

Codar

Software Version: 1.70

Windows® and Linux operating systems

Installation and Configuration 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

Installation Overview 7
System requirements 7
Installation steps 7
Install and configure database 8
Oracle Database 8
Install Oracle Database and JDBC drivers 8
Download Oracle JDBC drivers 8
Configure Oracle Database 9
Create Oracle database instances for Codar 9
Configure Oracle database user and role for Codar 10
Configure a reporting role and read-only user for Codar (required for reporting) 11
Configure Oracle database user and role for Identity Management component 12
Configure Oracle database user and schema for embedded Operations Orchestration 13
Configure Oracle for localization (required for localization) 14
Create Oracle tablespace for Codar (recommended) 14
Microsoft SQL server 14
Install Microsoft SQL Server 14
Configure Microsoft SQL Server 15
Enable TCP/IP on Microsoft SQL server 15
Configure Microsoft SQL server database user for Codar 15
Configure Microsoft SQL reporting database role and read-only user for Codar (required for reporting) 16
Configure Microsoft SQL server database user for Identity Management component 17
Configure Microsoft SQL server database user for embedded Operations Orchestration 18
Create Microsoft SQL Server filegroup with embedded Operations Orchestration 19
PostgreSQL 19

Install PostgreSQL 19
Configure PostgreSQL users and database 19
Install external Operations Orchestration 24
Configure an internal user 24
Export Operations Orchestration root certificate 25
Install Codar 26
Install Codar on Windows 26
Install Codar on Linux 35
Configure group and user 35
Install Codar 35
Post-installation database configuration 45
Configure Oracle tablespace 45
Configure Microsoft SQL Server filegroup 45
Configure Operations Orchestration 47
Configure embedded Operations Orchestration 48
Add JRE to the system path 48
Configure internal users 49
Deploy content packs required by Codar 50
Verify deployed content packs 50
Deploy Operations Orchestration and component tool content packs 51
Set up system accounts for the Codar content pack 53
Set up system properties for the Codar content pack 53
Configure Single Sign-On 54
Configure external Operations Orchestration 54
Add JRE to system path 55
Install Codar content packs 56
Configure internal users 56
Deploy content packs required by Codar 57
Verify the deployed content packs 57
Deploy the Operations Orchestration and component tool content packs 58
Set up system accounts for Codar content pack 59
Set up system properties for Codar content pack 60
Configure Single Sign-On 60

Configure Single Sign-On between Codar and Operations Orchestration ... 61
Enable Single Sign-On ... 61
Configure LDAP Users for Single Sign-On ... 62
Post-installation ... 63
Install VMware vCenter ... 63
Configure VMware vCenter ... 64
Install HPE Helion Development Platform ... 65
Configure HDP ... 65
Modify the proxy settings ... 66
Modify system properties in Operations Orchestration Central ... 66
Set HDP provider properties in Codar ... 67
Install SiteScope ... 67
Configure SiteScope ... 67
Enable Codar to configure SiteScope monitors ... 68
Manually import additional Codar templates ... 68
Configure Codar credential profiles ... 69
Configure SiteScope administrator credentials ... 69
Install Server Automation ... 69
Configure Server Automation ... 70
Create Codar service account ... 70
Create Codar administrators group and assign permissions ... 71
Validate Codar service account ... 72
Validate Server Automation client ... 72
Prepare VMware template ... 73
Template preparation overview ... 74
Detailed process ... 74
Provision an operating system on a virtual machine ... 75
Sanitize agent configuration on a template machine ... 75
Basic customization ... 77
Install prepared template ... 77
Configure resource providers ... 77
Apply Codar licenses ... 78
OSI capacity ... 79
Jenkins ... 79
Install Collabnet Subversion Edge ... 79

Install Tortoise 79
Install Jenkins 80
Install the JDK 80
Install the Maven plug-in 80
Configure Jenkins to use with Codar 80
Install Codar Jenkins plug-in 81
Enable the Codarr Jenkins plug-in 81
Configure Pet Clinic sample application project 82
Configure plug-in for Pet Clinic sample application 82
Sample Pet Clinic extended properties file 84
Create custom design 85
Import and configure sample designs 86
Import sample designs 86
Configure sample designs 86
Send documentation feedback 87

Installation Overview

This guide provides information for installing the HPE Codar application. Successful implementation of the application requires knowledge of the integrated products, as well as the Codar solution. 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.

System requirements

You should review the *Codar System and Software Support Matrix* for version requirements.

You can get this document from the HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals**

Installation steps

The main installation steps depend on whether you are installing the embedded or external HPE Operations Orchestration to integrate with Codar. If you choose to integrate Codar with embedded Operations Orchestration, embedded Operations Orchestration is installed automatically with Codar.

Following are the main installation steps:

1. "Install and configure database" on page 8: Oracle, Microsoft SQL, or PostgreSQL.
2. "Install external Operations Orchestration" on page 24 (only if you chose to integrate with external Operations Orchestration).
3. "Install Codar" on page 26.
    a. "Install Codar on Windows" on page 26 or "Install Codar on Linux" on page 35
    b. "Post-installation database configuration" on page 45
4. "Configure Operations Orchestration" on page 47.
5. "Post-installation" on page 63

Install and configure database

Install a database that will be used as the primary data-source for Codar. You can install and configure one of the following databases.

- Oracle Database, see "Oracle Database" below
- Microsoft SQL Server, see "Microsoft SQL server" on page 14
- PostgreSQL, see "PostgreSQL" on page 19

Oracle Database

You must complete the following installation and configuration steps to use Codar with the Oracle Database.

- "Install Oracle Database and JDBC drivers" below
- "Download Oracle JDBC drivers" below
- "Configure Oracle Database" on the next page

Install Oracle Database and JDBC drivers

See the *Codar System and Software Support Matrix*, for a list of supported database versions.

The guide is available in HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals** .

Install the Oracle Database according to the manufacturer's documentation. Database installation is typically done in partnership with a database administrator.

Download Oracle JDBC drivers

For a list of supported JDBC driver versions, see the *Codar System and Software Support Matrix.*

This guide is available in HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals** .

Download a supported version of the JDBC `.jar` file(s) and save them on the system on which Codar will be installed. Record the location where you save the files, because this information must be provided when you install Codar.

Configure Oracle Database

These tasks must be completed before Codar is installed.

> **Note:** These tasks are relevant to both embedded and external Operations Orchestration, except where indicated.

- "Create Oracle database instances for Codar" below
- "Configure Oracle database user and role for Codar" on the next page
- "Configure a reporting role and read-only user for Codar (required for reporting)" on page 11
- "Configure Oracle database user and role for Identity Management component" on page 12
- "Configure Oracle database user and schema for embedded Operations Orchestration" on page 13
- "Configure Oracle for localization (required for localization)" on page 14
- "Create Oracle tablespace for Codar (recommended)" on page 14

Create Oracle database instances for Codar

Separate database instances are required for Codar and the components it uses. You must create a separate database instance for:

- Embedded Operations Orchestration - only if you use embedded Operations Orchestration
- Identity Management component
- Codar

Work with the database administrator to create a database that is used by the embedded Operations Orchestration, Codar (if it has not already been created), and the Identity Management component. See the *Operations Orchestration Database Guide* for more information about database requirements for Operations Orchestration.

You must provide the service name (global database name) of these databases when prompted for the database information during the installation of Codar. For example, when prompted for the Codar database information, provide the service of the Codar database. When prompted for the Identity Management component database information, provide the service name of the Identity Management component database. When prompted for the embedded Operations Orchestration database information, provide the service name of the embedded Operations Orchestration database.

> **Tip:** You can run the following query to find the `SERVICE_NAME` on the Oracle 12c/11g systems:
>
> `select global_name from global_name;`

Configure Oracle database user and role for Codar

A database user is needed when installing Codar. Work with the database administrator to configure the database role and user (or see 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 `c$ad$b` are not valid names.

To configure an Oracle database user and role for Codar, complete the following steps:

1. Create a schema for Codar by creating a database user (for example, codardbuser).
2. Create a role for this Codar database user (for example, codardbrole) and grant the following privileges to the role:
   - `CREATE SESSION`
   - `CREATE TABLE`
   - `CREATE VIEW`
   - `CREATE SEQUENCE`
   - `CREATE ANY SYNONYM`
   - `UNLIMITED TABLESPACE`
3. Grant the role to the Codar database user.
4. Alter the Codar database user by setting this role as the user's default role.

For example, run the following commands to create codardbrole and codardbuser:

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

You must provide this user name and password when prompted for the Codar database user during the installation of Codar.

Configure a reporting role and read-only user for Codar (required for reporting)

If you are using both the Cloud Service Automation and Codar licenses, you can use the Cloud Service Automation reporting capabilities. If you want to use the reporting capabilities, you must add an Oracle reporting database role and read-only user when installing Codar. For details about the Cloud Service Automation reporting capabilities, see the *Cloud Service Automation Reporting and Auditing Whitepaper*.

> **Note:** You must apply both the Cloud Service Automation and Codar licenses to use the reporting capabilities.

Work with the database administrator to create a role and read-only user to do the following (or see the manufacturer's documentation for more information).

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

To create and configure a reporting database role and read-only user for Codar and Cloud Service Automation, complete the following steps:

1. Create a database user (for example, `CODARReportingDBUser`).
2. Create a role for this Codar database user (for example, `CODARReportingDBRole`) and grant the `CREATE SESSION` privilege to the role.
3. Grant the role to the Codar database user.
4. Alter the Codar database user by setting this role as the user's default role.

For example, run the following commands to create the `CODARReportingDBRole` role and `CODARReportingDBUser` read-only user:

```
Create user CODARReportingDBUser identified by CODARReportingDBUser;
Create role CODARReportingDBRole;
Grant CREATE SESSION to CODARReportingDBUser;
Grant CODARReportingDBRole to CODARReportingDBUser;
Alter user CODARReportingDBUser default role CODARReportingDBRole;
```

If you configure this user, you must provide this user's user name and password when prompted for the Codar reporting database user during the installation of Codar.

Configure Oracle database user and role for Identity Management component

A database user is needed when installing Identity Management component for Codar. Work with the database administrator to do the following (or see 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 `c$ad$b` are not valid names.

To configure an Oracle database role and user for Identity Management component, complete the following steps:

1. Create a schema for the Identity Management component by creating a database user (for example, `codaridmdbuser`).
2. 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`
3. Grant the role to the Codar database user.
4. Alter the Codar database user by setting this role as the user's default role.

For example, run the following commands to create `codaridmdbrole` and `codaridmdbuser`:

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

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

Configure Oracle database user and schema for embedded Operations Orchestration

A database user for embedded Operations Orchestration is required when installing Codar. Work with the database administrator to do the following (or see 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 `c$ad$b` are not valid names.

1. Create a schema for the embedded Operations Orchestration by creating a database user (for example, `codaroodbuser`).
2. Create a role for the user (for example, `codaroodbrole`) and grant the following privileges to the role:
   - `CONNECT`
   - `CREATE VIEW`
   - `CREATE SEQUENCE`
   - `CREATE TABLE`
   - `CREATE PROCEDURE`
   - `UNLIMITED TABLESPACE`
3. Grant the role to the Codar database user.

For example, run the following commands to create the codaroodbuser user:

```
Create user codaroodbuser identified by codaroodbuser default tablespace system temporary tablespace temp
quota unlimited on system account unlock;
Grant CONNECT to codaroodbuser;
Grant CREATE VIEW, CREATE SEQUENCE, CREATE TABLE, CREATE PROCEDURE, UNLIMITED TABLESPACE to codaroodbuser;
Commit;
```

You must provide this database user name and password when prompted for the Operations Orchestration database information during the installation of Codar.

Configure Oracle for localization (required for localization)

If you need to support localization, the Oracle database instance must support UTF-8 character encoding and multi-byte characters. Work with the database administrator to set the following parameters to the specified values (or see the manufacturer's documentation for more information):

- `NLS_CHARACTERSET = AL32UTF8`
- `NLS_LENGTH_SEMANTICS = CHAR`

Create Oracle tablespace for Codar (recommended)

If you chose to install embedded Operations Orchestration, for performance reasons, HPE recommends that you create a new tablespace which stores LOBs for the CODAR_DOCUMENT table. Work with the database administrator to create a tablespace to be used by Codar (or see the manufacturer's documentation for more information). HPE recommends that the initial tablespace size should be at least 3 GB.

> **Note:** The tablespace must be created before installing Codar and then must be configured immediately after Codar is installed.

Microsoft SQL server

You must complete the following installation and configuration steps if you wish to use MS-SQL with Codar.

"Install Microsoft SQL Server" below

"Configure Microsoft SQL Server" on the next page

Install Microsoft SQL Server

See the *Codar System and Software Support Matrix*, for a list of supported database versions.

The guide is available in HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals** .

Database installation is typically done in partnership with a database administrator. The Microsoft SQL Server must be installed with mixed mode authentication. During the installation of the Microsoft SQL Server, select **Mixed Mode (SQL Server authentication and Windows authentication)** from the Database Engine Configuration dialog for Authentication Mode.

Configure Microsoft SQL Server

The following tasks must be completed before Codar is installed. Work with the database administrator to complete these tasks, or see the manufacturer's documentation for more information.

> **Note:** These tasks are used with both embedded and external Operations Orchestration, except where indicated.

- "Enable TCP/IP on Microsoft SQL server " below
- "Configure Microsoft SQL server database user for Codar" below
- "Configure Microsoft SQL reporting database role and read-only user for Codar (required for reporting)" on the next page
- "Configure Microsoft SQL server database user for Identity Management component" on page 17
- "Configure Microsoft SQL server database user for embedded Operations Orchestration" on page 18
- "Create Microsoft SQL Server filegroup with embedded Operations Orchestration" on page 19

Enable TCP/IP on Microsoft SQL server

TCP/IP must be enabled on the Microsoft SQL Server for Codar to access the database. By default, TCP/IP may be disabled on the Microsoft SQL Server. Verify the TCP/IP configuration.

From the SQL Server Configuration Manager, complete the following steps:

1. Select **SQL Server Network Configuration** > **Protocols for <*instance_name*>**.
2. Double-Click **TCP/IP** to open the TCP/IP Properties dialog.
3. From the TCP/IP Properties dialog, select the **IP Addresses** tab.
4. Verify that TCP/IP is active and enabled, and verify that the TCP port is set to 1433. Update any properties that are not set correctly.

Configure Microsoft SQL server database user for Codar

A Codar database user is needed when installing Codar.

> **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 `c$ad$b` are not valid names.

To create a database user for Codar, complete the following steps:

1. Create a new database for Codar (for example, `codardb`)

   > **Caution:** Use the default database option collation value of `SQL_Latin1_General_CP1_CI_AS`.
   >
   > Do NOT use the collation value `SQL_Latin1_General_CP1_CS_AS`. Codar does not work with a database that is configured with this collation value.

2. Add a database user (for example, `codardbuser`) with the following roles:
   - `db_datareader`
   - `db_datawriter`
   - `db_owner`

   For example, run the following commands to create the `codardbuser` user with the specified roles:

   Microsoft SQL Server 2012

   ```
   USE csadb; -- or connect to csadb in another way
   CREATE LOGIN codardbuser WITH PASSWORD = '<codardbuser_password>';
   CREATE USER csadbuser FOR LOGIN codardbuser;
   ALTER ROLE db_datareader ADD MEMBER codardbuser;
   ALTER ROLE db_datawriter ADD MEMBER codardbuser;
   ALTER ROLE db_owner ADD MEMBER codardbuser;
   ```

   You must provide this database name, database username, and user's password when prompted for the CSA database information during the installation of CSA.

You must provide this user name and password when prompted for the Codar database user during the installation of Codar.

Configure Microsoft SQL reporting database role and read-only user for Codar (required for reporting)

If you are using both the Cloud Service Automation and Codar licenses, you can use the Cloud Service Automation reporting capabilities. If you want to use the reporting capabilities, you must add a Microsoft SQL reporting database role and read-only user when installing Codar. For details about the Cloud Service Automation reporting capabilities, see the *Cloud Service Automation Reporting and Auditing Whitepaper*.

> **Note:** You must apply both the Cloud Service Automation and Codar licenses to use the reporting capabilities.

> **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 `c$ad$b` are not valid names.

Add a reporting database user to the Codar database with no roles.

For example, run the following commands to create the `CODARReportingDBUser` read-only user:

```
CREATE LOGIN CODARReportingDBUser WITH PASSWORD = '<codarreportingdbuser_password>';
CREATE USER CODARReportingDBUser FOR LOGIN CODARReportingDBUser WITH DEFAULT_SCHEMA = codar;
```

If you configure this user, you must provide this user's user name and password when prompted for the Codar reporting database user during the installation of Codar.

Configure Microsoft SQL server database user for Identity Management component

An Identity Management component database user is needed when installing Codar.

> **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 `c$ad$b` are not valid names.

To create an Identity Management component database user for Codar, complete the following steps:

1. Create a new database for the Identity Management component (for example, `codaridmdb`).

   > **Caution:** Use the default database option Collation value of `SQL_Latin1_General_CP1_Cl_AS`.
   >
   > Do NOT use the collation value `SQL_Latin1_General_CP1_CS_AS`. Codar does not work with a database configured with this collation value.

2. You can use the existing database user you created for the Codar database (for example, `codardbuser`) or you may create a new database user for the Identity Management component database (for example, `codaridmdbuser`). If you create a new user, add an Identity Management component database user with the following roles:
   - `db_datareader`
   - `db_datawriter`
   - `db_owner`

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

Configure Microsoft SQL server database user for embedded Operations Orchestration

An Operations Orchestration database user for embedded Operations Orchestration is needed when installing Codar.

> **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 `c$ad$b` are not valid names.

To create an Operations Orchestration database user for Codar, complete the following steps:

1. Create a new database for Operations Orchestration.

   As of the release date of the Codar software (found at the beginning of this guide), the mandatory database options for the Microsoft SQL Server for Operations Orchestration are:

   - **Allow Snapshot Isolation**: True
   - **Is Read Committed Snapshot On**: True
   - **Auto Shrink**: False
   - **Auto Create Statistics**: True

   > **Caution:** You should verify the latest mandatory options and follow the instructions in the *Operations Orchestration Database Guide* when creating the *Operations Orchestration* database.

   > **Note:** Operations Orchestration recommends using the database option collation value of `SQL_Latin1_General_CP1_CS_AS`. When creating the database used by Operations Orchestration, this collation value is valid.

2. Create a new user for Operations Orchestration database (for example, codaroodbuser) and assign the following roles to that user:

   - `db_datareader`
   - `db_datawriter`
   - `db_owner`

You must provide this user name and password when prompted for the Operations Orchestration database user during the installation of Codar.

Create Microsoft SQL Server filegroup with embedded Operations Orchestration

If you chose to install embedded Operations Orchestration, for performance reasons, HPE recommends that you associate a new filegroup with the `CSA_DOCUMENT` table. Work with the database administrator to configure a filegroup to be used by Codar (or see the manufacturer's documentation for more information). HPE recommends that the initial filegroup size should be at least 3 GB.

The filegroup is configured after Codar is installed.

PostgreSQL

You must complete the following installation and configuration steps if you wish to use PostgreSQL with Codar.

"Install PostgreSQL" below

"Configure PostgreSQL users and database" below

Install PostgreSQL

See the *Codar System and Software Support Matrix*, for a list of supported database versions.

The guide is available in HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals** .

Install the database according to the manufacturer's documentation. Database installation is typically done in partnership with a database administrator.

Configure PostgreSQL users and database

The following tasks must be completed before Codar is installed. Work with the database administrator to complete the following tasks (or see the manufacturer's documentation for more information).

At least two database users are needed when installing Codar.

To configure PostgreSQL users and database, complete the following steps.

1. On the system hosting the database, install `postgres-client` if it is not already installed. As the root user, enter the following:

   Windows and Linux Ubuntu:

   ```
   apt-get install postgresql-client
   ```

   Linux Red Hat Enterprise

   ```
   rpm ivh postgres-client.rpm
   ```

2. For Linux Red Hat Enterprise, set the shared library path to include the PostgreSQL libraries (`<postgresql_installation>/lib`). For example, if you installed PostgreSQL in `/opt/PostgreSQL/9.2/`, run the following command:

   ```
   export LD_LIBRARY_PATH=/opt/PostgreSQL/9.2/lib:$LD_LIBRARY_PATH
   ```

3. Log in to `psql` as the `postgres` user.

   a. Enter the following:

   ```
   psql -h localhost -U postgres -d template1
   ```

   b. When prompted, enter the password for the postgres user.

4. Create a Codar database user (for example, `codardbuser`). The Codar database user is required. This user should inherit rights from parent roles and be a superuser.

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

   From the psql prompt, enter the following:

   ```
   create role codardbuser login password '<codardbuser_password>' superuser inherit;
   ```

   This is the user to whom you will grant access to the Codar database when you create this database.

5. For Windows and Linux Red Hat Enterprise, create an Operations Orchestration database user (for example, `codaroodbuser`). The Operations Orchestration database user, used by the embedded Operations Orchestration, is required. This user should inherit rights from parent roles and be a superuser.

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

   From the psql prompt, enter the following:

   ```
   create role codaroodbuser login password '<odaroodbuser_password>' superuser inherit;
   ```

This is the user to whom you will grant access to the Operations Orchestration database when you create this database.

6. Optionally, create an Identity Management component database user (for example, `codaridmdbuser`). This user should inherit rights from parent roles and be a superuser.

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

   From the psql prompt, enter the following:

   ```
   create role codaridmdbuser login password '<codarimdbuser_password>' superuser inherit;
   ```

   This is the user to whom you will grant access to the Identity Management component database when you create this database. If you do not create this user, you can use the Codar database user (for example, `codardbuser`) instead.

7. Optionally, create a reporting database user for Codar (for example, `CODARReportingDBUser`). A reporting database user is needed only if you want to use the reporting capabilities of Cloud Service Automation, and you are using both the Cloud Service Automation and Codar licenses. For details about the Cloud Service Automation reporting capabilities, see the *Cloud Service Automation Reporting and Auditing Whitepaper*. This user should have read-only rights.

   > **Note:** You must be using both the Cloud Service Automation and Codar licenses to use the reporting capabilities.

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

   From the psql prompt, enter the following:

   ```
   create role CODARReportingDBUser login password
   '<CODARReportingDBUser_password>' nosuperuser nocreatedb nocreaterole
   inherit;
   ```

   If you configure this user, you must provide this user's user name and password when prompted for the Codar reporting database user during the installation of Codar.

8. Create a new database for Codar. Grant the Codar database user all rights to this database. If you added a reporting database user in previous step, then grant the reporting database user read-only access to this database.

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

   For example, if you create a database named codardb, an Codar user named `codardbuser`, and a reporting database user `CODARReportingDBUser`, from the psql prompt, enter the following commands:

```
create database codardb with owner=codardbuser connection limit=-1;
grant all on database codardb to codardbuser;
grant connect on database codardb to CODARReportingDBUser;
```

You must provide this database name, database user name and, user's password when prompted for the Codar database information during the installation of Codar.

9. For Windows and Linux Red Hat Enterprise, create a new database for Operations Orchestration. Grant the Operations Orchestration database user all rights to this database. See the *Operations Orchestration Database Guide* for more information about database requirements for Operations Orchestration.

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

   For example, if you create a database named `codaroodb` and an Operations Orchestration user named `codaroodbuser`, from the psql prompt, enter the following commands:

   ```
   create database codaroodb with owner=codaroodbuser connection limit=-1;
   grant all on database codaroodb to codaroodbuser;
   ```

   You must provide this database name, database user name and, user's password when prompted for the Operations Orchestration database information during the installation of Codar.

10. Create a new database for the Identity Management component. Grant the Identity Management component database user (if you configured this user) or Codar database user all rights to this database.

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

    For example, to create a database named `codaridmdb` granting access to the Identity Management component database user named `codaridmdbuser`, from the psql prompt, enter the following commands:

    ```
    create database codaridmdb with owner=codaridmdbuser connection limit=-1;
    grant all on database codaridmdb to codaridmdbuser;
    ```

    If you did NOT create an Identity Management component database user named `codaridmdbuser`, create a database named `codaridmdb` and grant access to this database to the Codar database user named `codardbuser`. From the psql prompt, enter the following commands:

    ```
    create database codaridmdb with owner=codardbuser connection limit=-1;
    grant all on database codaridmdb to codardbuser;
    ```

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

11. Exit psql. From the psql prompt, enter the following:

\q

Install external Operations Orchestration

Install Operations Orchestration to the correct version and patch level.

If you are using an existing installation of Operations Orchestration, verify that the correct versions of patches and updates have been applied. See the *Codar System and Software Support Matrix* for version requirements.

> If you are using an earlier version of Operations Orchestration:
>
> **You must upgrade the HPE Operations Orchestration to supported version given in Codar System and Software Support Matrix before installing Codar**.
>
> After upgrading Operations Orchestration to the supported version, update it by following the instructions below.

> **Caution:** The Codar Installer installs an Embedded Operations Orchestration new instance during a new Codar 1.70 installation. The installer will also uninstall the same Embedded Operations Orchestrationinstance, regardless of whether it was loaded into a default or non-default installation path.

Configure an internal user

This internal user is used to configure Operations Orchestration for Codar. This step is required if you are going to integrate Operations Orchestration with Codar using the installer.

To configure an internal user, do the following:

1. Log in to the existing Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security** > **Internal Users**.
4. Click the Add (**+**) icon.

5. Enter the following information:

Field	Recommended value
User Name	admin
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

6. Click **Save**.
7. Enable authentication by selecting **Enable Authentication**.
8. Click **OK** in the confirmation dialog.

Export Operations Orchestration root certificate

Export the Operations Orchestration certificate from the Operations Orchestration truststore.

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 the Codar truststore by the Codar installer. SSL must be configured between Codar and Operations Orchestration.

For example, do the following:

1. On the system running Operations Orchestration, open a command prompt and change to the directory where Operations Orchestration is installed.
2. Run the following command:

   For Operations Orchestration 10.21 on Windows:
   `.\java\bin\keytool -export -alias tomcat -file C:\oo.cer -keystore .\Central\var\security\key.store -storepass <password>`

   For Operations Orchestration 10.21 on Linux:
   `./java/bin/keytool -export -alias tomcat -file /tmp/oo.cer -keystore ./Central/var/security/key.store -storepass <password>`

   where `C:\oo.cer` and `/tmp/oo.cer` are examples of file names and locations used to store the exported root certificate (you can choose a different file name and location).
3. 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.

Install Codar

See the appropriate sections for instructions on installing Codar:

- "Install Codar on Windows" below
- "Install Codar on Linux" on page 35
- "Post-installation database configuration" on page 45

> **Note:** 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.

Install Codar on Windows

> **Note:** Installation log files are written to the `CODAR_HOME\_Codar_1_60_0_installation\Logs\` folder.

To install Codar, 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` file. Go to the directory to which the files have been extracted and run the `setup.exe` installation file.
3. On the Introduction screen, read the information and click **Next**.
   a. Read the license agreement and select **I accept the terms of the License Agreement**. Click **Next** to continue with the installation.
4. Select **HPE Codar**, its feature name, and click **Next**.
5. Choose a location in which to install Codar and click **Next** (`CODAR_HOME` is set to this location).

   The default location is C:\Program Files\HPE\Codar.

> **Note:** If the folder in which you choose to install Codar is not empty, existing content in the folder may be overwritten or deleted when Codar is installed, upgraded, or uninstalled.

> **Caution:** The entire folder path cannot contain more than one dollar sign symbol ($). For example, `C:\HP\C$A\Java` and `C:\HP\CSA\Java$` are valid paths. However `C:\HP\C$A\Java$` and `C:\HP\C$$A\Java` are not valid paths.

6. Select the JRE that will be used by Codar.

   In this document, the folder in which the JRE is installed is referred to as `CSA_JRE_HOME`.

   For a list of supported JREs, see the *Codar System and Software Support Matrix.* This guide is available in HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals** .

   - **Open JRE**
     The Open JRE is bundled with Codar. If you want to use the Open JRE, click **Open JRE** and click **Next**.

     The default location in which the Open JRE is installed is C:\Program Files\HPE\Codar`\openjre`.

   - **Oracle JRE**
     If you have installed a supported version of Oracle JRE to be used by Codar, click **Oracle JRE**, select the location in which you installed this JRE, and click **Next**.

     The default location displayed for the Oracle JRE home is either a supported JRE that is configured in the system registry or a supported JRE in a path that is defined in the system path variable.

     If this is not the JRE that must be used by Codar, click **Choose** and select the location in which you installed the JRE that must be used by Codar.

   > **Caution:** The entire folder path cannot contain more than one dollar sign symbol ($).

7. Enter the port number in the **HPE Codar Port** field and click **Next**. The default port number is 8444.
8. 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
ooInboundUser	Used for HPE Operations Orchestration 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
ooInboundUser=p0s7f1tbmlse18v2
consumer=23tdvbntir6thmf3
csaTransportUser=jjcigu4kl6a989km
codarIntegrationUser=m16c2de8gaqqcc7c
securityEncryptedSigningKey=2surchgk13lsk7ll
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.

9. 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**.
10. 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 1.70. 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.

11. Select the type of database installed (Oracle, Microsoft SQL, or PostgresSQL) and click **Next**.

    For an Oracle database, you must also enter the **JDBC Driver Directory**. This is the absolute folder path to the location of the JDBC drivers (these are the JDBC drivers you downloaded onto the Codar system). For a list of supported JDBC driver versions, see the *Codar System and Software Support Matrix*.

    > **Caution:** The entire folder path cannot contain more than one dollar sign symbol ($).

12. Define the database instance on which the Codar database components should be installed or where the Codar database schema already exists. Separate database instances are required for Codar and the components it uses. You must create a separate database instance for:

    - Embedded Operations Orchestration
    - Identity Management component
    - Codar

    Enter the following database information and click **Next**.

Field	Description
<*database_type*> Database Host	The host name or IP address of the server where the database is located. When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.
<*database_type*> Database Port	The database port number, such as 1433 (Microsoft SQL Server), 1521 (Oracle), or 5432 (PostgreSQL).
HPE Codar Database Name/Oracle service name	The name of the database instance on which the Codar database schema will be installed (For example, codardb). ◦ If you are creating a new Codar database schema, this is the name of the database instance on which the Codar database components will be installed. ◦ If you are using an existing Codar database schema that was created as part of a prior successful installation of Codar version 1.70, this is the name of the database instance on which the Codar database schema exists. ◦ For an Oracle database, this is the service name.
HPE Codar Database User Name	The user name of the database user you configured for Codar in the database (for example, codardbuser).
HPE Codar Database Password	The password for the database user.

13. If you have created a reporting database role and read-only user when you configured the Codar database, select **Reporting User** and enter the following information:

> **Note:** You must be using both the Cloud Service Automation and Codar licenses to use the Cloud Service Automation reporting capabilities. For details, see the *Cloud Service Automation Reporting and Auditing Whitepaper*.

Field	Description
HPE Codar Reporting Database User Name	The user name of the database user you configured for reporting purposes for Codar. For details on configuring the reporting database user, see one of these sections, depending on which database you installed: "Configure Oracle Database" on page 9, "Configure Microsoft SQL Server" on page 15, or "Configure PostgreSQL users and database" on page 19.
HPE Codar Reporting Database User Password	This is the password for the Codar reporting database user.

14. Enter the database information for the database used by the Identity Management component and click **Next**. The database used by the Identity Management component must be the same type of database used by Codar. Enter the following database information:

Field	Description
<*database_type*> Database Host	The host name or IP address of the server where the Identity Management component database is located.
<*database_type*> Database Port	The Identity Management component database port number, such as 1433 (Microsoft SQL Server), 1521 (Oracle), or 5432 (PostgreSQL).
IDM Database Name/Oracle service name	The name of the database instance used by the Identity Management component. For example, `codaridmdb`. For an Oracle database, this is the Oracle service name.
IDM Database User Name	The user name of the database user you configured for the Identity Management component database (for example, `codaridmdbuser` or `codardbuser`). For details on configuring the Identity Management component database user, see one of these sections, depending on which database you installed: "Configure Oracle Database" on page 9, "Configure Microsoft SQL Server" on page 15, or "Configure PostgreSQL users and database" on page 19.
IDM Database Password	The password for the Identity Management component database user.

15. From the Enter host name screen, enter the fully-qualified domain name of the system on which you are installing Codar. The fully-qualified domain name is used to generate the self-signed SSL certificate which is used when https browser requests are issued for Codar. This self-signed certificate expires 120 days after Codar is installed.

> **Caution:** If you enter an IP address, after installation completes, you must manually generate a self-signed certificate using the fully-qualified domain name of the system on which you installed Codar and manually reconfigure Codar to use this certificate. For more information, see the *Codar Configuration Guide*.

16. By default, Single Sign-On (SSO) is included with Codar. The Single Sign-On that is included can only be used when launching an application, such as Operations Orchestration, from the Codar Console. See the Single Sign-On documentation for more information on integrating Single Sign-On with an application.

    If you want to use Single Sign-On, you can enable it by selecting **Enable HPE SSO**.

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

    > **Note:** You must enter the full domain name of the server. For example, if you are installing Codar on a system whose fully-qualified domain name is `machine1.development.xyz.com`, you must enter `development.xyz.com`. If you enter only `xyz.com`, you will not be able to log in to the Codar Console.

    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 whether you want to install the embedded (new) Operations Orchestration instance with Codar or if you are integrating with an external (existing) instance of Operations Orchestration.
    - To install the embedded Operations Orchestration, select **Install embedded HPE OO** and click **Next**. Proceed to Steps 18 - 20.
    - To integrate with an external (existing) instance of Operations Orchestration, select **Use external HPE OO** and click **Next**. Proceed to Step 21.

18. If you chose to install the embedded Operations Orchestration, choose Operations Orchestration installation path as location and click **Next**.

    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 **Install sample content** and click **Next**.

    To deploy the sample content at a later time, select **Skip content installation** and click **Next**.

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

19. Configure an internal Operations Orchestration user and click **Next**. This user is used for provisioning topology designs.

Field name	Description
HPE OO User Name	The name of the user used for provisioning topology designs. This user is given the ADMINISTRATOR and SYSTEM_ADMIN roles. The recommended user name is **admin**.
HPE OO Password	The password used by Operations Orchestration for the user who provisions topology designs. The recommended password is **cloud**.
Confirm Password	Re-enter the password for confirmation.
HPE OO Port	The embedded Operations Orchestration port number, such as 8445, used to access Operations Orchestration Central. By default, Operations Orchestration uses this port and port 8080. Applications running on the system on which Codar and the embedded Operations Orchestration are installed should not be using these ports.

20. Enter the database information for the database used by the embedded Operations Orchestration and click **Next**. The database used by the embedded Operations Orchestration must be the same type of database used by Codar.

Field name	Description
<*database_type*> Database Host	The host name or IP address of the server where the embedded Operations Orchestration database is located. When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.
<*database_type*> Database Port	The embedded Operations Orchestration database port number, such as 1433 for Microsoft SQL Server, 1521 for Oracle, or 5432 for PostgreSQL.
HPE OO Database Name or Oracle HPE OO SID	The name of the database instance used by the embedded Operations Orchestration. For an Oracle database, this is the service name.
HPE OO Database User Name	The user name of the database user you configured for the Operations Orchestration database. See one of these sections, depending on which database you installed: "Configure Oracle Database" on page 9, "Configure Microsoft SQL Server" on page 15, or "Configure PostgreSQL users and database" on page 19.
HPE OO Database Password	The password for the Operations Orchestration database user.

21. If you chose to integrate with an external (existing) Operations Orchestration, define the existing Operations Orchestration instance with which Codar is to be integrated. Enter the following information (select **Enter** after each entry) and click **Next** when

done.

Field	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 Operations Orchestration's certificate. The hostname is used for SSL 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 Codar, selecting the Process ID opens Operations Orchestration to the detailed page of the selected process when these properties are configured). When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.
Operations Orchestration Port	The port number used to communicate with Operations Orchestration, such as 8445. By default, Operations Orchestration uses this port and port 8080. **Caution:** Ensure that port 8080 is not being used on the system where you install Codar and the embedded Operations Orchestration. If this port is used, then Operations Orchestration flows will not work properly.
Operations Orchestration User	The name of the user who logs in to Operations Orchestration Central. HPE recommends that you use the `admin user` you defined in "Install external Operations Orchestration" on page 24.
Operations Orchestration Password	The password used 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 Operations Orchestration's certificate and copy it to the Codar system.

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.

If you are using unsupported version of Operations Orchestration, you will get a **warning** message. HPE recommends that you stop the current installation, check the System and Software Support Matrix document, install or upgrade to a supported Operations Orchestration version, then restart the Codar installation.

If you continue with the installation, you may get provisioning errors. Using an unsupported version of Operations Orchestration may also result in a limited amount of demo content that users can select for installation.

(**Not Recommended**) If you have understood the warning, click **Next** to continue with the installation.

22. 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 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 Iaas 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 Iaas 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.

23. Review your selections and click **Install** to complete the installation.
24. You may be asked to restart your system.

    Click **Yes, restart my system** to restart your system when you exit the installer.

Click **No, I will restart my system myself** to restart your system at a more convenient time.

25. Click **Done** to exit the installer.
26. Verify that the Codar and Operations Orchestration services have started by navigating to **Start**> **Administrative Tools** > **Services**. The service may take up to five minutes to start.

    If the service has not started, right-click on the service and select **Start**.

    The installer creates the Codar services. If you opted to install the Codar database components, the installer also starts these services. The Codar service must be running before you can access the Codar Console.

Install Codar on Linux

> Before installing Codar on Linux, ensure that **Unzip** utility and **bzip2** are installed in the Linux machine.

Configure group and user

To configure a group and user for Codar, complete the following steps:

1. Log in to the system as the root user.
2. Create a group called `codargrp`. Enter the following:

   `addgroup codargrp` (Ubuntu)
   `groupadd codargrp` (Red Hat Enterprise Linux)
3. Create a user called `codaruser` and assign this user to the `codargrp`. Enter the following:

   `adduser -g codargrp -m codaruser` (Ubuntu)
   `useradd -g codargrp -m codaruser -s /bin/bash` (Red Hat Enterprise Linux)
4. Assign a password to the `codaruser`. Enter the following:

   ```
   passwd codaruser
   ```

   When prompted, enter the password.

Install Codar

Note: Installation log files are written to the `/_Codar_1_70_0_installation/Logs/` directory and are named `codar_*.txt`.

To install Codar on Linux, complete the following steps.

1. Log in to the system as the root user.
2. Create an installation directory for Codar (this document assumes that you will install the product in `/usr/local/hpe/codar` and all examples used in this document are based on this assumption). Enter the following:

   ```
   mkdir -p /usr/local/hpe/codar
   ```

3. For the installation directory, set the owner to codaruser and the group to codargrp. Enter the following:

   ```
   chown -R codaruser:codargrp /usr/local/hpe/codar
   ```

4. Log out as the root user and log in as codaruser.
5. Copy the Codar installation file (`setup-codar.bin`) to the system and go to the directory in which it has been copied.
6. Verify that `setup-codar.bin` is owned by codaruser and that codaruser has full permissions for the file. If necessary, complete the following steps:
   a. Log in as the root user
   b. Enter one or both of the following commands:

      ```
      chown codaruser setup-codar.bin
      chmod u+rwx setup-codar.bin
      ```

   c. Log out as the root user and log in as codaruser.
7. Check the values of the `CSA_HOME`, `PS1`, and `TITLEBAR` 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.
8. Run the `setup-codar.bin` installation file.

   Note: You must run `setup-codar.bin` as the codaruser. If you install 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** to scroll through the entire agreement.
11. Select **Y** and **Enter** to accept the license agreement and continue with the installation. Select **N** press **Enter** to exit the installation.

12. Select **HPE Codar** and press **Enter**.
13. Enter a location in which to install Codar (enter the absolute path to the location) and press **Enter**. Or, press **Enter** to accept the default location.

    The default location is `/usr/local/hpe/codar`.

    > **Note:** If the directory in which you choose to install Codar is not empty, existing content in the directory may be overwritten or deleted when Codar is installed, upgraded, or uninstalled.

    If prompted, verify the installation folder. If the folder is correct, select **Y** and **Enter** to continue with the installation. If the folder is not correct, select **N** and **Enter** to re-enter the installation folder.
14. Choose the JRE that will be used by Codar.

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

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

    Open JRE

    The Open JRE is bundled with Codar. If you want to use the Open JRE, type **1** and press **Enter**.

    The default location in which the Open JRE is installed is `/usr/local/hpe/codar/openjre`.

    Oracle JRE

    If you have installed a supported version of Oracle JRE to be used by Codar, type **2** and press **Enter**. Type the location in which you installed this JRE and press **Enter** key.

    The default location displayed for the Oracle JRE Home is either a supported JRE that is configured in the system registry or a supported JRE in a path that is defined in the system path variable. If this is not the JRE that should be used by Codar, type in the location in which you installed the JRE that will be used by Codar and press **Enter** key.

    Proceed to Step 26 for instructions on configuring Oracle JRE.
15. Enter the port number in the **HPE Codar Port** field and press **Enter** key. The default port number is 8444.
16. 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
ooInboundUser	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
ooInboundUser=p0s7f1tbmlse18v2
consumer=23tdvbntir6thmf3
csaTransportUser=jjcigu4kl6a989km
codarIntegrationUser=m16c2de8gaqqcc7c
securityEncryptedSigningKey=2surchgk13lsk7ll
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**.

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

    Type **yes** to install Codar database components and create the Codar database schema. When you select this option, the Codar process automatically starts when you exit the installer.

    Type **no** if you are using an existing Codar database schema that was created as part of a prior successful installation of Codar version 1.70. When you select this option, the Codar process does not start when you exit the installer. See the end of this section for information on how to start and stop the Codar service.

19. Define the database instance on which the Codar database components should be installed. Enter the following database information (press **Enter** after each entry).

    a. Enter the type of database you have installed: MSSql (Microsoft SQL Server), Oracle, or Postgres (PostgreSQL).

       For an Oracle database, you must also enter the **JDBC Driver Directory**. This is the absolute directory path to the location of the JDBC drivers (these are the JDBC drivers you downloaded onto the Codar system). For a list of supported JDBC driver versions, see the *Codar System and Software Support Matrix*.

    b. Enter the database hostname. This is the hostname or IP address of the server where the database is located. When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`. The default value is the IP address of the localhost (127.0.0.1).

    c. Enter the database port. This is the database port number, such as 1433 (Microsoft SQL Server), 1521 (Oracle), or 5432 (PostgreSQL).

    d. Enter the database name. This is the name of the database instance on which the Codar database schema will be installed.

       If you are creating a new Codar database schema, this is the name of the database instance on which the Codar database components will be installed.

       If you are using an existing Codar database schema that was created as part of a prior successful installation of Codar version 1.70, this is the name of the database instance on which the Codar database schema already exists.

       If you followed the examples in this document, enter **codardb**.

    e. Enter the Codar database user name. This is the user name of the database user you configured for Codar in the appropriate database configuration section of this guide.

       If you followed the examples in this document, enter **codardbuser**.

    f. Enter the Codar database password. This is the password for the Codar database user.

    g. Enter the Codar reporting database user name (optional). This is the user name of the database user you configured for reporting purposes for Codar. For details on configuring the reporting database user, see one of these sections, depending on which database you installed: "Configure Oracle Database" on page 9, "Configure Microsoft SQL Server" on page 15, or

"Configure PostgreSQL users and database" on page 19.

h. Enter the password for the Codar reporting database user.

> **Note:** You must be using both the Cloud Service Automation and Codar licenses to use the Cloud Service Automation reporting capabilities. For details, see the *Cloud Service Automation Reporting and Auditing Whitepaper*.

20. Provide the database instance used by the Identity Management component. Enter the following database information (press **Enter** after each entry).

    a. Enter the **database hostname**. The host name or IP address of the server where the database is located. When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.

    b. Enter the **database port**. This is the database port number, such as 1433 (Microsoft SQL Server), 1521 (Oracle), or 5432 (PostgreSQL).

    c. Enter the **Identity Management component Database Name/Oracle SID**. The name of the database instance used by the Identity Management component.

    d. Enter the **Identity Management component Database User Name**. This is the user name of the database user you configured for the Identity Management component database. For details on configuring the Identity Management component database user, see one of these sections, depending on which database you installed: "Configure Oracle Database" on page 9, "Configure Microsoft SQL Server" on page 15, or "Configure PostgreSQL users and database" on page 19.

    e. Enter the **Identity Management component database password**. This is the password for the Identity Management component database user.

21. Enter the Codar server host name. This is the **fully-qualified domain name of the system on which you are installing Codar**. The fully-qualified domain name is used to generate the self-signed SSL certificate which is used when https browser requests are issued for Codar. This self-signed certificate expires 120 days after Codar is installed.

    > **Caution:** If you enter an IP address, after installation completes, you must manually generate a self-signed certificate using the fully-qualified domain name of the system on which you installed Codar and manually reconfigure Codar to use this certificate.

22. By default, Single Sign-On (HPE SSO) is included with Codar. The Single Sign-On that is included with Codar can only be used when launching an application, such as Operations Orchestration or HPE IT Executive Scorecard, from the Codar Console. See the Single Sign-On documentation for more information on integrating Single Sign-On with an application.

    If you do not want to use Single Sign-On, you can disable it. Type **2** and select **Enter**.

    To enable Single Sign-On, type **1** and select **Enter**. Enter the Domain name of the network to which the server belongs (the server on which you are installing Codar) and select **Enter**.

> **Note:** You must enter the full domain name of the server. For example, if you are installing Codar on a system whose fully-qualified domain name is `machine1.marketing.xyz.com`, you must enter marketing.`xyz.com`. If you enter only `xyz.com`, you will not be able to log in to the Codar Console.

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.

23. Specify whether you want to install the embedded (new) Operations Orchestration instance with Codar or if you are integrating with an external (existing) instance of Operations Orchestration.
    - Select **1** and **Enter** to integrate with an external (existing) instance of Operations Orchestration. Proceed to Step 20a.
    - Select **2** and **Enter** to install the embedded Operations Orchestration. Proceed to Step 20b.

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

    To deploy the sample content during the installation process, type 1 (Install sample content) and press **Enter**.

    To deploy the sample content at a later time, type **2** (Skip content installation) and press **Enter**. If you choose to skip content installation, you can install the content at a later time, by running the . For details, see the *Cloud Service Automation Content Pack User Guide*.

    a. If you are integrating with an external (existing) Operations Orchestration, define the Operations Orchestration instance with which Codar is to be integrated. Enter the following information (press **Enter** after each entry). Proceed to step 21.

        i. Enter the **Operations Orchestration host name**. 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 the Operations Orchestration 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).

        ii. 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.

        > **Caution:** Ensure that port 8080 is not being used on the system where you install Codar and the embedded Operations Orchestration. If this port is used, then Operations Orchestration flows will not work properly.

        iii. Enter the **Operations Orchestration user**. This is the name of the user who logs in to Operations Orchestration

Central. HPE recommends that you use the `admin` user. If you followed all the steps documented in "Install external Operations Orchestration" on page 24, this is the `admin` user.

iv. Enter the **Operations Orchestration password**. This is the password used to log in to Operations Orchestration Central. If you followed all the steps documented in "Install external Operations Orchestration" on page 24, use the password `cloud`

v. Re-enter the Operations Orchestration password.

vi. Enter the **Operations Orchestration certificate file**. This is 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 certificate and copy it to the Codar system (see "Install external Operations Orchestration" on page 24 for more information).

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

b. If you are installing embedded Operations Orchestration, enter a location and press **Enter**.

i. Enter the database information for the database used by the embedded Operations Orchestration (press **Enter** after each entry). The database used by the embedded Operations Orchestration must be the same type of database used by the Codar (Microsoft SQL Server, Oracle, or PostgreSQL).

A. Enter the **database hostname**. This is the hostname or IP address of the server where the embedded Operations Orchestration database is located. When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.

B. Enter the **database port**. This is the embedded Operations Orchestration database port number, such as 1433 for Microsoft SQL Server, 1521 for Oracle, or 5432 for PostgreSQL.

C. Enter the **Operations Orchestration database name or Oracle Operations Orchestration SID**. This is the name of the database instance used by the embedded Operations Orchestration. For an Oracle database, this is the Oracle service name.

D. Enter the **Operations Orchestration database user name**. This is the user name of the database user you configured for the Operations Orchestration database.

E. Enter the Operations Orchestration database password. This is the password for the Operations Orchestration database user.

F. Enter the **embedded Operations Orchestration port number**, such as 8445. By default, Operations Orchestration uses this port and port 8080. Applications running on the system on which Codar and the embedded Operations Orchestration are installed should not be using these ports.

ii. Configure an internal Operations Orchestration user (press **Enter** after each entry). This user is used for provisioning topology designs.

A. Enter the **Operations Orchestration user name**. This is the name of the user used for provisioning topology designs. This user is given the ADMINISTRATOR and SYSTEM ADMIN roles. The recommended user name is **admin**.

B. Enter the **Operations Orchestration password**. This is the password used by Operations Orchestration for the user who provisions topology designs. The recommended password is **cloud**.

24. 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 Iaas 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 Iaas 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*.

25. Review your selections and press **Enter** to complete the installation or **Ctrl**-**C** to exit the installation.
26. When the installation completes, press **Enter** to exit the installer.
27. If you selected to use the OpenJDK JRE with Codar and installed Codar on a system running a headless Ubuntu Linux version 14, install the **Standard Java or Java-compatible Runtime** package. Enter the following:

    ```
    apt-get install default-jre
    ```

28. Define the `CSA_HOME` and `JAVA_HOME` environment variables and add `/sbin` to the PATH variable for the codaruser user. Set `CSA_HOME` to the location where Codar is installed. In a startup script for the codaruser user (for example, `.profile` (Ubuntu) or `.bash_profile` (Red Hat Enterprise Linux)), add the following:

    ```
    export CSA_HOME=/usr/local/hpe/codar
    export JAVA_HOME=CSA_JRE_HOME
    export PATH=$PATH:/sbin
    ```

    where `CSA_JRE_HOME` is the directory where the JRE used by Codar is installed.

29. Source the startup file in which you set the `CSA_HOME`, `JAVA_HOME`, and `PATH` environment variables. If you edited `.bashrc` (Ubuntu) or `.bash_profile` (Red Hat Enterprise Linux), enter the following:

    `. ./.bashrc` (Ubuntu)
    `. ./.bash_profile` (Red Hat Enterprise Linux)

30. Create an Codar service to start and stop the Codar processes.
    a. Log in as the root user.
    b. Go to the directory in which Codar is installed. For example:

       ```
       cd /usr/local/hpe/codar
       ```

    c. Copy the `codar` script to the `/etc/init.d` directory. Enter the following:

       ```
       cp ./scripts/codar /etc/init.d
       ```

    d. Change permissions of the scripts. Enter the following:

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

    e. Log out as the root user.
31. Log in as codaruser and start the Codar service. Enter the following:

    ```
    service codar start
    ```

32. As `codaruser`, restart the Operations Orchestration Central service. Enter the following:

```
/usr/local/hpe/codar/OO/central/bin/central stop/usr/local/hpe/codar/OO/central/bin/central start
```

The Codar service must be running in order to access Codar Console. You can use the following commands:

`service codar start` - to start the Codar service

`service codar restart` - to restart the Codar service

`service codar stop` - to stop the Codar service

`service codar status` - to check the status of the Codar service

The Operations Orchestration Central service must be running in order to access Operations Orchestration Central. You can use the following commands:

`/usr/local/hpe/codar/OO/central/bin/central start` - to start the Operations Orchestration service

`/usr/local/hpe/codar/OO/central/bin/central stop`. - to stop the Operations Orchestration service

Post-installation database configuration

The following steps are required for either Oracle or Microsoft SQL Server, after you have installed Codar.

Configure Oracle tablespace

Configure the Oracle tablespace you created for Codar only if you are installing Codar for the first time and there is no data in the CODAR_DOCUMENT table. The tablespace must have been created before Codar is installed and then must be configured immediately after Codar is installed (see "Configure Oracle Database" on page 9 for information on creating the Oracle tablespace).

Work with the database administrator to perform the following (or see the manufacturer's documentation for more information):

Modify the CODAR_DOCUMENT table such that LOB segments are stored in the tablespace. For example:

```
ALTER TABLE CODAR_DOCUMENT
 MOVE LOB(content)
 STORE AS (TABLESPACE <new_tablespace>);
```

Configure Microsoft SQL Server filegroup

Configure the Microsoft SQL server filegroup you created for Codar only if you are installing Codar for the first time and there is no data in the CODAR_DOCUMENT table. The filegroup must have been created before Codar is installed and then must be configured immediately after Codar is installed (see "Configure Microsoft SQL Server" on page 15 for information on creating the Microsoft SQL server filegroup).

Work with the database administrator to perform the following (or see the manufacturer's documentation for more information):

1. Drop all constraints from the CODAR_DOCUMENT table.
2. Drop the CODAR_DOCUMENT table.
3. Recreate the CODAR_DOCUMENT table and associate it with the filegroup.
4. Recreate the constraints for the CODAR_DOCUMENT table.



Configure Operations Orchestration

The Codar solution includes a number of Operations Orchestration flows that perform Codar operations.

- If you installed embedded Operations Orchestration, see "Configure embedded Operations Orchestration" on the next page.
- If you installed external Operations Orchestration, see "Configure external

Hewlett Packard Enterprise

Configure embedded Operations Orchestration

Complete the following tasks to configure the embedded Operations Orchestration to integrate successfully with Codar (if you are configuring an exclusive stand-alone Operations Orchestration, you do not need to complete these tasks):

- "Add JRE to the system path" below
- "Configure internal users" on the next page
- "Deploy content packs required by Codar" on page 50
- "Verify deployed content packs" on page 50
- "Deploy Operations Orchestration and component tool content packs" on page 51
- "Set up system accounts for the Codar content pack" on page 53
- "Set up system properties for the Codar content pack" on page 53
- "Configure Single Sign-On" on page 54

> **Note:** In the following instructions, `CSA_HOME` is the directory in which Codar is installed and `ICONCLUDE_HOME` is where you installed Operations Orchestration.
>
> Be sure all the latest patches for Operations Orchestration have been installed. See the *Codar System and Software Support Matrix* for more information.

Add JRE to the system path

The Codar flows that are imported require that a JRE be included in the system path on the system running Codar.

To add a JRE to the system path on Windows, complete the following steps:

1. Open the **Environment Variables** dialog:
    a. Right-click **Computer** and select **Properties**.
    b. Select **Advanced System Settings**.
    c. Click **Environment Variables**.
2. Select the **Path** system variable.

3. Click **Edit**.
4. At the end of the value for **Variable value**, add a semicolon (;) and the following path:

   `CSA_JRE_HOME\bin`

   where `CSA_JRE_HOME` is the directory in which the JRE used by Codar is installed. .
5. Click **OK** and close all windows.

To add a JRE to the system path on Linux, complete the following steps:

Open a shell and enter the following command:

```
export PATH=$PATH:CSA_JRE_HOME/bin
```

where `CSA_JRE_HOME` is the directory in which the JRE used by Codar is installed.

> **Note:** By setting the system path, all applications (that require a JRE) use the JRE that is installed with HP Codar (if it is the only path or the first path set to a JRE in the system path). If you need to run another JRE with an application, you must type in the relative path to that JRE in order to run it (for example, when you configure SSL).

Configure internal users

Internal users can be used to configure Operations Orchestration for Codar.

> **Note:** The user is automatically added while installing Codar.

1. Log in to the existing Operations Orchestration central,
2. Click the **System Configuration** button.
3. Select **Security > Internal Users**.
4. Click the **Add** (+) icon.
5. Enter the following information:

Field	Recommended value
User Name	codaroouser

Field	Recommended value
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

The codaroouser user is used to import the Operations Orchestration flows. When importing flows, this user is configured in the Operations Orchestration input file used by the process definition tool.

6. Click **Save**.
7. Enable authentication by selecting the **Enable Authentication** check box.
8. Click **OK** in the confirmation dialog.
9. Log out of Operations Orchestration Central and log back in as the codaroouser.

Deploy content packs required by Codar

There are three sets of content packs that should be deployed for Codar: the base Operations Orchestration content packs, the Codar component tool content packs, and the Codar content pack.

The base Operations Orchestration and Codar component tool content packs were deployed automatically when you installed Codar. If these content packs failed to deploy during installation, you must deploy them manually.

Download the Codar 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. The Codar content pack must be deployed after the base Operations Orchestration content packs have been deployed. For details about the Content Capsule Installer, see the *Cloud Service Automation Content Pack User Guide*.

Verify deployed content packs

To verify that the Operations Orchestration and component tool 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 Operations Orchestration Central.
2. Click the **Content Management** button.
3. Click the **Content Packs** tab.
4. From Operations Orchestration Central, click the **Content Management** button.
5. Click the **Content Packs** tab.
6. Click the **Deploy New Content** icon.
7. In the Deploy New Content dialog, click the **Add files for deployment** icon.
8. 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.

   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.

Deploy Codar content pack

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

Download the Codar HP 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*.

Set up system accounts for the Codar content pack

Set up system accounts for the Codar content pack:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Select **Configuration Items** > **System Accounts**.
4. Click the **Add** icon.
5. Enter the following information if it is not already configured:

Field	Recommended value
System Account Name	`CODAR_REST_CREDENTIALS`
User Name	`ooInboundUser`
Password	cloud

> **Note:** The **User Name** configured for the CODAR_REST_CREDENTIALS System Account setting must match the **Override Value**(Operations Orchestration version 10.21) configured for the `CODAR_OO_USER` system property setting.

6. Click **Save**.

Set up system properties for the Codar content pack

Set up the following system properties for the Codar content pack:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Select **Configuration Items** > **System Properties**.
4. Click the **Add** icon.
5. Enter the following information if it is not already configured:

Field	Recommended Value
Name	`CODAR_REST_URI`
Override Value	`https://<codar_hostname>:8444/csa/api`

6. Click **Save**.

Configure Single Sign-On

For instructions, see "Configure Single Sign-On between Codar and Operations Orchestration" on page 61.

Configure external Operations Orchestration

Complete the following tasks to configure Operations Orchestration to integrate with Codar:

- "Add JRE to system path" on the next page
- "Install Codar content packs" on page 56
- "Configure internal users" on page 56
- "Deploy content packs required by Codar" on page 57
- "Set up system accounts for Codar content pack" on page 59
- "Set up system properties for Codar content pack" on page 60
- "Configure Single Sign-On" on page 60

> **Note:** In the following instructions, `CSA_HOME` is the directory in which Codar is installed and `ICONCLUDE_HOME` is where you installed Operations Orchestration.
>
> Be sure all the latest patches for Operations Orchestration have been installed. See the *Codar*

> *System and Software Support Matrix* for more information.

Add JRE to system path

The Codar flows that are imported require that a JRE be included in the system path on the system running Codar.

On Windows:

1. Open the **Environment Variables** dialog:
   a. Right-click **Computer** and select **Properties**.
   b. Select **Advanced System Settings**.
   c. Click **Environment Variables**.
2. Select the **Path** system variable.
3. Click **Edit**.
4. At the end of the value for **Variable value**, add a semicolon (;) and the following path:

   If Operations Orchestration and Codar are installed on the same system:

   ```
   ICONCLUDE_HOME\java\bin
   ```

   or

   If Operations Orchestration and Codar are installed on different systems:

   ```
   CSA_JRE_HOME\bin
   ```
5. Click **OK** and close all windows.

On Linux:

Open a shell and enter the following command:

If Operations Orchestration and Codar are installed on the same system:

```
export PATH=$PATH:$ICONCLUDE_HOME/java/bin
```

or

If Operations Orchestration and Codar are installed on different systems:

```
export PATH=$PATH:CSA_JRE_HOME/bin
```

Note: By setting the system path, all applications (that require a JRE) use the JRE that is installed with Operations Orchestration or Codar (depending on the path you configured and if it is the only path or the first path set to a JRE in the system path). If you need to run another JRE with an application, you must type in the relative path to that JRE in order to run it (for example, when you configure SSL).

Install Codar content packs

Install the Codar content packs by running the Content Capsule Installer. Download the Codar 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 running the Content Capsule Installer, see the *Cloud Service Automation Content Pack User Guide*.

Configure internal users

Internal users can be used to configure Operations Orchestration for Codar.

1. Log in to Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security** > **Internal Users**.
4. Click the Add (**+**) icon.
5. Enter the following information:

Field	Recommended value
User Name	codaroouser
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

   The codaroouser user is used to import the Operations Orchestration flows. When importing flows, this user is configured in the Operations Orchestration input file used by the process definition tool.
6. Click **Save**.
7. Enable authentication by selecting the **Enable Authentication** check box.
8. Select **OK** in the confirmation dialog.

9. Enter the following information:

Field	Recommended value
User Name	admin
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

10. Click **Save**.
11. Enable authentication by selecting **Enable Authentication**.
12. Click **OK** in the confirmation dialog.
13. Log out of Operations Orchestration Central and log back in as the codaroouser.

Deploy content packs required by Codar

Download the Codar 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 the 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 the 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. Select, open, and deploy the following Codar 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`

   The deployment may take a few minutes and the dialog will show a progress bar.
8. Click the **Deploy New Content** icon.
9. Click the **Add files for deployment** icon.
10. Navigate to the `CSA_HOME\Tools\ComponentTool\contentpacks\` directory, select all the content packs, and click **Open**.
11. Click **Deploy**.

    The deployment may take a few minutes and the dialog will show a progress bar.
12. When the deployment succeeds, click **Close** to close the dialog.

Set up system accounts for Codar content pack

Set up system accounts for the Codar content pack:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Select **Configuration Items** > **System Accounts**.
4. Click the **Add** icon.
5. Enter the following information if it is not already configured:

Field	Recommended value
System Account Name	CSA_REST_CREDENTIALS
User Name	ooInboundUser
Password	cloud

> **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Override Value**(Operations Orchestration version 10.21) configured for the CODAR_OO_USER System Property setting.

6. Click **Save**.

Set up system properties for Codar content pack

Set up the following system properties for the Codar content pack:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Select **Configuration Items** > **System Properties**.
4. Click the **Add** icon.
5. Enter the following information if it is not already configured:

Field	Recommended Value
Name	CSA_REST_URI
Override Value	https://<*codar_hostname*>:8444/csa/api

6. Click **Save**.

Configure Single Sign-On

For instructions, see "Configure Single Sign-On between Codar and Operations Orchestration" on the next page.

Configure Single Sign-On between Codar and Operations Orchestration

If Single Sign-On was enabled during installation of Codar, Single Sign-On can be configured between Codar and Operations Orchestration. Configuring Single Sign-On allows you to launch Operations Orchestration from the Codar Console without having to log in to Operations Orchestration.

Codar provides an out-of-the-box user (**admin**) and password (**cloud**) and, earlier in this guide, you configured an internal user for Operations Orchestration with the same user name and password. When Single Sign-On is configured between Codar and Operations Orchestration, this user can be used for single sign-on. That is, if you are logged in to Codar as the admin user, you can launch Operations Orchestration from the Codar Console and not have to log in to Operations Orchestration.

You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure Codar and the embedded Operations Orchestration to use the same LDAP source or, if Codar and the embedded Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the Codar user must be assigned to the Codar Administrator or Service Operations Manager role and the embedded Operations Orchestration user must be assigned any role that allows flows to be viewed.

> **Note:** To use Single Sign-On between Codar and Operations Orchestration, the systems on which Codar and Operations Orchestration are installed must be in the same domain.

Enable Single Sign-On

To configure and enable Single Sign-On on Operations Orchestration, complete the following steps:

1. Log in to Operations Orchestration Central.

2. Click the **System Configuration** button.

3. Select **Security > SSO**.

4. Select the **Enable** checkbox.

5. Enter the **InitString**. The initString setting for Codar and Operations Orchestration must be configured to the same value. In Codar, initString is configured in the crypto element in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEBINF\hpssoConfiguration.xml` file. The initString value represents a secret key and should be treated as such in your environment (this string is

used to encrypt and decrypt the `LWSSO_COOKIE_KEY` cookie that is used to authenticate the user for single sign-on).

6. Enter the **Domain**. This is the domain name of the network of the servers on which Codar and Operations Orchestration are installed.

7. Click **Save**.

Configure LDAP Users for Single Sign-On

In order to enable single sign-on for LDAP users, you must either configure Codar and Operations Orchestration to use the same LDAP source or, if Codar and Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the Codar user must be assigned to the Codar Administrator or Service Operations Manager role and the Operations Orchestration user must be assigned any role that allows flows to be viewed.

To configure LDAP for Operations Orchestration, complete the following steps:

1. Log in to Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security > LDAP**.
4. Enter the information to configure LDAP.
5. Click **Save**.

Post-installation

You have completed the initial installation and configuration of Codar and can begin familiarizing yourself with the capabilities of Codar.

Launch the Codar Console (type the following URL in a supported Web browser: `https://<codar_hostname>:8444/csa`) and log in using the out-of-the-box user (`admin`) and password (`cloud`).

See the following sections for post-installation options:

- "Install VMware vCenter" below
- "Install SiteScope" on page 67
- "Install Server Automation" on page 69
- "Configure resource providers" on page 77
- "Apply Codar licenses" on page 78
- "Jenkins" on page 79
- "Import and configure sample designs" on page 86

Install VMware vCenter

Install vCenter according to the manufacturer's recommendations. For example, follow the VMware best practices for managing individual ESX servers from a vCenter instance. You can find the VMware documentation at http://www.vmware.com/support/pubs/.

You must have a vCenter instance that can support the flows that actuate vSphere VMs. See *Codar System and Software Support Matrix* for version requirements.

Both the *Codar Console Help*, which is available in a printable PDF format, and the *Codar System and Software Support Matrix* are available on the HPE Software Support website at https://softwaresupport.hpe.com (this site requires HPE Passport ID). Select **Dashboards > Manuals**

Configure VMware vCenter

Configure VMware vCenter by installing prepared templates. In the vSphere environment, a template is a master copy of a virtual machine that can be used to create many clones. A clone is a copy of a virtual machine.

You can learn more about creating templates and working with clones in vSphere by referring to VMware's *vSphere Virtual Machine Administration Guide for vCenter Server* (EN-000312-02), available in the VMware documentation. You can find the VMware documentation at http://www.vmware.com/support/pubs/.

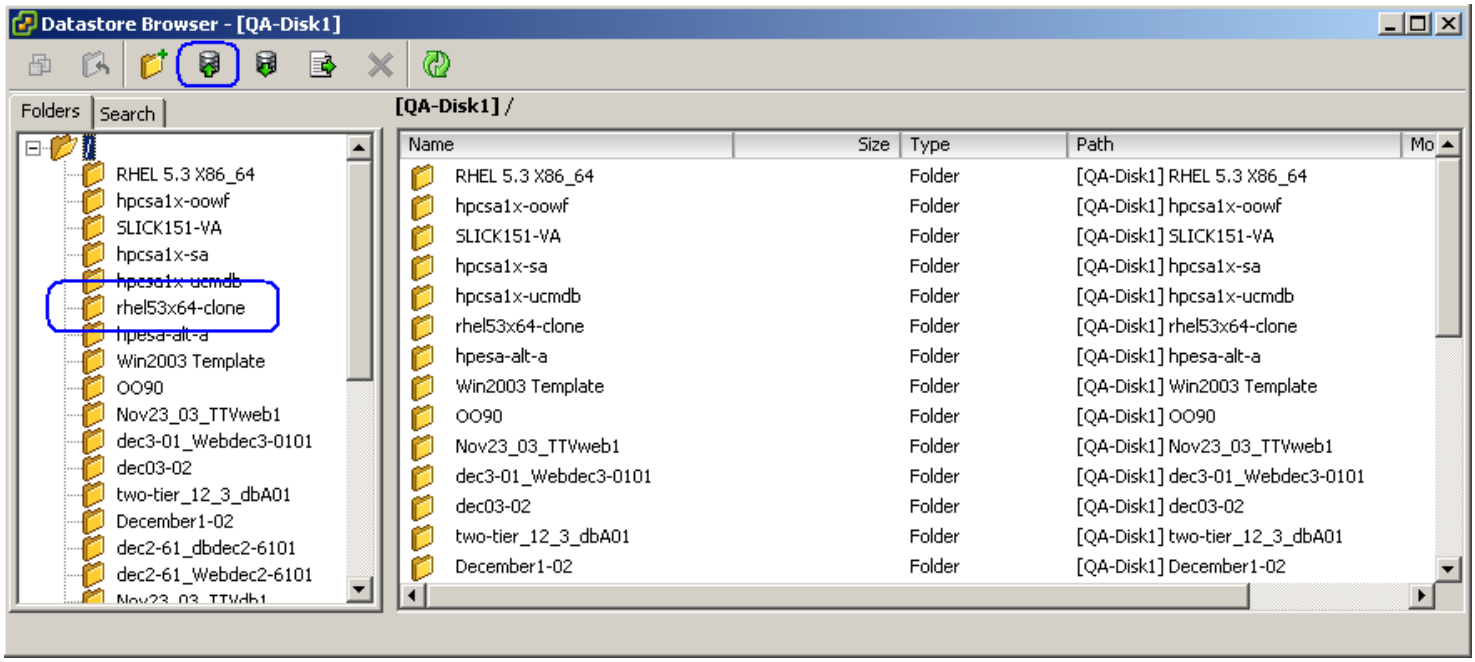
Virtual machines created by the Codar solution are created based on virtual machine templates. To allow applications (such as Apache) to be deployed to the image, you must create a template that includes HPE Server Automation Agent software. See *Prepare a VMware Template to Self-Register with Server Automation* for more information.

To install a prepared template, do the following:

1. Locate a prepared template.
2. Copy the template folder to the system containing the vSphere client software.
3. From your vSphere client software menu, select **View** > **Inventory** > **Datastores** to see a list of available datastores on your vCenter server.
4. Right-click one of the available datastores and select **Browse Datastore** to see the directory structure of that datastore.
5. Copy the template folder to the datastore by clicking on the **Upload files to this datastore** button.

   The following image shows the Datastore Browser window with **Upload files to this datastore** highlighted. It also shows a

`rhel53x64-clone` folder that was uploaded to this datastore:



Consult the vSphere documentation for additional details. You can find the VMware documentation at http://www.vmware.com/support/pubs/.

Install HPE Helion Development Platform

Helion Development Platform (HDP) is a PaaS service that is successfully integrated with Codar using the HDP content pack. Codar is integrated with the HDP service and application components.

Codar supports only those HDP clients that run on Red Hat Enterprise Linux and Ubuntu operation systems.

Install Helion Development Platform (HDP) according to the instructions at http://docs.hpcloud.com. Ensure that the latest version of GitHub is installed on the client system.

Configure HDP

The following tasks are required to configure the HDP client.

Modify the proxy settings

If the HDP server and client are not in the same network, then you need to change the following proxy settings in the `.bashrc` file. This file is located in the HDP client system.

- `PATH=$PATH:$HOME/bin:/etc/helion-client`

  where, `/etc/helion-client` is the path in which HDP client is installed.
- `export PATH`
- `export http_proxy=http://<proxyHost>:<proxyPort>`
- `export https_proxy=http://<proxyHost>:<proxyPort>`
- `export no_proxy=localhost,127.0.0.1`

Modify system properties in Operations Orchestration Central

The HDP content pack is installed as a part of the Codar installer if you installed the HP Codar content capsule during the Codar installation.

To update system properties:

1. Log in to Operations Orchestration Central.
2. Click the **Content Management** button.
3. Select **Configuration Items** > **System Properties**.
4. Select the system properties and click the **Edit** icon.
5. Update the `HDP_Client_Profile` and `HDP_Application_Timeout` properties as follows:
   - `HDP_Client_Profile = . ~/.bashrc` (for Red Hat Enterprise Linux systems)
   - `HDP_Client_Profile = . ~/.profile` (for Ubuntu systems)
   - `HDP_Application_Timeout` : The default value set for this property is 30 minutes. You can reconfigure this property with the required timeout value. For example, you can set the HDP application start timeout to 30m, 1h, or 1d where m indicates minutes, h indicates hours, and d indicates days.

Set HDP provider properties in Codar

The HDP provider is visible in Codar as **HPE Helion Development Platform**. You must configure the properties of this provider.

1. Navigate to **Providers** > **HPE Helion Development Platform**.
2. Click the **Components** tab.
3. Select the application for which you want to configure the properties and click the **Properties** tab.
4. Configure the following properties by selecting the gear icon and clicking **Edit Component**.

Property	Description
clientHost	IP address of the HDP client that accesses the HDP server
clientPassword	Password of the HDP client
clientPrivateKey	SSH private key of the HDP client. Set either the clientPassword or the clientPrivateKey, but not both.
clientUser	Name of the HDP client system

Install SiteScope

Install SiteScope to the correct version and patch level. See *Codar System and Software Support Matrix* for version requirements.

Installation notes:

- Do not install SiteScope on the Operations Orchestration server. It must be on its own server.
- Calculate the resources needed for the SiteScope server using the information in the SiteScope documentation. This calculation should include the number of target servers that you expect Codar to monitor.
- During installation, you can change the port for the SiteScope service to avoid potential conflicts with other web servers that use the default port value of 8080. Select any available port on the system and keep track of the port number that you select.

Configure SiteScope

The following tasks are required to configure SiteScope to integrate successfully with Codar:

- "Enable Codar to configure SiteScope monitors" below
- "Manually import additional Codar templates" below
- "Configure Codar credential profiles" on the next page
- "Configure SiteScope administrator credentials" on the next page

Enable Codar to configure SiteScope monitors

SiteScope is installed with a default of secured API calls required for configuring monitors. Codar does not support secured API calls; therefore, you must change this setting. To re-configure SiteScope so it does not use secure APIs, you must make the following change to the configuration:

1. Stop the SiteScope service by typing the following command in a console window:

   ```
   net stop SiteScope
   ```

2. Open the SiteScope `<sitescopeInstallDir>\groups\master.config` file in a text editor.
3. Change the `_accessControlled=true` property value to `_accessControlled=false`.
4. Restart the SiteScope service by typing the following command in a console window:

   ```
   net start SiteScope
   ```

Manually import additional Codar templates

Two additional Codar templates, `CSA templates Silver` and `CSA templates Gold`, must be manually imported. These templates are used by the `CSA_BP_VCENTER_COMPUTE_SITESCOPE_MODIFY_v3.20.00.zip` service design.

1. Log in to the SiteScope Dashboard.

   > **Note:** You must be able to access files in the `CODAR_HOME\CSAKit-4.5\Lib\sitescope` directory from the SiteScope Dashboard. If necessary, copy this directory to the system from which you are launching the SiteScope Dashboard.

2. Select the **Templates** context.
3. In the template tree, right-click **SiteScope** and select **Import**.
4. Browse to `CSA_HOME\CSAKit-4.5\Lib\sitescope` (or the directory to which this directory was copied) and import `CSA templates Silver.tmpl`.
5. Repeat steps 3 and 4, but import `CSA templates Gold.tmpl`.

Configure Codar credential profiles

Configure the credentials used to log in to every Windows system and every Linux system monitored by SiteScope. The credentials to all Windows systems must be the same. Likewise, the credentials to all Linux systems must be the same.

1. Log in to the SiteScope Dashboard.
2. Select **Preferences** context > **Credential Preferences**.
3. Edit the **LINUX-CSA-TARGETS** credential profile and supply login credentials for your Linux environment.
4. Edit the **WINDOWS-CSA-TARGETS** credential profile and supply login credentials for your Windows environment.

Configure SiteScope administrator credentials

Configure the credentials used to log in as the administrator of SiteScope. These credentials are used by Codar when configuring SiteScope resource providers from the Codar Console.

1. Log in to the SiteScope Dashboard.
2. Select **Preferences** context > **User Management Preferences**.
3. Right-click **SiteScope Administrator** and select **Edit User**.
4. If not already specified, enter a login name and password for the SiteScope administrator.

Install Server Automation

Install Server Automation to the correct version and patch level. See *Codar System and Software Support Matrix* for version requirements.

You can determine your version and patch level by using the Server Automation Client and selecting **Help** > **About**.

Installation notes:

- You can use the DHCP services included with Server Automation. For information on configuring a DHCP server with Server Automation, see *Server Automation Simple/Advanced Installation Guide*.
- The Server Automation Client should be installed on the Operations Orchestration server.

- The Server Automation Client does not register right away after installation. A delay occurs before you can continue with configuration.

Configure Server Automation

The following tasks are required to configure Server Automation to allow read and write access to the required areas:

- "Create Codar service account" below
- "Create Codar administrators group and assign permissions" on the next page
- "Validate Codar service account" on page 72
- "Validate Server Automation client" on page 72

Create Codar service account

1. Open the Server Automation Web Client in a browser.
2. Log in using the Server Automation Administrator user name and password (created when the Server Automation server was installed).
3. Click **Administration** > **Users & Groups**.
4. Click **New User** in the Users tab toolbar and complete the following fields using the values listed in the following table:

Field Name	Value
Last Name	Service Account
First Name	CSA
Full Name	CSA Service Account
Email Address	*<your email address>*
User Name	hpcsa
Password	*<password>*

5. Select **Superusers** from the Group Membership list to enable this option.
6. Click **Save**.
7. Click **Log Out**.

Create Codar administrators group and assign permissions

1. Open the Server Automation Web Client in a browser.
2. Log in using the Server Automation Administrator user name and password.
3. Click **Administration** > **Users & Groups**.
4. Select the **Groups** tab.
5. Click **New Group** and complete the following fields using the values listed in the following table:

Field Name	Value
Group Name	hpcsa-admin
Group Description	HPCSA Administrators
Not Assigned	Read & Write
Opsware	Read

6. Click **Save**.
7. Select **hpsca-admin** in the list of groups.
8. Select the **Users** tab and add the **admin** and **hpcsa** users to the hpcsa-admin group.
9. Click **Save**.
10. Select the **Facilities** tab and select **Read & Write** to the appropriate facility.

    If only one facility exists, select **Read & Write** for it.
11. Click **Save**.
12. Select the **Features** tab and click **Select All** in the header row to select all features.
13. Click **Save**.
14. Select the **Client Features** tab and change all values to **Read & Write** and **Yes** where applicable.
15. Click **Save**.
16. Select the **Other** tab and select all options *except* **Generate Security Reports**.
17. Click **Save**.
18. Select the **OGFS Permissions** tab, click **Add Permissions**, and enter the following permissions:

- **Features**: Select **Run Command on Server**.
- **Servers**: Click the **Customers** option and select **Not Assigned** from the list.
- **Login Names**: Select **Opsware user name**, and select **Log in as** and enter `root`.

19. Click **Grant**.
20. Click **Add Permissions** and enter the following permissions:
    - **Features**: Select **Launch Global Shell**.
21. Click **Grant**.
22. Click **Log Out**.

Validate Codar service account

1. Open the Server Automation Web Client in a browser and verify that the login screen appears.
2. Log in using the Codar Service Account credentials you created in the previous steps.
3. Verify that the Server Automation Web Client home page is displayed. A list of tasks and jobs is shown.
4. Click the **Managed Servers** option on the left side of the screen and verify that a list of servers with their IP addresses and operating system information is displayed.
5. Click **Log Out** and close the Web browser.

Validate Server Automation client

1. Connect to the system where Operations Orchestration is installed.
2. Verify that the client is installed.
    - If an icon appears on the desktop labeled Server Automation Client or a link appears in the Start Menu, the client is installed. Continue to step 3.
    - If neither the icon nor the Start Menu link appear, then you need to install the client by performing the following steps:
        i. Open the Server Automation Web Client in a browser and select **Download Opsware Launcher** at the login screen.
        ii. Install the client using the default parameters.

    You must have a JRE installed in order to use the Opsware Launcher on a Windows system.

3. Launch the client with the following credentials:
   - **Username**: hpcsa
   - **Password**: <hpcsa password>
   - **Core Server**: <SA Server Host Name>

   The above login information may vary depending on your installation.
4. Verify that the Server Automation application starts and Device Groups appear in the left hand navigation pane.
5. Click **All Managed Servers** and verify that a list of servers with their names, IP addresses, and operating system information is displayed.
6. Exit the client.

Prepare VMware template

The steps below prepare a VMware template to self-register with Server Automation.

Virtual machines (VMs) created by the Codar solution are created based on virtual machine templates. The Codar flows reference a vSphere template name, and perform a clone operation to provision new virtual machines. These templates would generally provide an operating system image only, with no application software installed.

To allow applications (such as Apache) to be deployed to the image, you must install and configure Server Automation and create a template that includes the Server Automation Agent software. That is, in order to manage the virtual server and to install application software, the clones are configured to self-register upon power-on with an Server Automation system. Once registered as a managed server, software policies are applied to the server in order to install and configure the correct applications. See the *Server Automation Policy Setter Guide* and the *Server Automation Application Deployment User Guide* in the Server Automation documentation for more information on managing servers and configuring software policies.

- "Template preparation overview" on the next page
- "Detailed process" on the next page
- "Provision an operating system on a virtual machine" on page 75
- "Sanitize agent configuration on a template machine" on page 75
- "Basic customization" on page 77
- "Install prepared template" on page 77

Template preparation overview

For cloned virtual machines to register with the Server Automation system upon power-on, prepare a template with an Server Automation agent. The following is a general outline of the steps to be performed:

- First, create a virtual machine with the appropriate operating system image that you would like to template. Provision the VM with an operating system through any method supported by vSphere:
  - Manually install the operating system on a prepared, configured VM.
  - Provision the operating system through a network boot operation from the Server Automation system.

  See the appropriate vSphere documentation to create a new virtual machine with an installed operating system image.
- When preparing a virtual machine as a template to be used to clone many new virtual machines, leave the configuration as generic as possible. No hostname can be configured, and the network configuration can be obtained via DHCP.
- Install and test the appropriate VMware Tools on the virtual machine.
- Install the Server Automation agent. The agent registers the template with the Server Automation system so that this machine is in a Managed state for the next step.
- An APX utility in the Server Automation system library is run to prepare the agent on the virtual machine to re-install and register with the Server Automation system on the next bootup.
- The virtual machine is shut down and converted to a template.
- Delete the virtual machine server record from the Server Automation system.

Detailed process

See the vSphere documentation set for detailed information on the creation, configuration, and operating system installation for a new virtual machine. There are several options to install an operating system onto a new virtual machine. One of the options available is to use the PXE network boot facility from the Server Automation server, with an operating system installation profile that integrates the installation of an Server Automation agent. A virtual machine which is provisioned using this method starts the agent upon bootup, and attempts to register it with the Server Automation system.

If you use another method to provision an operating system on the virtual machine, the Server Automation agent can be installed from the Server Automation system. See the product documentation for an expanded discussion of this process. The following instructions describe one method.

Provision an operating system on a virtual machine

1. Boot the virtual machine and make sure that it is connected to the network. Verify that the Server Automation (SA) system can be reached.
2. Discover the virtual machine in the **Unmanaged Servers** (SA 9.x) or **SA Agent Installation** (SA 10.x) window in Server Automation. You can scan an entire subnet or enter the IP address for the virtual machine and initiate a scan to discover it.
3. Select the virtual machine, right-click, and then select **Manage Server** (SA 9.x) or **Install SA Agent** SA 10.x). A new dialog opens.
4. Provide the appropriate login credentials, and select the action to verify prerequisites, copy installer, and install the agent. Set any desired Installer Options at this time, referring to the Server Automation documentation for details.
5. Click **OK**.

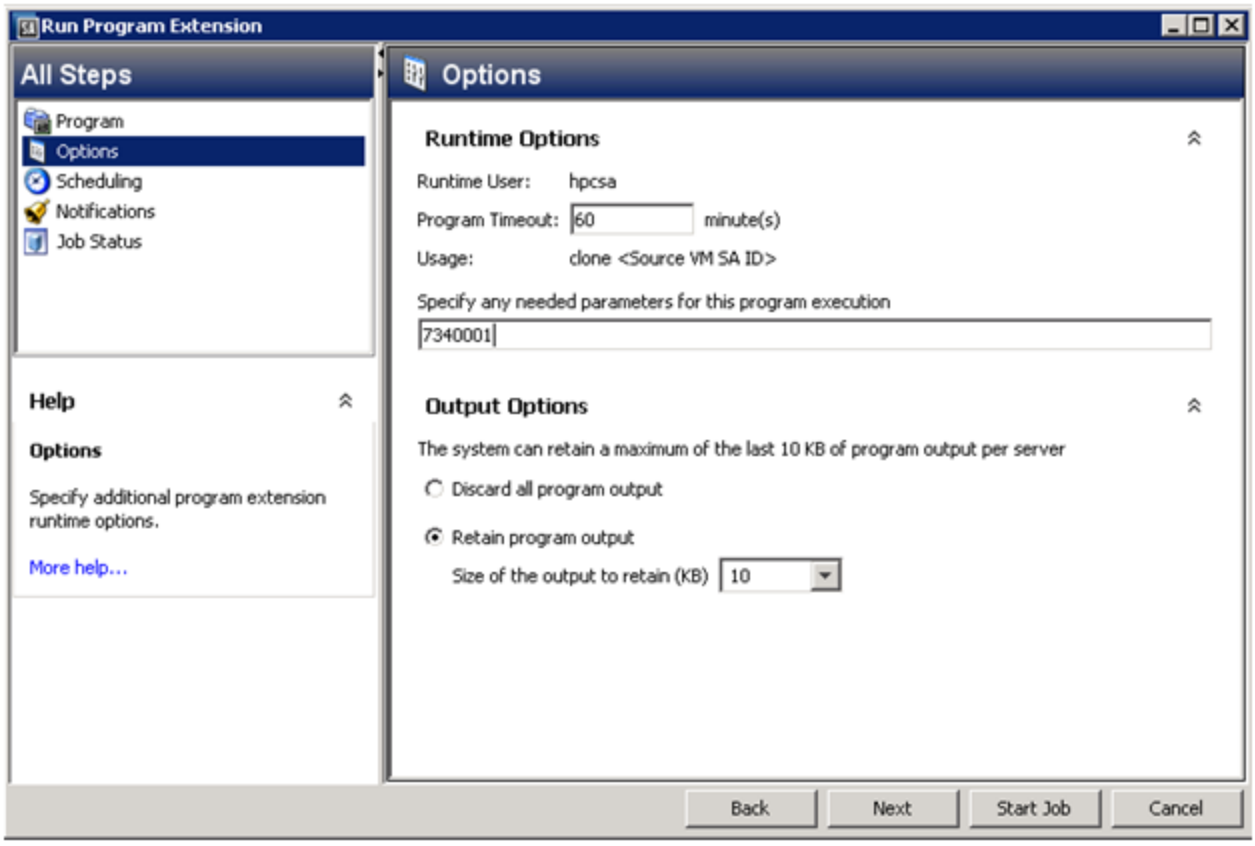
   When the installation process completes successfully, the agent is installed, and the virtual machine is visible in the **All Managed Servers** tab. The hostname has not been set, as we plan to convert this virtual machine to a generic template. So, the default host name is used for the virtual machine.
6. From the **Server Information Properties** tab, select the virtual machine and press **Enter**.
7. Select **Properties**.
8. Record the **Object ID** of the virtual machine, which can be found in the Management Information section of the Properties panel.

Sanitize agent configuration on a template machine

The agent on our virtual machine template must be prepared to install and register a new machine server with Server Automation each time we create a new clone. To prepare the agent we must sanitize the agent configuration on our template machine by doing the following:

1. Switch to the **Library** tab in the Server Automation client.
2. Expand the **Extensions** folder.
3. Select **Program**.
4. Locate the **BRDC HPSA agent sanitizer** Automation Platform Extension (APX).
5. Execute the BRDC HPSA agent sanitizer APX:
   a. Right-click the APX and select **Run**.
   b. Select the **Options** tab in the Run Program Extensions dialog.
   c. In the **Specify any needed parameters for this program execution** field, enter the **Object ID**, which you previously

obtained for the virtual server template:



d. Click **Start Job**.

e. Shut down the virtual machine after the job completes successfully and the agent has been prepared.

   Do not reboot this virtual machine again until after it has been converted to a vSphere template.

f. Using the vSphere client, convert this virtual machine to a template.

g. The last step is to clean up the server records for the virtual machine template from Server Automation. In the All Managed Servers tab:

   i. Deactivate the server.

   ii. Delete the server.

The template is now ready to use to clone new virtual machines. Codar uses a simple customization template that sets the hostname equal to the VM name. Additional customization is possible during the clone operation. See "Basic customization" on the next page.

When a newly cloned virtual machine powers up, the Server Automation Agent installs and then contacts the Server Automation system to self-register. Shortly after power on, you can refresh the All Managed Servers view in the Server Automation client to locate the new virtual machine record.

Basic customization

Perform the following basic customizations:

1. On the vCenter environment click **View** > **Management** > **Customization Specifications Manager**.
2. Click the **New** icon.
3. Select Windows or Linux for your Target Virtual Machine OS. You can create one of each.
4. If you are creating a Windows target, name it `useVmName_Windows`. If you are creating a UNIX target, name it `useVmName_Linux`.
5. Customize as appropriate, noting two important items:
   - On the screen with the NetBIOS Name you must choose **Use the virtual machine name**.
   - If the virtual machine name exceeds 15 characters, it will be truncated.

Install prepared template

The template must be installed on the system containing the vSphere client software. See *Configure VMware vCenter* for more information.

Consult the vSphere documentation for additional details. You can find the VMware documentation at http://www.vmware.com/support/pubs/.

Configure resource providers

HPE recommends that you follow this procedure to create two resource providers. These resource providers should be associated with two different data centers which are associated with two different environments, likely named Development and Testing.

To configure a resource provider,

1. Open Codar at https://<*ipadress*>:<port>/csa

   where <*ipadress*> is the IP address or host name of the Codar server, and <port> is the port number, which is 8444 by default.
2. Log in as the administrator. The default user name is **admin** and the default password is **cloud**.
3. Click the Providers tile.
4. Under All Providers on the left, select the provider type that will be used for application deployment.

5. Click **Create** and enter details for the resource provider you will use for application deployment.
6. After the provider has been created, select the Properties tab and provide the values for the properties that are defined for the provider type.

   For example, if the provider chosen is the vCenter provider, you might create a property named **DATACENTERNAME** with the value **DEVELOPMENT**.
7. Return to the main Providers screen and choose **By Environment** in the drop-down field in the upper right corner of the screen.
8. Click **Create your first Resource Environment.**
9. Enter details for the resource environment.

   The resource environment you enter here should be the same as the Environment you entered in "Install Codar Jenkins plug-in" on page 81.
10. Click **Select Resource Providers**.
11. Add the provider you created and then click **Save**.

Apply Codar licenses

After installation is complete, apply a Codar permanent license. You can then apply an HPE Cloud Service Automation permanent license, if desired. After the Cloud Service Automation license is installed, you can use all of Codar and Cloud Service Automation features.

The following license types are available:

- Codar permanent license only.
- Cloud Service Automation permanent license only.

If you install Cloud Service Automation, then you must add a Cloud Service Automation license first. If you install Codar, then you must install a Codar license first. After you apply a base license, you can add an upgrade license. If you have licenses for both, you can apply a Cloud Service Automation and a Codar license.

When upgrading, if a Cloud Service Automation license is applied to Codar, or the Codar license is applied to Cloud Service Automation, the upgraded product is always Cloud Service Automation. For details, see "Appendix A: Cross-product upgrade between Codar and Cloud Service Automation" in the *Codar Upgrade Guide*.

OSI capacity

The number of operating systems you can use in active applications or subscriptions is known as the OSI capacity. If you have Cloud Service Automation and Codar licenses, then the OSI capacity is the lowest of the two. Here's an example: You have a Cloud Service Automation license with 100 OSI and a Codar license with 50 OSI, so your OSI capacity is 50.

Jenkins

Jenkins is optional, but you must install Jenkins and dependencies if you intend to use the sample design, and it is required for the Sample Continuous Deployment Demo purpose.

You should consult product documentation for installation and usage instructions.

Using Jenkins with Codar requires the following dependencies:

- Collabnet Subversion Edge: collab.net/support/documentation
- TortoiseSVN: tortoisesvn.net/support.html
- Jenkins: jenkins-ci.org/
- JDK 8
- Maven: maven.apache.org/guides/index.html

Install Collabnet Subversion Edge

Download and install a version appropriate to your system from collab.net/downloads/subversion.

Install Tortoise

Download and install the latest version from tortoisesvn.net. Use the default settings.

After installation, you will see new options when you right-click a file or folder in Windows Explorer.

Install Jenkins

Download the Windows installer for Jenkins from jenkins-ci.org.

After installation, you should access the Jenkins server at http://localhost:8080 to validate the installation.

Install the JDK

Install the JDK version 8 on the Jenkins server.

If you already have the JDK version 7 installed on the Jenkins server and do not want to upgrade, you must enable the 'TLSv1.2' protocol using the 'https.protocols' parameter. For more information, refer to **Diagnosing TLS, SSL, and HTTPS** (diagnosing_tls_ssl_and_https).

Install the Maven plug-in

Download and install Maven from maven.apache.org.

Configure Jenkins to use with Codar

The following steps are for Jenkins version 1.583.

To configure Jenkins to use with Codar, complete the following steps:

1. Make sure the JDK and Maven are installed.
2. Log in to the Jenkins Dashboard in a browser at `http://<host>:<port>/`, substituting the host and port information appropriate for your Jenkins environment.
3. Click **Manage Jenkins**.
4. Click **Configure System**.
5. In the JDK section, click **Add JDK**.
6. Enter the name and path for `JAVA_HOME`.

7. Deselect **Install automatically**.
8. In the Maven section, click **Add Maven**.
9. Enter the name and path for `MAVEN_HOME`.
10. Deselect **Install automatically**.
11. Enter the value for `MAVEN_OPTS`.
12. Click **Save**.

Install Codar Jenkins plug-in

To install the Codar Jenkins plug-in, complete the following steps:

1. Log in to the Jenkins Dashboard in a browser at `http://<host>:<port>/`, substituting the host and port information appropriate for your Jenkins environment.
2. Click **Manage Jenkins** from the Dashboard
3. Click the **Manage plug-ins**.
4. Select the **Advanced** tab.
5. In the **Upload plug-in** section, browse to select the following file:

   C:\Program Files\HPE\Codar`\CSAKit-4.5\Content Archives\topology\Jenkins plugin\HP_Codar.hpi`
6. Click **Upload**.
7. Select the Installed tab and verify that the Codar plug-in was installed.

Enable the Codarr Jenkins plug-in

To enable the Codar Jenkins plug-in, complete the following steps:

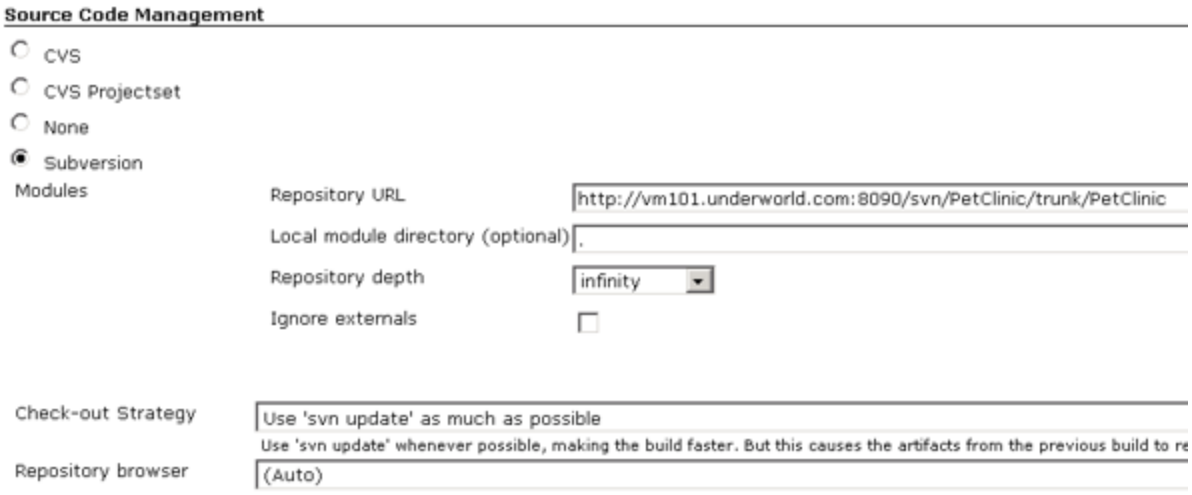
1. Click **Manage Jenkins** from the Dashboard.
2. Click **Configure System**.
3. Scroll down to the Codar Plug-in section of the **Configure System** page and select the **Enable** check box.
4. Click **Save**.

Configure Pet Clinic sample application project

Codar includes a Pet Clinic sample application project, which is available on HPE Live Network (HPE LN) at https://hpln.hpe.com/group/project-codar.

To configure the Pet Clinic sample application project, complete the following steps:

1. Check in the source code for the PetClinic project into the Subversion server.
2. Create a new PetClinic project in the Jenkins server using the **Build a maven2/3 project** option.
3. Click the **PetClinic** link on the Jenkins Dashboard, and then click the **Configure** link on the page that opens.
4. Configure Subversion for Source Code Management for the PetClinic project by choosing the **Subversion Modules** option and adding the Subversion PetClinic source code URL in the Repository URL field.
5. After saving, update the Subversion credentials like this:

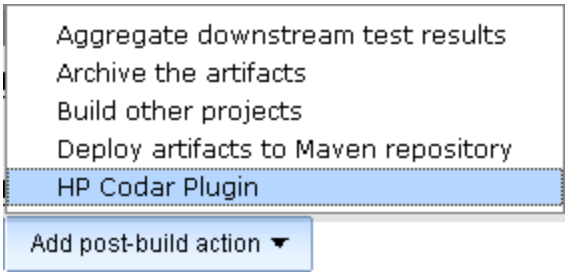


6. Configure Jenkins to automatically trigger a build if any code is checked-in by selecting the **Poll SCM** check box and adding ***/5 * * * *** as the schedule.
7. Scroll down and click **Add post-build action**, select **Archive the artifacts**, and then enter `*/*.war, target/classes/*/*.sh` in the **Files to archive** text box.

Configure plug-in for Pet Clinic sample application

To configure the plug-in for the Pet Clinic projects, complete the following steps:

1. Click the **PetClinic** link on the Jenkins Dashboard, and then click the **Configure** link on the page that appears.
2. Click **Add post build action** and select **HP Codar plug-in**.



3. Enter the applicable Codar plug-in properties:
   - **HostName** – The host name or IP address of the server on which Codar is installed.
   - **Port** – The port number on which the Codar application is listening.
   - **Username** – The name of a user that has Codar administrative privileges.
   - **Password** – The password for the Codar user.

     > **Caution:** Do not use the default Codar admin user because this might be a security issue. After installing Codar and configuring LDAP, add a user to the Application Architect role. Use the credentials for that user here.

   - **Application Design Location** – The relative path and filename from the source repository URL of the application design `JSON` file, which contains the application to be deployed by Codar (for example, `designs\PetClinicApp.json`). See "API calls" in the *Codar API and CLI Reference Guide* for information on how to get the `JSON` file using REST APIs.
   - **Environment** – The environment in Codar in which the provider that is to be used for deployment is contained.

     > **Note:** The environment value is mandatory if you want to use Codar for continuous deployment.

   - **Package properties** – Specify the component properties of the design that will be parameterized within the build. The input to this field should be specified in this format:

     ```
     component1id:property1id:property1value,component2id:property2id:property2value,
     component3id:property3id:property3value
     ```

     - **Component Id/Name**– The ID of the component in the application design. This can be obtained from the Application design's `json` file. A PetClinic application component could be : `PetClinic_Application__VERSION__1__GROUPID__com.hp.csa.type0001`.
     - **Property Name** – The name of the property within the component. This can be obtained from the Application design's `json` file. For example, an `artifacturl` property within the PetClinic application could be : `artifacturl_a36`.

- **Property Value** – The value of the property. If it is a Jenkins build output artifact, then the URL of the artifact will be automatically computed and the value will represent the complete HTTP URL from which this artifact can be downloaded. For example, the Jenkins build artifact for PetClinic could be : `petclinic.war`.
- For example: `PetClinic_Application__VERSION__1__GROUPID__com.hp.csa.type0001:artifacturl_a36:petclinic.war`

- **Extended Properties File** – Optionally enter the name of the properties file. This properties file needs to be specified only when the user wants to specify a different CI process than what is provided by default. This properties file can specify a different Operations Orchestration flow containing necessary CI logic. You can specify a different flow ID by creating a property file with **key** as the `uuid` and **value** as the uuid of Operations Orchestration flow. For example, `uuid=asdaasdasdsdasdad99f`.

  You can also specify the required properties to this flow as key value pairs in this property file.

- **NodeId** – Enter the component ID for which you want to extract component properties. These component ids can be obtained from the Application design `JSON` file which has been exported. Multiple components are specified by separating those with commas.

  For example, you may want to retrieve an IP address and host name of the VCenter component, `VcenterServerType__VERSION__04.20.0000__GROUPID__com.hp.csa.type0002`, to run tests on the provisioned server.

- **Httpusername** – Enter the user name for accessing artifacts from HTTP location. For example, the username for the Jenkins Server.
- **HttpPassword** – Enter the password for accessing artifacts from HTTP location. For example, the password of the Jenkins Server.
- **SSLCertificatePath** – Enter the SSL certificate path for Codar and pick up the certificate from the Codar setup. The certificate will be in the machine where Codar is installed in the path C:\Program Files\HPE\Codar`\IA-openjre\lib\security\cacerts`.
- **CertificatePassword** – Enter the SSL certificate keystore password for Codar. By default it is **changeit**.

Sample Pet Clinic extended properties file

Change the extended properties file to the following

```
## Properties accessed by the ARA API to invoke OO flows.

##This properties file contains the oo flow id(uuid) as well as the relevant parameters to be passed to the oo flow.

##Dynamic properties can be specified by <<property>> prefixing and suffixing with angular brackets. These properties
```

```
## will be substituted with the value passed in JSON input.

csaTruststore=C:/codar/cacerts

#uuid of the oo flow. This flow contains the necessary logic for the Continuous integration process.

#uuid=377898bc-d92e-4e6a-b542-718539fdcb9a

#Specify the artifacts that are built by Jenkins to manage it within ARA. These artifacts would be
dynamically obtained from Jenkins and deployed via ARA.

##Format is
component1id:property1id:property1value,component1id:property2id:property2value,component2id:property3id:
property3value where

##where COMPONENT1id - represents the id of the component as displayed in the design

## property1id - represents the property of the component which needs to be dynamically replaced

##property1value - will represent the artifacts which need to be deployed.

##Sample

##Pet_Clinic_DB_Configuration_87424824_fdfd_485d_b392_7e5b58cadb1a_320fb4ee61694fd9a4ea347537d08fcb__
VERSION__1__GROUPID__com.hp.csa.type.VMWARE_VCENTER0001:artifacturl:petclinic.war

#The server node which needs to be queried for obtaining IP address. This is relevant for Continuous
Delivery where tests can be run against the provisioned virtual machine via ip address.

#serverNodeId=VcenterServerType__VERSION__04.10.00000002

#componentid:propertyname:jenkinsout,componentid:propertyname:jenkinsout
```

Create custom design

You can configure continuous deployment for custom applications by creating custom Operations Orchestration flows.

If a custom application in an enterprise needs continuous deployment users can create deployment scripts using Chef or Operations Orchestration. Those flows can be embraced (imported) as components in Codar and used in the creation of an application design, which can then be exported from Codar in JSON format and checked into the source repository. Jenkins can be configured for a continuous build. When an application developer checks in the code, a Jenkins build is triggered and the application is deployed using an application model on a specific environment.

Import and configure sample designs

Sample application designs are installed with Codar Console.

These designs are imported to the Codar Console 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*.

Import sample designs

Complete the following steps to import any other sample designs manually:

1. Click the **Designs** tile in the Codar Console to go to the main Topology Designs screen.
2. Click **Import**.
3. Select a sample application zip file and click **Import**.
4. Repeat these steps to import the other sample design zip files.

The topology designs for these applications should now be listed under All Designs in the main Topology Designs screen.

Configure sample designs

Imported sample Codar Console designs can be configured using the instructions provided in the *Cloud Service Automation Content Pack User Guide*.

The sample designs can be validated by deploying the designs using the Test run functionality.

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 Installation and Configuration Guide (Codar 1.70)

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!