The following is a list of files that you may have customized for the Identity Management component and the actions required when you upgrade Codar:

File	Action
applicationContext.xml (Identity Management component)	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext.properties	No action required.
applicationContext-common.xml	No action required.

Files, actions, and locations

applicationContext.xml (Identity Management component)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.70 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

applicationContext.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

applicationContext-common.xml	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

Configure IPv6

The following is the file that you may have customized if you configured IPv6 and the actions required when you upgrade Codar.

File	Action
standalone.xml	No action required.

Files, actions, and locations

standalone.xml	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.70 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\configuration\

Configure JBoss password vault

The following is the file that you may have customized if you configured the JBoss password vault and the actions required when you upgrade Codar.

File	Action
vault.bat	No action required.

Files, actions, and locations

vault.bat	
Action	No action required. If this file was customized, the customizations have been restored.
File location in Codar 1.7	CSA_HOME\jboss-as\bin\

vault.bat	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\standalone\

Configure Oracle RAC

The following is the file that you may have customized if you configured Oracle RAC and the actions required when you upgrade Codar.

File	Action
standalone.xml	No action required.

Files, actions, and locations

standalone.xml	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\configuration\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_ installation\Backup\standalone\configuration\

Configure Codar to use a single sign-on

The following is a list of files that you customized when configuring Codar to use a single sign-on (SSO) and the actions required when you upgrade Codar:

File	Action
applicationContext.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext-security.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).

File	Action
rb.json	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (default)	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (pilot)	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (custom theme)	Required. If this file was customized, you must customize this file again (see the table below for more information).
hpssConfiguration.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).

Files, actions, and locations

applicationContext.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

applicationContext-security.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up</p>

applicationContext-security.xml	
	file does not contain all the required attributes for the current version.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

rb.json	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\locales\<locale>\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\dist\locales\<locale>\

main.css (default)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\default\styles\

main.css (default)	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_ installation\Backup\portal\node_modules\mpp- ui\themes\default\styles\ Linux: CSA_HOME/_Codar_1_70_0_ installation/Backup/portal/node_modules/mpp- ui/dist/themes/default/styles/</p>

main.css (pilot)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp- ui\dist\themes\pilot\styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_ installation\Backup\portal\node_modules\mpp- ui\themes\pilot\styles\ Linux: CSA_HOME/_Codar_1_70_0_ installation/Backup/portal/node_modules/mpp- ui/dist/themes/pilot/styles/</p>

main.css (<theme_directory>)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new</p>

main.css (<theme_directory>)	
	<p>file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\<theme_directory>\styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\<theme_directory>\styles\</p> <p>Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/<theme_directory>/styles/</p>

hpssoConfiguration.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

Integrate Codar with SiteMinder

The following is a list of files that you customized when integrating Codar with SiteMinder and the actions required when you upgrade Codar:

File	Action
applicationContext-security.xml (Codar Console)	No action required.
applicationContext.xml (Codar Console)	Required. If this file was customized, you must customize this file again (see the table below for more information).
ssologout.jsp	Required. If this file was customized, you must customize this file again (see the table below for more information).
web.xml	Required. If this file was customized, you must customize this file again (see the table below for more information).
applicationContext-security.xml (Identity Management component)	Required. If this file was customized, you must customize this file again (see the table below for more information).
rb.json	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (default)	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (pilot)	Required. If this file was customized, you must customize this file again (see the table below for more information).
main.css (custom theme)	Required. If this file was customized, you must customize this file again (see the table below for more information).

Files, actions, and locations

applicationContext-security.xml (Codar Console)	
Action	No action required.
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

applicationContext.xml (Codar Console)	
Action	Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.

applicationContext.xml (Codar Console)	
	<p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

ssologout.jsp	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

web.xml	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>

web.xml	
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\csa.war\WEB-INF\

applicationContext-security.xml (Identity Management component)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\

rb.json	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\locales\<locale>\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-

rb.json	
	ui\dist\locales\ <locale>\< td=""> </locale>\<>

main.css (default)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\default\styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\default\styles\</p> <p>Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/default/styles/</p>

main.css (pilot)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\pilot\styles\

main.css (pilot)	
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\pilot\styles\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/pilot/styles/</p>

main.css (<theme_directory>)	
Action	<p>Required. If this file was customized, you must customize this file again. If you do not remember the customizations you made to the file, see the backed up copy and compare it to the file installed with Codar 1.7.</p> <p>Caution: Do NOT copy the backed up file over the new file. The file has changed in Codar 1.7 and the backed up file does not contain all the required attributes for the current version.</p>
File location in Codar 1.7	CSA_HOME\portal\node_modules\mpp-ui\dist\themes\ <i><theme_directory></i> \styles\
Backed up Codar 1.50 or 1.60 file location in Codar 1.7	<p>Windows: CSA_HOME_Codar_1_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\<i><theme_directory></i>\styles\ Linux: CSA_HOME/_Codar_1_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/<i><theme_directory></i>/styles/</p>

Upgrade shortcuts on Windows

If you created Codar shortcuts in the default directory (for example, C:\Users*<user>*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\HPE\Codar), these shortcuts are automatically upgraded.

If you created Codar shortcuts and saved them to another directory other than the default directory (for example, in a Program Group, in the Start Menu, on the desktop, or in the Quick Launch Bar), you should delete these shortcuts as they will no longer work.

Optionally, you can change the target of the shortcuts to `CSA_HOME_Codar_1_70_0_installation\Change HPE Codar Installation.exe`.

Deploy content pack for topology designs

Download the Codar HPE Cloud Content Capsule using the Content Capsule Installer. You can access the Content Capsule Installer from the `CSA_HOME\tools\CSLContentInstaller` directory after installing Codar. For details about the Content Capsule Installer, see the *Cloud Service Automation Content Pack User Guide*.

The Codar content pack must be deployed after the base Operations Orchestration content packs have been deployed.

Verify deployed content packs

To verify that all content packs were successfully deployed during installation, complete the following steps:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Click the **Content Packs** tab.
4. Look for the names and versions of content packs in the list. If a content pack is missing, follow the instructions below to manually deploy it.

The content packs that should have been automatically deployed are:

- CSA-HPOO
- CODAR
- EXISTING-INFRASTRUCTURE-WINDOWS
- CSA-VMWARE
- CSA-SITESCOPE
- CSA-SA
- CSA-HP-HELION-PUBLIC-CLOUD
- CSA Chef Provisioner
- CSA-AMAZON
- SM

- SA
- Virtualization
- HP Solutions
- Cloud
- Base
- EXISTING-INFRASTRUCTURE
- CSA-Docker

Deploy Operations Orchestration and component tool content packs

If one or more of the base Operations Orchestration or Codar component tool content packs are not deployed, you must deploy them manually.

To manually deploy the Operations Orchestration or Codar component tool content packs, complete the following steps:

1. Log in to the existing Operations Orchestration Central.
2. Click the **Content Management** button.
3. Click the **Content Packs** tab.
4. In the Deploy New Content dialog, click the **Add files for deployment** icon.
5. Click the **Deploy New Content** icon.
6. Click the **Add files for deployment** icon.
7. Navigate to the `CSA_HOME\oo\OOContentPack\` directory. From the subdirectories, select a content pack and click **Open** then **Deploy**. Select, open, and deploy the following base content packs in the order shown below:
 - `oo10-base-cp-1.4.4`
 - `oo10-cloud-cp-1.4.0`
 - `oo10-hp-solutions-cp-1.4.0`
 - `oo10-virtualization-cp-1.4.0`

- oo10-sa-cp-1.2.0.001
- oo10-sm-cp-1.0.3

Note: Do not deploy the Codar content pack until after you have deployed the base content packs. The Codar content pack must be deployed separately and after you have deployed the base content packs.

The deployment may take a few minutes and the dialog will show a progress bar.

8. When the deployment succeeds, click **Close** to close the dialog.
9. Click the **Deploy New Content** icon.
10. Click the **Add files for deployment** icon.
11. Navigate to the `CSA_HOME\Tools\ComponentTool\contentpacks\` directory, select all the content packs, and click **Open**.
12. Click **Deploy**.

The deployment may take a few minutes and the dialog will show a progress bar.

13. When the deployment succeeds, click **Close** to close the dialog.

Import service designs

The sample service designs are installed with Codar if you selected the **Install sample content** option during installation.

These designs are imported to Codar when the Cloud Content Capsule is downloaded using the Content Capsule Installer. You can access the Content Capsule Installer from the `CSA_HOME\tools\CSLContentInstaller` directory.

For details about the Content Capsule Installer, see the *Cloud Service Automation Content Pack User Guide*.

Note: HPE recommends that you start using the new versions of the service designs immediately.

Upgrade resource providers

See the resource provider README file to verify whether the resource provider requires an upgrade.
The README file can be found in the following location:

`CSA_HOME\CSAKit-4.5\Lib\\.`

Clear web browser cache

It may be necessary to clear your web browser cache on systems that previously accessed Codar prior to upgrading to the new versions.

Restart Codar service

Restart Codar service on Windows:

To restart the Codar service on Windows, complete the following steps:

1. On the server that hosts Codar, navigate to **Start > Administrative Tools > Services**.
2. Right-click on the **Codar service** and select **Restart**.

Restart Codar service on Linux

To restart the Codar service on Linux, complete the following steps:

1. On the server that hosts Codar, log in as **codaruser**.
2. Enter the following:

```
service codar restart
```

Package deployment behavior post upgrade

After you upgrade Codar from 1.50 or 1.60 to 1.70, the lifecycle stage of an existing Instance for package deployment will be set to DEVELOPMENT by default, regardless of its lifecycle stage prior to the upgrade. Therefore, even if a package had an instance that was deployed in production stage prior to the upgrade, it cannot be published post upgrade directly. The package must be deployed once again in PRODUCTION stage, and only then can it be published.

Appendix A: Cross-product upgrade between Codar and Cloud Service Automation

This appendix shows the upgrade result if you have an existing HPE Cloud Service Automation (CSA) 4.2 or 4.5 or 4.6 installation, and you want to upgrade to Cloud Service Automation 4.7 with Codar 1.7. The upgrade result from Cloud Service Automation 4.2 or 4.5 or 4.6 will always be Cloud Service Automation 4.7, as shown in the table below.

For information on upgrading Cloud Service Automation 4.2 or 4.5 to 4.6, see the *Upgrade guide*. For information on running the CSA 4.6 installer, see the *Installation guide*.

Existing installation	Upgrade installer used	Upgraded to
CSA 4.2 or CSA 4.5 or CSA 4.6 instant-on	Codar 1.7	CSA 4.7 instant-on
CSA 4.2 or CSA 4.5 or CSA 4.6 no license	Codar 1.7	CSA 4.7 no license
CSA 4.2 or CSA 4.5 CSA 4.6 license	Codar 1.7	CSA 4.7 license
Codar 1.50 or 1.60 no license	CSA 4.7	Codar 1.7 no license
Codar 1.50 or 1.60 license	CSA 4.6	Codar 1.7 license
CSA 4.2 or CSA 4.5 or CSA 4.6 with CSA and Codar licenses	Codar 1.7	CSA 4.7 with CSA and Codar licenses
Codar 1.5 or 1.6 with CSA and Codar licenses	CSA 4.7	CSA 4.7 with CSA and Codar licenses

Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Upgrade Guide (Codar 1.7)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to clouddocs@hpe.com.

We appreciate your feedback!

