Cloud Service Automation

Software Version: 4.80

For Microsoft Windows and Linux operating systems

Installation Guide

Document Release Date: January 2017
Software Release Date: January 2017

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

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

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 HPE 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 HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

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 HPE 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.

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

Contents

Installation Overview 5
CSA Prerequisites 6
Configure a CSA Group and User for Linux (Required) 7
Install and Configure a Database 8
Install Oracle Database and JDBC Drivers 8
Install the Oracle Database (Required) 8
Configure multi-language support (Optional) 8
Download Oracle JDBC Drivers (Required) 9
Configure Oracle 9
Create Database Users for CSA 9
Create a Tablespace for LOBs (Recommended) 11
Install Microsoft SQL Server 13
Configure Microsoft SQL Server 13
Enable TCP/IP (Required) 13
Configure a Microsoft SQL Server User for CSA (Required) 14
Create a Filegroup for LOBs 16
Install PostgreSQL 19
Configure PostgreSQL 19
Configure PostgreSQL Users and Database (Required) 19
Install and Configure Cloud Service Automation 21
Install Operations Orchestration 22
Configure an Internal User (Required) 22
Export Operations Orchestration's Root Certificate (Required) 23
Install Cloud Service Automation for Windows 25
Install Cloud Service Automation for Linux 38
Install Cloud Service Automation with Remote MPP for Windows 51
Install Cloud Service Automation with Remote MPP for Linux 54
Install and Configure Remote Console Service 58
Installation through the Install Script 58
Configure SSL for Remote Console Service 62
Configure Remote Console Service in CSA 66

Modify Remote Console Service default configurations 67
Modify Marketplace Portal default configuration for remote console service 69
Post Install Configuration 71
Enable RDP (Mandatory for Connect RDP option) 71
Uninstall Remote Console Service 71
Secure the Marketplace Portal 73
Update and Redeploy the Service Manager Base Content Pack 74
What's next? 77
Global Search 77
Install a new Operations Orchestration license 77
Configure CSA 78
Checksum-checker Tool 79
Before Running the Checksum-checker Tool 79
Using Checksum-checker 79
Appendix A: Install an Instance of the Marketplace Portal on a Remote System 81
Copy the CSA Certificate 81
Install CSA for MPP for Windows 82
Install CSA for MPP for Linux 82
Secure the Marketplace Portal 82
Update the Marketplace Portal in the Cloud Service Management Console 83
Launch the Marketplace Portal 84
Start, Stop, or Restart the Marketplace Portal on the Remote System 86
Send documentation feedback 87

Installation Overview

Installing the Cloud Service Automation (CSA) application and successful implementation of the application requires knowledge of the integrated products, as well as the CSA solution. Information provided here augments information provided in the integrated products documentation but is not intended to replace that documentation. Primary product documentation contains the most up-to-date information. Cross references are provided to those documents where appropriate.

For information about how these parts fit together, see the Cloud Service Automation Concepts Guide.

You should review the *Cloud Service Automation System and Software Support Matrix* Guide for version requirements.

Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

In order to install CSA, perform the following steps. It is recommended that you perform each step in the following order:

1. Configure a group and user.

   > **NOTE** Only Linux users need to configure a group and user.

2. Install and configure one of the following databases:
   a. "Install Microsoft SQL Server" on page 13
   b. "Install Oracle Database and JDBC Drivers" on page 8
   c. "Install PostgreSQL" on page 19
3. Install Operations Orchestration.

   > **NOTE:** Install Operations Orchestration only in case you are not using embedded OO which comes with CSA.

4. Install Cloud Service Automation:
   a. Install CSA for Windows
   b. Install CSA for Linux
   c. Install CSA with Remote MPP
5. Secure the Marketplace Portal.
6. Update and redeploy the Service Manager Base Content Pack.

7. What's next?
8. "Appendix A: Install an Instance of the Marketplace Portal on a Remote System" on page 81

CSA Prerequisites

> **Important Note** Individual platform, database, middleware, and integrations may vary widely for individual CSA installations.

Prior to any CSA installation, it is important to review the *Cloud Service Automation System and Software Support Matrix* Guide for a complete list of :

- Supported database versions.
- Supported platforms.
- Middleware options.
- Recommended integrations.

Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

Configure a CSA Group and User for Linux (Required)

Configure a group and user for CSA:

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

   ```
   groupadd csagrp
   ```

3. Create a user called csauser and assign this user to the csagrp. Enter the following:

   RHEL: `useradd -g csagrp -m csauser -s /bin/bash`

4. Assign a password to the CSA user. Enter the following:

   ```
   passwd csauser
   ```

   When prompted, enter the password.

Install and Configure a Database

During this step you install a database instance to be used as the primary data-source for CSA. Oracle, MS SQL Server, and PostgreSQL are the available options for installation.

1. "Install Oracle Database and JDBC Drivers" below
2. "Install Microsoft SQL Server" on page 13
3. "Install PostgreSQL" on page 19

Install Oracle Database and JDBC Drivers

Installing the Oracle database for CSA involves the following steps:

1. Install the Oracle Database
2. Download the Oracle JDBC Drivers
3. Configure Oracle

Install the Oracle Database (Required)

For a list of supported database versions, see the *Cloud Service Automation System and Software Support Matrix*.
Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a 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 multi-language support (Optional)

To support characters of any language worldwide, use Unicode (`AL32UTF8`) as Database Character Set (set property `NLS_CHARACTERSET = AL32UTF8`).

Set the property `NLS_LENGTH_SEMANTICS = CHAR;`

Work with your database administrator to set the parameter (or see the manufacturer's documentation for more information).

> **Note:** Once the database is created, national language support cannot easily be changed.

Download Oracle JDBC Drivers (Required)

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

Download a supported version of the `JDBC.jar` file or files and save them on the system on which CSA will be installed. Note the location where you save the file or files as you must provide this information when installing CSA.

Configure Oracle

> **Note:** These tasks must be completed before installing CSA.

Separate database users are required for CSA and its components. You must create a separate database user for:

- Identity Management component
- CSA
- Embedded Operations Orchestration (Optional)

> **Note:** If you want to use external Operations Orchestration, no additional schema is needed.

Create Database Users for CSA

Work with the database administrator to create a database that is used by the embedded Operations Orchestration, CSA (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.

> **Caution:** The database name and username cannot contain more than one dollar sign symbol ($). For example, c$adb is a valid name but c$$adb and cadb are not valid names.

To create database users for CSA, follow these steps:

1. Create a user for CSA (for example, `csadbuser`) with permissions to create sessions, tables, views, sequences and to store data to the default tablespace. (Replace the `<csadbuser_password>` token with your desired user password.)

   ```
   create user csadbuser

   identified by "<csadbuser_password>";

   grant CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE SEQUENCE, UNLIMITED TABLESPACE to csadbuser;

   grant CREATE ANY SYNONYM to csadbuser ; -- optional - this step is needed only if you would like to use the reporting user (below).
   ```

   Provide this username and password when prompted for the CSA database information during the installation of CSA.

2. (Optional) Create a read-only reporting user (for example, `CSAReportingDBUser`). The user is needed only if you want to use the reporting capabilities of CSA.(Replace the `<CSAReportingDBUser_password>` token with your desired user password.).

   ```
   create user CSAReportingDBUser

   identified by "<CSAReportingDBUser_password>";

   grant CREATE SESSION to CSAReportingDBUser_password;
   ```

   Provide this username and password when prompted for the CSA reporting user information during the installation of CSA.

3. Create a user for the Identity Management component (for example, `csaidmdbuser`) with permissions to create sessions, tables and to store data to the default tablespace. (Replace the `<csaidmdbuser_password>` token with your desired user password.)

   ```
   create user csaidmdbuser

   identified by "<csaidmdbuser_password>";

   grant CREATE SESSION, CREATE TABLE, UNLIMITED TABLESPACE to csaidmdbuser;
   ```

   Provide this username and password when prompted for the Identity Management component database information during the installation of CSA.

4. Create a user for the embedded Operations Orchestration (Optional - needed only if you want to install the embedded OO). For example, `csaoodbuser` with permissions to create sessions, tables, sequences and to store data to the default tablespace. (Replace the `<csaoodbuser_password>` token with your desired user password.)

   ```
   create user csaoodbuser

   identified by "<csaoodbuser_password>";

   grant CREATE SESSION, CREATE TABLE, CREATE SEQUENCE, UNLIMITED TABLESPACE to
   csaoodbuser;
   ```

   Provide this username and password when prompted for the Operations Orchestration database information during the installation or upgrade of CSA.

5. Create a user for the Workflow Designer component (for example, `csaooddbuser`)) with permissions to create sessions, tables and to store data to the default tablespace. (Replace the `<csaooddbuser_password>` token with your desired user password.)

   ```
   create user csaooddbuser

   identified by "<csaooddbuser_password>";

   grant CREATE SESSION, CREATE TABLE, UNLIMITED TABLESPACE to csaooddbuser;
   ```

   Provide this username and password when prompted for the Workflow Designer component database information during the installation of CSA.

   > **NOTE**: If you are using Oracle 11g R2 or 11g R2 RAC, it is recommended to apply patch **20299013** before installing Operations Orchestration.

Create a Tablespace for LOBs (Recommended)

For performance reasons, HPE recommends that you create a new tablespace which stores LOBs for the `CSA_DOCUMENT` table. These tasks can be completed after CSA is installed. Create a new tablespace (for example, `csadbuserlob`). Work with your database administrator (or see the manufacturer's documentation for more information). HPE recommends that the initial tablespace size should be at least 3 GB.

```
CREATE TABLESPACE csadbuserlob
 DATAFILE 'csadbuserlob.dbf'
 SIZE 3G AUTOEXTEND ON;
```

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

```
ALTER TABLE csa_document
 MOVE LOB(content)
 STORE AS (TABLESPACE csadbuserlob);
```

Install Microsoft SQL Server

For more information on installing Microsoft SQL Server, see the *Cloud Service Automation System and Software Support Matrix* Guide for a list of supported database versions.
Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

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

Configure Microsoft SQL Server

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

Enable TCP/IP (Required)

TCP/IP must be enabled on the Microsoft SQL Server in order for CSA to log on to 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:

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 TCP/IP is active and enabled, and verify the TCP port is set to 1433. Update any properties that are not set correctly.

Configure a Microsoft SQL Server User for CSA (Required)

An CSA database user is needed when installing CSA.

> **Caution:** The database name and username cannot contain more than one dollar sign symbol ($). For example, c$adb is a valid name but c$$adb and cadb are not valid names.

To create a database user for CSA, do the following:

1. Log on to the SQL Server as the sa user (or another user that can create logins, users and databases) using your favorite sql editor, for example, Microsoft SQL Server Management Studio.
2. Create a login for all needed CSA databases (for example, csadbuser):

   ```
   CREATE LOGIN csadbuser WITH PASSWORD = '<csadbuser_password>';
   ```

   You must provide this database username and password when prompted for the CSA , OO and the Identity Management component database information during the installation or upgrade of CSA.
3. Create a new database for CSA (for example, csadb) and a user (for example, csadbuser) within the database with db_owner role:

   `CREATE DATABASE csadb;` -- optionally you can use COLLATE option with case insensitive collation, for example, `SQL_Latin1_General_Cp1_CI_AS;`

   `USE csadb;` -- or connect to csadb in another way.

   ```
   CREATE USER csadbuser FOR LOGIN csadbuser;
   ```

   ```
   ALTER ROLE db_owner ADD MEMBER csadbuser;
   ```

   It is recommended to set the following parameters on the `csadb` database:

   ```
   ALTER DATABASE csadb SET ALLOW_SNAPSHOT_ISOLATION OFF;
   ```

   ```
   ALTER DATABASE csadb SET READ_COMMITTED_SNAPSHOT ON;
   ```

   > **Caution:** CSA requires 'Case Insensitive' Collation of the database. The CSA database collation and the `tempDB` collation in SQL server must be the same. You must provide this database name when prompted for the CSA database information during the installation of CSA.

4. (Optional) Create a reporting read-only user. The user is needed only if you want to use the reporting capabilities of CSA:

   ```
   CREATE LOGIN CSAReportingDBUser WITH PASSWORD ='<CSAReportingDBUser_password>';

   USE csadb; -- or you can connect to csadb in another way.

   CREATE USER CSAReportingDBUser FOR LOGIN CSAReportingDBUser;

   ALTER ROLE db_datareader ADD MEMBER CSAReportingDBUser;
   ```

   Provide this login name and password when prompted for the CSA reporting database user during the installation of CSA.

5. Create a new database for the Identity Management component and a user (for example, `csadbuser`) within the database with the `db_owner` role:

   ```
   CREATE DATABASE idmdb;

   USE idmdb; -- or you can connect to idmdb in another way.

   CREATE USER csadbuser FOR LOGIN csadbuser;

   ALTER ROLE db_owner ADD MEMBER csadbuser;
   ```

   It is recommended to set following parameters on idmdb database:

   ```
   ALTER DATABASE idmdb SET ALLOW_SNAPSHOT_ISOLATION ON;

   ALTER DATABASE idmdb SET READ_COMMITTED_SNAPSHOT ON;
   ```

   > **Caution:** The Identity Management component requires 'Case Insensitive' Collation of the database. The Identity Management component database collation and the `tempDB` collation in SQL server must be the same. Provide this database name when prompted for the Identity Management component database information during the installation of CSA.

6. (Optional - needed only if you want to install embedded OO). Create a database for embedded Operations Orchestration (for example, csaoodb) and a user (for example, csadbuser) within the database with db_owner role.

   See the *Operations Orchestration Database Guide* for more information about database requirements for Operations Orchestration

   Note: OO requires 'Case Sensitive' Collation of the database (for example, `SQL_Latin1_General_Cp1_CS_AS`):

   ```
   CREATE DATABASE oodb COLLATE SQL_Latin1_General_Cp1_CS_AS;
   USE oodb; -- or you can connect to the oodb in another way.
   ```

```
CREATE USER csadbuser FOR LOGIN csadbuser;
ALTER ROLE db_owner ADD MEMBER csadbuser;
```

As of the current release date of CSA in this guide, the mandatory database options for the Microsoft SQL Server for Operations Orchestration are:

```
ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT:

ALTER DATABASE oodb SET ALLOW_SNAPSHOT_ISOLATION ON;

ALTER DATABASE oodb SET READ_COMMITTED_SNAPSHOT ON;
```

> **Caution:** Verify the latest mandatory options and follow the instructions in the Operations Orchestration Database Guide when creating the Operations Orchestration database. Provide this database name when prompted for the Operations Orchestration database information during the installation of CSA.

7. Create a new database for the Workflow Designer component and a user (for example, `csaooddbuser`) within the database with the `db_owner` role:

```
CREATE DATABASE ooddb;

USE ooddb; -- or you can connect to ooddb in another way.

CREATE USER csadbuser FOR LOGIN csadbuser;

ALTER ROLE db_owner ADD MEMBER csadbuser;
```

It is recommended to set following parameters on ooddb database:

```
ALTER DATABASE ooddb SET ALLOW_SNAPSHOT_ISOLATION ON;

ALTER DATABASE ooddb SET READ_COMMITTED_SNAPSHOT ON;
```

> **Caution:** The Workflow Designer requires 'Case Insensitive' Collation of the database. The Workflow Designer database collation and the `tempDB` collation in SQL server must be the same. Provide this database name when prompted for the Workflow Designer component database information during the installation of CSA.

Create a Filegroup for LOBs

(Optional – performance optimization) If you extensively attach documents to CSA artifacts, it might be convenient for performance reasons to separate the table CSA_DOCUMENT (containing

attached documents) to a different filegroup on a standalone disk. Discuss this option with your database administrator to discover if it might be suitable in your case.

Example: Moving the CSA_DOCUMENT table to a non-default filegroup:

1. Create a filegroup with a file:

```
ALTER DATABASE csadb ADD FILEGROUP csa_lob_group;

ALTER DATABASE csadb ADD FILE (NAME = csa_lob_file, FILENAME= 'D:\DATA\csa_lob_
file.mdf', SIZE = 3GB, FILEGROWTH = 10%) TO FILEGROUP csa_lob_group;
```

> **Note:** Please change FILENAME and SIZE parameters accordingly.

2. Create a new table CSA_DOCUMENT_NEW as a mirror of the original CA_DOCUMENT table, that overrides the filegroup option:

```
use csadb;

create table CSA_DOCUMENT_NEW (
       CONSUMER_VISIBLE tinyint,
       CONTENT image,
       CONTENT_LENGTH numeric (19,0),
       DOC_ORDER int,
       HEIGHT nvarchar(255),
       MIME_TYPE nvarchar(255),
       URL nvarchar(255),
       WIDTH nvarchar(255),
       UUID nvarchar(255) not null,
       ARTIFACT_CONTEXT_ID nvarchar(255) not null,
       ARTIFACT_CONTEXT_TYPE_ID nvarchar(255),
       DOCUMENT_TYPE_ID nvarchar(255) not null,
       primary key (UUID)
       ) ON csa_lob_group;
```

```
create index FKB7B1E7C97F204E54_i on CSA_DOCUMENT_NEW (ARTIFACT_CONTEXT_ID);
create index FKB7B1E7C915AC76B9_i on CSA_DOCUMENT_NEW (ARTIFACT_CONTEXT_TYPE_
ID);

create index FKB7B1E7C9E7C20D41_i on CSA_DOCUMENT_NEW (DOCUMENT_TYPE_ID);

alter table CSA_DOCUMENT_NEW add constraint FKB7B1E7C97F204E54 foreign key
(ARTIFACT_CONTEXT_ID) references CSA_ARTIFACT;

alter table CSA_DOCUMENT_NEW add constraint FKB7B1E7C915AC76B9 foreign key
(ARTIFACT_CONTEXT_TYPE_ID) references CSA_CATEGORY;

alter table CSA_DOCUMENT_NEW add constraint FKB7B1E7C9E7C20D41 foreign key
(DOCUMENT_TYPE_ID) references CSA_CATEGORY;

alter table CSA_DOCUMENT_NEW add constraint FKB7B1E7C98A34BFD7 foreign key
(UUID) references CSA_ARTIFACT;
```

> **Note:** For reference, see the latest definition of the CSA_DOCUMENT table and related indexes and constraints in `CSA_HOME\scripts\create-mssql-schema.sql`.

3. Copy the data from the the original CSA_DOCUMENT table to CSA_DOCUMENT_NEW:

```
INSERT INTO CSA_DOCUMENT_NEW (CONSUMER_VISIBLE, CONTENT, CONTENT_LENGTH, DOC_
ORDER, HEIGHT, MIME_TYPE, URL, WIDTH, UUID, ARTIFACT_CONTEXT_ID, ARTIFACT_
CONTEXT_TYPE_ID, DOCUMENT_TYPE_ID)
SELECT CONSUMER_VISIBLE, CONTENT, CONTENT_LENGTH, DOC_ORDER, HEIGHT, MIME_TYPE,
URL, WIDTH, UUID, ARTIFACT_CONTEXT_ID, ARTIFACT_CONTEXT_TYPE_ID, DOCUMENT_TYPE_
ID FROM CSA_DOCUMENT;
```

4. Drop the original table CSA_DOCUMENT:

```
DROP TABLE CSA_DOCUMENT;
```

5. Rename CSA_DOCUMENT_NEW back to CSA_DOCUMENT.

```
EXEC sp_rename 'CSA_DOCUMENT_NEW', 'CSA_DOCUMENT';
```

Install PostgreSQL

For more information on installing PostgreSQL, see the *Cloud Service Automation System and Software Support Matrix* Guide for a list of supported database versions.
Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a 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

> **Note:** Complete the following tasks before CSA is installed. Work with the database administrator to complete the following tasks (or see the manufacturer's documentation for more information).

> **Caution:** The username cannot contain more than one dollar sign symbol ($). For example, c$adb is a valid name but c$$adb and cadb are not valid names.

Configure PostgreSQL Users and Database (Required)

1. Log on to PostgreSQL server as the postgres user (or another user that can create users and databases) using your favorite sql editor, for example using psql: `psql -U postgres`
2. Create a CSA database user (for example, csadbuser). This user should inherit rights from parent roles:

   ```
   create user csadbuser login password '<csadbuser_password>' inherit;
   ```

   Provide this database username and password when prompted for the CSA , OO and the Identity Management component database information during the installation or upgrade of CSA.
3. (*Optional*) Create a reporting read-only user. The user is needed only if you want to use the reporting capabilities of CSA:

```
create user csareportingdbuser login password '<csareportingdbuser_password>'
inherit;
```

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

4. Create a new database for CSA (for example, csadb) with owner csadbuser.

   ```
   create database csadb with owner=csadbuser;
   ```

   Optionally, if you want to use reporting functionality, allow csareportingdbuser to connect to the csadb database:

   ```
   grant connect on database csadb to csareportingdbuser;
   ```

5. (*Optional - needed only if you want to install embedded*OO) Create a database for embedded Operations Orchestration (for example, csaoodb).

   See the *Operations Orchestration Database Guide* for more information about database requirements for Operations Orchestration.

   ```
   create database oodb with owner=csadbuser;
   ```

6. Create a new database for the Identity Management component.

   ```
   create database idmdb with owner=csadbuser;
   ```

7. Create a new database for the Workflow Designer component.

   ```
   create database ooddb with owner=csadbuser;
   ```

8. (Optional post install step) Grant read-only access for a reporting user. It is needed only if you want to use the reporting user.

   This step has to be processed after the installation is finished, because database tables and views have to be created prior to running this command.

   a. Connect to the csadb database. For example if you are using psql, use following statement:

      ```
      \connect csadb
      ```

   b. Grant read-only access for the reporting user with this command:

      ```
      grant select on all tables in schema public to csareportingdbuser;
      ```

Install and Configure Cloud Service Automation

During one of the following steps, you will install a CSA instance. Although Operations Orchestration is an Optional application, it should be installed before installing CSA.

- "Install Operations Orchestration" on page 22
- "Install Cloud Service Automation for Windows " on page 25
- "Install Cloud Service Automation for Linux" on page 38
- "Install Cloud Service Automation with Remote MPP for Windows " on page 51
- "Install Cloud Service Automation with Remote MPP for Linux " on page 54

Install Operations Orchestration

Install Operations Orchestration to the correct version and patch level.

> This section is optional. Cloud Service Automation can install an embedded Operations Orchestration to the correct version.

For more information on installing Operations Orchestration, see the *Cloud Service Automation System and Software Support Matrix* for version requirements.
Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

CSA can be installed with Operations Orchestration by using the following two options:

- CSA can be installed with embedded Operations Orchestration 10.70 or
- CSA can be connected to already installed Operations Orchestration

If you are using an existing installation of Operations Orchestration, verify that the correct versions of patches and updates have been applied.

> **Caution:** If you are using an earlier version of Operations Orchestration:
>
> **YOU MUST UPGRADE HPE Operations Orchestration TO VERSION 10.50 BEFORE INSTALLING CSA**.
>
> After upgrading to Operations Orchestration 10.50, update it by following the instructions below.

> **Caution:** During a new CSA 4.80 installation, if you choose to include embedded instance of Operations Orchestration, the CSA Installer installs Operations Orchestration 10.70 instance.
>
> In case of a complete CSA uninstallation, the installer will also uninstall the Embedded Operations Orchestration 10.70 instance, regardless of whether it was loaded into a default or non-default installation path.

Configure an Internal User (Required)

The CSA Installer will require the Operations Orchestration administrator credentials where administrator for this purpose is any user that has the ADMINISTRATOR and SYSTEM_ADMIN roles.

If you want to use single sign-on and the user name for Operations Orchestration administrator is different than "admin", you may want to setup an account with user name as "admin" and assign ADMINISTRATOR and SYSTEM_ADMIN roles. This will enable you to click through from CSA to Operations Orchestration without an extra login step.

You can review, add, or manage users and their roles in Operations Orchestration through the Operations Orchestration Central; click System Configuration, Security, Internal Users. Ensure that "Enable authentication" option is turned on (once the administrative user is defined).

Export Operations Orchestration's Root Certificate (Required)

Export Operations Orchestration's certificate from Operations Orchestration's truststore and, if Operations Orchestration and CSA are not installed on the same system, copy the certificate to the CSA system. This certificate will be imported into CSA's truststore by the CSA installer. TLS must be configured between CSA 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:

   Windows:

   ```
   .\java\bin\keytool -export -alias tomcat -file C:\oo.crt -
   keystore .\Central\var\security\key.store -storepass changeit
   ```

   Linux:

   ```
   ./java/bin/keytool -export -alias tomcat -file /tmp/oo.crt -
   keystore ./Central/var/security/key.store -storepass changeit
   ```

   where `C:\oo.crt` and `/tmp/oo.crt` are examples of filenames and locations used to store the exported root certificate (you can choose a different filename and location).
3. If Operations Orchestration is not running on the same system as CSA, copy `oo.crt` from the Operations Orchestration system to the system running CSA.

> **Note:** The CSA 4.80 installer allows CSA to point to an external Operations Orchestration (OO) 10.70 instance without warning, regardless of whether the OO is installed. Verify the following use cases are working correctly:

- Import topology/sequence component/design
- Fulfill topology/sequence design, invoke public actions, and then remove the topology/sequence design

Install Cloud Service Automation for Windows

The following installation steps are for Windows:

> **Note:** Installation log files are written to the `%CSA_HOME%\_CSA_4_80_0_installation\Logs\` directory.

> **Caution:** The memory requirements for any CSA installation are as follows:
>
> - A CSA installation with the External Operations Orchestration option requires a minimum of 4.5 GB *available* RAM.
> - A CSA installation with the Embedded Operations Orchestration option requires a minimum of 6 GB *available* RAM.
> - It is strongly recommended that you install CSA on a system with *at least* 16 GB RAM.
>
> For a complete listing of resource requirements and compatibility information, see the *Cloud Service Automation System and Software Support Matrix* for the relevant product release.

To install Cloud Service Automation (CSA), 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.zip` file.
   a. Navigate to the directory to which the files have been extracted.
   b. Run the `setup.bat` installation file.

   > **Note:** A command window (which will display until the script has completed) and a dialog that shows the progress of installation preparation are displayed. Do not close either window. The installation preparation progress dialog disappears after the installation preparation has completed.
3. On the Introduction screen, read the information and click **Next**.
4. Read the license agreement and select **I accept the terms of the License Agreement**. Click **Next** to continue with the installation.

   If the following error message displays:

```
Another version of CSA is configured in the registry. However, CSA has been
uninstalled (the CSA installation directory %CSA_HOME% does not exist). You
must exit the installer and delete the entry in the registry before installing
CSA. See the Cloud Service Automation Installation Guide for more information
about deleting the registry entry.
```

exit the installer. Locate the `C:\Program Files\Zero G Registry\.com.zerog.registry.xml` file (you may need to show hidden files), make a backup copy, delete all CSA entries from the `.com.zerog.registry.xml` file, and restart the installer.

5. Select **CSA and Marketplace Portal** and click **Next**.

   Selecting **CSA and Marketplace Portal** installs the entire CSA application, including the Cloud Service Management Console, Identity Management component, and Marketplace Portal, on the system.

   Selecting **Marketplace Portal** installs only the Marketplace Portal on the system.

6. Choose a location in which to install CSA and click **Next** (`CSA_HOME` is set to this location).

   The default location is `C:\Program Files\HPE\CSA`.

   > **Note:** If the directory in which you choose to install CSA is not empty, existing content in the directory may be overwritten or deleted when CSA is installed, upgraded, or uninstalled. There is a validation in installer which will block the installation.
   >
   > **Caution:** The entire directory path cannot contain more than one dollar sign symbol ($). For example, C:\HPE\C$A\Java and C:\HPE\CSA\Java$ are valid paths. However C:\HPE\C$A\Java$ and C:\HPE\C$$A\Java are not valid paths.

7. Select the JRE that will be used by CSA.

   In this documentation, the directory in which the JRE is installed will be referred to as *<csa_jre>*.

   For a list of supported JREs, see the *Cloud Service Automation System and Software Support Matrix*.
   Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

   OpenJDK JRE

   The OpenJDK JRE is bundled with CSA. If you want to use the OpenJDK JRE, select **Open JRE** and click **Next**.

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

Oracle JRE

If you have installed a supported version of Oracle JRE to be used by CSA, select **Oracle JRE**, choose 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 should be used by CSA, click **Choose** and select the location in which you installed the JRE that will be used by CSA.

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

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

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

   Click **No** if you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version 4.80. When you select this option, you cannot use the installer to deploy sample content and the CSA service does not start after you exit the installer.

   > **Note:** In this version of CSA, Organizations are now stored in the Identity Management component, not in CSA. If you selected **Yes** during the installation, the CSA installer will populate the database and migrate the organizations automatically; however, if you selected **No** during the installation, you will need to populate the database and migrate organizations manually using CSA tools.

   Follow the next steps if you selected **No** during the installation and need to import content into the database and your organizations into the Identity Management component for CSA:

   a. Run the **SchemaInstallationTool** to populate the database.

      > **NOTE**: Before executing schema installation tool make sure JDBC drivers are copied to the tools folder: `C:\Program Files\HPE\CSA\Tools\SchemaInstallationTool`.
      > For Example: `MSSQL-DB-- jtds-1.3.1`

   b. Run the **OrgMigrationTool** to migrate organizations from CSA to the Identity Management component.

> **NOTE**: **OrgMigrationTool** is applicable only for upgrade from CSA 4.6 and not from CSA 4.7.

You can access the **SchemaInstallationTool** by using the following command:

i. Navigate to the `<CSA_HOME>\Tools\SchemaInstallationTool\` directory.

ii. Run `<JAVA_HOME>\bin\java.exe –jar schema-installation-tool.jar`

Do the following to access the **OrgMigrationTool**:

i. Navigate to the `<CSA_HOME>\Tools\OrgMigrationTool\` directory.

ii. `Run <JAVA_HOME>\bin\java.exe -jar org-migration-tool.jar -c config.properties --csa.home <CSA_HOME> -t json -j <JDBC_DRIVER_JAR>`

You can access the **UCMDBComponentImportTool** by using the following command:

i. Navigate to the `<CSA_HOME>\Tools\UCMDBComponentImportTool\` directory.

ii. Run `<JAVA_HOME>\bin\java.exe –jar ucmdb-component-import-tool-04.80.000-SNAPSHOT.jar`

See the end of this section for information about how to start and stop the CSA service.

9. Select the type of database installed (Microsoft SQL Server, Oracle, or PostgreSQL) and click **Next**.

   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 CSA system).

   - For a list of supported JDBC driver versions, see the *Cloud Service Automation System and Software Support Matrix Guide*.
   - Click **Choose** to select the correct JDBC directory.

10. Define the database instance on which the CSA database components should be installed or where the CSA database schema already exists. Enter the following database information and click **Next**.

Field Name	Description
Database Host	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]`.
Database	The database port number. For example, **1433:** (Microsoft SQL Server), **1521:**

Field Name	Description
Port	(Oracle), **5432:** (PostgreSQL).
Database Name / Oracle service name	The global database or service name of the database instance on which the CSA database schema will be installed (for example, csadb). If you are creating a new CSA database schema, this is the database or service name of the database instance on which the CSA database components will be installed. If you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version 4.80, this is the database or service name of the database instance on which the CSA database schema exists.
Database Username	The username of the database user you configured for CSA in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide (for example, csadbuser).
Database Password	The password for the database user.

If you created an Oracle reporting database role and read-only user, *OR* a MS SQL Server or PostgreSQL reporting database user when you configured the database, select the **Reporting User** checkbox and enter the following information:

Field Name	Description
CSA Reporting Database Username	The username of the database user you configured for reporting purposes for CSA in the *Configure Oracle / Microsoft SQL Server / PostgreSQL* section of this guide (for example, CSAReportingDBUser).
CSA Reporting Database Password	The password for the CSA reporting database user.

11. 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 CSA (Microsoft SQL Server, Oracle, or PostgreSQL).

    > **NOTE**: For Microsoft SQL Server, it is mandatory to enable the snapshot isolation for Identity Management componentdatabase which can be achieved through following two database statements:

```
ALTER DATABASE idmdb SET ALLOW_SNAPSHOT_ISOLATION ON;
```

```
ALTER DATABASE idmdb SET READ_COMMITTED_SNAPSHOT ON;
```

Field Name	Description
Database Host: MSSQL, Oracle, or PostgreSQL	The hostname or IP address of the server where the Identity Management component database is located. **Note:** When specifying an IPv6 address, it must be enclosed in square brackets. For example, `[f000:253c::9c10:b4b4]` or `[::1]`.
Database Port: MSSQL, Oracle, or PostgreSQL	The Identity Management component database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).
HPEIdentity Management component Database Name / Oracle Service Name	The global database or service name of the database instance used by the Identity Management component (for example, csaidmdb). For an Oracle database, this is the System ID (SID).
HPEIdentity Management componentDatabase Username	The username of the database user you configured for the Identity Management component database in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide (for example, csaidmdbuser or csadbuser).
HPEIdentity Management component Database Password	The password for the Identity Management component database user.

12. From the hostname configuration screen, enter the **fully-qualified domain name of the system on which you are installing CSA**. This name is used to generate the self-signed certificate and configure CSA, the Marketplace Portal, and the Identity Management component.

    The self-signed certificate is used when https browser requests are issued for the Cloud Service Management Console or the Marketplace Portal. This self-signed certificate expires 120 days after CSA 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 CSA and manually reconfigure CSA and the Marketplace Portal to use

this certificate. For more information, see the *Cloud Service Automation Configuration Guide*.

13. Do one of the following to integrate with an external (existing) instance of Operations Orchestration or to install the embedded (new) Operations Orchestration instance with CSA.
    - **External OO:** to integrate with an external (existing) instance of Operations Orchestration, complete the following steps:
        i. Select **Use external OO**.
        ii. Click **Next**.
        iii. Select **Enter**.

        Note: If you are using an unsupported version of Operations Orchestration, you will get a **warning** message. If you continue with the installation, you may get provisioning errors. Using an unsupported version of Operations Orchestration could result in a limited amount of demo content that users can select for installation.

        Stop the current installation and do the following:

        i. Check the System and Software Support Matrix document for the supported Operations Orchestration versions.
        ii. Install or upgrade to a supported Operations Orchestration version.
        iii. Restart the CSA installation.
    - **Embedded OO:** To install the embedded (new) Operations Orchestration instance, complete the following steps:
        i. Select **Install embedded OO**.
        ii. Click **Next**.
        iii. Select **Enter** to install the embedded Operations Orchestration.

    After you successfully complete one of the above options, select the CSA content you would like to import (either CSA or Codar) to continue.

14. Define the Operations Orchestration instance with which CSA is to be integrated. Enter the following information related to external OO and click **Next**.

Field Name	Description
HPE OO Hostname	The This is the fully-qualified domain name or IP address of the server on which

Field Name	Description
	Operations Orchestration is located. Specify the host name that was used to generate Operations Orchestration's certificate. The host name is used for TLS validation and to build the URL that the Cloud Service Management Console uses to interact with Operations Orchestration (for example, in the subscription event overview section of the **Operations** area in the Cloud Service Management Console, 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]`.
HPE OO Port	The port number used to communicate with Operations Orchestration, such as 8443. The port number is used to build the URL that the Cloud Service Management 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.
HPE OO User	The name of the user who logs on to Operations Orchestration Central. You should use the `admin` user. If you followed all the steps documented in the *Install Operations Orchestration* section of this guide, this is the `admin` user.
HPE OO Password	The password used by the OO user to log on to Operations Orchestration Central. If you followed all the steps documented in the *Install Operations Orchestration* section of this guide, use the password `cloud`.
HPE OO Certificate File	The file name and location of Operations Orchestration's certificate from Operations Orchestration's truststore on the CSA system. If you have not already done so, export Operations Orchestration's certificate and copy it to the CSA system. See the *Install Operations Orchestration* section in the *Installation Guide* or the *Initial Setup* section in the *Upgrade Guide* for more information).

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

15. Choose a location in which to install the embedded Operations Orchestration and click **Next**.
16. 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 username is **admin**.
HPE OO User Password	The password used by Operations Orchestration for the user who provisions topology designs. The recommended password is **cloud**.
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. The embedded Operations Orchestration should not use the same port as other applications running on the system.

17. 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 CSA *(Oracle / Microsoft SQL Server / PostgreSQL)* .

Field Name	Description
Database Host: MSSQL, Oracle, or PostgreSQL	The hostname or IP address of the server where the embedded Operations Orchestration database is located.
Database Port: MSSQL, Oracle, or PostgreSQL	The embedded Operations Orchestration database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).
HPE OO Database Name / Oracle Operations Orchestration service name	The service or global database name of the database instance used by the Identity Management component (for example, csaidmdb). For an Oracle database, this is the System ID (SID).
HPE OO Database Username	The username of the database user you configured for the Operations Orchestration database in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide (for example, csaidmdbuser or csadbuser).
HPE OO Database Password	The password for the Operations Orchestration database user.

18. On the **Workflow Designer** screen, configure a Workflow Designer component. Depending on

whether you wish to add a new

database or reuse an existing one, select one of the following options, and click **Next**.

- No. I will provide new database information.
- Yes. Reuse configuration files from an existing node.

19. Based on the option you selected in the previous step, do one of the following:

- If you chose to provide new database information, specify the following details:

Field Name	Description
Database Host: MSSQL, Oracle, or PostgreSQL	The hostname or IP address of the server where the database is located.
Database Port: MSSQL, Oracle, or PostgreSQL	The database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).
Workflow Designer Database Name/ Oracle service name	The name of the database instance on which the CSA database schema will be installed. • If you are creating a new CSA database schema, this is the name of the database instance on which the CSA database components will be installed. • If you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version 4.80, this is the name of the database instance on which the CSA database schema exists. • For an Oracle database, this is the System ID (SID). **NOTE**: The database used by the embedded Workflow Designer must be the same type of database used by CSA (Oracle / Microsoft SQL Server / PostgreSQL) .
Workflow Designer Database User Name	The user name of the database user you configured for the Workflow Designer database in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide (for example, csadbuser).
Workflow Designer Database Password	The password for the database user.

- If you chose to provide configuration files from an existing node, select the respective properties files available in an existing Workflow Designer to reuse the configuration values for the new installation by clicking the **Choose** button and navigating to the respective location of the

properties file.

Following are the parameters representing configuration files on machine with finished installation:

```
CSA_HOME/workflow-designer/designer/conf/database.properties
CSA_HOME/workflow-designer/designer/var/security/secured.properties
CSA_HOME/workflow-designer/designer/var/security/encryption.properties
CSA_HOME/workflow-designer/designer/var/security/encryption_repository
```

where `CSA_HOME` is the directory in which CSA is installed.

20. Enter the **Workflow Designer Port number** click **Next**. The default port number is **8446**.
21. Verify the default endpoint details and click **Next**.

    You can change the endpoint details by clicking **Use a specific endpoint to connect to Workflow Designer**, and providing the required details.

    > **NOTE:** By default, there is no need to specify the **Workflow Designer** component endpoint as it is running on the same machine as HPE Cloud Service Automation. However, in case of a cluster installation, it is possible to connect to the component using a virtual IP (load balancer).

22. You can choose to deploy the required content during installation (making the sample service designs available in the Design area of the Cloud Service Management Console) or deploy the content at a later time (see the *CSA/Codar Content at a Glance Guide* or *Cloud Service Automation Configuration Guide* for more information).

    To deploy the required content during the CSA installation process, select **Install additional provider integration service designs, components and content** and click **Next**.

    To deploy the required 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. See the *CSA/Codar Content at a Glance Guide* or *Cloud Service Automation Configuration Guide* for more information.

    > **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. In some instances, 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 CSA, Elasticsearch 1.6.1, HPE Search Service, and Marketplace Portal, and Operations Orchestration Central services have started by navigating to **Start > Administrative Tools > Services**. It can take up to five minutes for the CSA to start. If one or more services have not started, right-click on the service and select **Start**.

    The installer creates the CSA and HPE Marketplace Portal services. If you opted to install the CSA database components, the installer starts these services. The CSA service must be running in order to access the Cloud Service Management Console, and the HPE Marketplace Portal service must be running in order to access the Marketplace Portal, and the HPE Operations Orchestration Central service must be running in order to access Operations Orchestration Central.

To start, stop, and restart the CSA, Elasticsearch 1.6.1, HPE Search Service, and Marketplace Portal, and Operations Orchestration Central services, navigate to **Start > Administrative Tools > Services**, right-click on a service, and select the desired action.

Install Cloud Service Automation for Linux

The following installation steps are for Linux:

> **Note:** Installation log files are written to the `$CSA_HOME/_CSA_4_80_0_installation/Logs/` directory and are named `csa_*.txt`.

> **Caution:** The memory requirements for any CSA installation are as follows:
>
> - A CSA installation with the External Operations Orchestration option requires a minimum of 4.5 GB *available* RAM.
> - A CSA installation with the Embedded Operations Orchestration option requires a minimum of 6 GB *available* RAM.
> - It is strongly recommended that you install CSA on a system with *at least* 16 GB RAM.
>
> For a complete listing of resource requirements and compatibility information, see the *Cloud Service Automation System and Software Support Matrix* for the relevant product release.

To install CSA, complete the following steps.

1. Log on to the system as the root user.
2. Run the following command to install the unzip utility, assuming it is not already installed:

   ```
   apt-get install unzip
   ```

3. Enter the following command to create an installation directory for CSA :
   `mkdir -p /usr/local/hpe/csa`

   > **Note:** This document assumes that you install the product in the `/usr/local/hpe/csa` directory. All of the examples shown in this document use this path and directory.

4. For the installation directory, run the following command to set the owner to csauser and the group to csagrp:

   ```
   chown -R csauser:csagrp /usr/local/hpe/csa
   ```

5. Log off as the root user and log on as the csauser.

6. Copy the CSA installation file (`setup.bin`) to the system and go to the directory in which it has been copied.
7. Verify that `setup.bin` is owned by csauser and that csauser has full permissions to the file. If necessary, do the following:
   a. Log on as the root user
   b. Enter one or both of the following commands:

      ```
      chown csauser setup.bin
      chmod u+rwx setup.bin
      ```

   c. Log off as the root user and log on as the csauser.
8. 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 causes the installer to fail. Either set the variable to a value that does not contain an escape sequence or change the variable so that is it not set.
9. Run the `setup.bin` installation file as csauser.

   > **Note:** You must run `setup.bin` as csauser. If you install CSA as another user, you might not be able to run CSA.

10. Read the Introduction. Click **Enter** to continue with the installation.
11. Read the license agreement. Click **Enter** to scroll through the entire agreement.
12. Select **Y** and **Enter** to accept the license agreement and continue with the installation. Select **N** and **Enter** to exit the installation.

    If you see an error similar to the following message, complete the steps show beneath this message:

    Another version of CSA is configured in the registry. However, CSA has been uninstalled (the CSA installation directory *$CSA_HOME* does not exist). You must exit the installer and delete the entry in the registry before installing CSA.

    a. Exit the installer.
    b. Locate the `$HOME/.com.zerog.registry.xml` file (for example, `/home/csauser/.com.zerog.registry.xml`)
    c. Make a backup copy of the `.com.zerog.registry.xml` file.
    d. Delete all of the CSA entries from the `.com.zerog.registry.xml` file.

e. Run the `setup.bin` installation file as the csauser and follow the interactive instructions as shown in the previous steps.

13. Select **CSA and Marketplace Portal**, then click **Enter**.

> **Note:** Selecting **CSA and Marketplace Portal** installs the entire CSA application, including the Cloud Service Management Console, Identity Management component, and Marketplace Portal, on the system.
>
> Selecting **Marketplace Portal** installs only the Marketplace Portal on the system.

14. Accept the default location or enter the absolute path to a location in which to install CSA, then select **Enter**.

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

15. Do one of the following to select the JRE that will be used by CSA:
    - If you want to use the OpenJDK JRE, which is is bundled with CSAenter **1**.
    - If you have installed a supported version of Oracle JRE to be used by CSA, enter **2**, then enter the location in which you installed this JRE.

> **Note:** In this instruction set, the directory in which the JRE is installed is referred to as `$CSA_JRE_HOME`. For a list of supported JREs, see the *Cloud Service Automation System and Software Support Matrix*.

16. Complete only one of the following options to install the CSA database components on the database instance and create the CSA database schema, if it does not already exist.

> **Note:** In this version of CSA, Organizations are now stored in the Identity Management component, not in CSA. If you selected **Yes** during the installation, the CSA installer will populate the database and migrate the organizations automatically; however, if you selected **No** during the installation, you will need to populate the database and migrate organizations manually using CSA tools.

    - Options 1: Type **Yes** to install CSA database components and create the CSA database schema. When you select this option, the CSA process automatically starts when you exit the installer.
    - Option 2: Type **No** and complete the following steps if you are using an existing HPECSA database schema that was created as part of a prior successful installation of CSA version 4.80. When you select this option, you cannot use the installer to deploy sample content and

the CSA process does not start when you exit the installer.

Do the following if you need to import content into the database and your organizations into the Identity Management component for CSA:

i. Run the **SchemaInstallationTool** to populate the database.

   A. `Go to <CSA_HOME>/Tools/SchemaInstallationTool/`

   B. `Run <JAVA_HOME>/bin/java –jar schema-installation-tool.jar`

ii. Run the **OrgMigrationTool** to migrate organizations from CSA to the Identity Management component.

   A. `Go to <CSA_HOME>/Tools/OrgMigrationTool/`

   B. `Run <JAVA_HOME>/bin/java –jar org-migration-tool.jar –c config.properties –csa.home <CSA_HOME> -t json –j <JDBC_DRIVER>`

See "Restarting the CSA Service: " on page 49 for information about how to start and stop the CSA service.

17. Define the database instance on which the CSA database components should be installed. Enter the following database information (select **Enter** after each entry).

a. Enter the type of database you have installed: MSSQL, Oracle, or PostgreSQL.

> **Note:** 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 CSA system). For a list of supported JDBC driver versions, see the *Cloud Service Automation System and Software Support Matrix*.

Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

b. Enter the database host name. This is the host name or IP address of the server on which the database is located.

> **Note:** 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. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).

d. Enter the Oracle service name or database name. This is the service or global database name

of the database instance on which the CSA database schema will be installed.

> **Note:** If you are creating a new CSA database schema, enter the service or database name of the database instance on which the CSA database components will be installed.
>
> If you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version HPE 4.80, enter the service or database name of the database instance on which the CSA database schema already exists.
>
> If you followed the examples in this document, enter csadb.

e. Enter the CSA database user name. This is the user name of the database user you configured for HPE Cloud Service Automation in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL*) section of this guide.

   If you followed the examples in this document, enter `csadbuser`.

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

g. Enter the CSA reporting database user name (optional). This is the user name of the database user you configured for reporting purposes for CSA in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL*) section of this guide.

   If you followed the examples in this document, enter `CSAReportingDBUser`.

h. Enter the CSA reporting database password. This is the password for the CSA reporting database user.

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

    a. Enter the database host name. This is the host name or IP address of the server on which the database is located.

    > **Note:** 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).

    b. Enter the database port. This is the database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).

    c. Enter the Oracle service or database name. This is the service or global database name of the database instance used by the Identity Management component.

    > **Note:** If you followed the examples in this document, enter `csaidmdb`.

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 in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide.

> **Note:** If you followed the examples in this document, enter `csaidmdbuser` or `csadbuser`.

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

19. Enter the CSA server host name. This entry is the **fully-qualified domain name of the system on which you are installing CSA**.

> **Note:** This host name is used to generate the self-signed certificate and configure CSA, the Marketplace Portal, and the Identity Management component.
>
> The self-signed certificate is used when https browser requests are issued for the Cloud Service Management Console and Marketplace Portal. This self-signed certificate expires 120 days after CSA 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 CSA and manually reconfigure CSA and the Marketplace Portal to use this certificate. For more information, see the *Cloud Service Automation Configuration Guide*.

20. Do one of the following to integrate with an external (existing) instance of Operations Orchestration or to install the embedded (new) Operations Orchestration instance with CSA.

- **External OO:** to integrate with an external (existing) instance of Operations Orchestration, complete the following steps:

  i. Select **Use external OO**.

  ii. Click **Next**.

  iii. Select **Enter**.

> **Note:** If you are using an unsupported version of Operations Orchestration, you will get a **warning** message. If you continue with the installation, you may get provisioning errors. Using an unsupported version of Operations Orchestration could result in a limited amount of demo content that users can select for installation.
>
> Stop the current installation and do the following:
>
> i. Check the System and Software Support Matrix document for the supported Operations Orchestration versions.

ii. Install or upgrade to a supported Operations Orchestration version.

iii. Restart the CSA installation.

- **Embedded OO:** To install the embedded (new) Operations Orchestration instance, complete the following steps:

  i. Select **Install embedded OO**.

  ii. Click **Next**.

  iii. Select **Enter** to install the embedded Operations Orchestration.

After you successfully complete one of the above options, select the CSA content you would like to import (either CSA or Codar) to continue.

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

    a. Enter the OO host name. This host name is referred to as the This is the fully-qualified domain name or IP address of the server on which Operations Orchestration is located. Specify the host name that was used to generate Operations Orchestration's certificate. The host name is used for TLS validation and to build the URL that the Cloud Service Management Console uses to interact with Operations Orchestration (for example, in the subscription event overview section of the **Operations** area in the Cloud Service Management Console, 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]`.

    b. Enter the OO port. This port is the port number used to communicate with Operations Orchestration, such as 8443. The port number is used to build the URL that the Cloud Service Management Console uses to interact with Operations Orchestration. By default, Operations Orchestration uses this port and port 8080. Applications running on the system on which Operations Orchestration is installed should not be using these ports.

    c. Enter the OO user. This user is the name of the user who logs on to Operations Orchestration Central. You should use the `admin` user. If you followed all the steps documented in the *Install Operations Orchestration* section of this guide, this is the `admin` user.

    d. Enter the OO password. This password is the password used by the OO user to log on to Operations Orchestration Central. If you followed all the steps documented in the *Install Operations Orchestration* section of this guide, use the password `cloud`.

e. Re-enter the OO password.

f. Enter the OO certificate file. This file is the file name and location of Operations Orchestration's certificate from Operations Orchestration's truststore on the CSA system. If you have not already done so, export Operations Orchestration's certificate and copy it to the CSA system. See the *Install Operations Orchestration* section in the *Installation Guide* or the *Initial Setup* section in the *Upgrade Guide* for more information).

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

22. Enter a location in which to install the embedded Operations Orchestration.

23. Enter the database information for the database used by the embedded Operations Orchestration (select **Enter** after each entry). The database used by the embedded Operations Orchestration must be the same type of database used by CSA *(Oracle / Microsoft SQL Server / PostgreSQL*).

a. Enter the database host name. This is the host name or IP address of the server where the embedded Operations Orchestration database is located.

b. Enter the database port. This is the embedded Operations Orchestration database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).

c. Enter the OO database or Oracle OO service name. This is the name of the database instance used by the embedded Operations Orchestration.

If you followed the examples in this document, enter `csaoodb`.

d. Enter the database username. This is the username of the database user you configured for the Operations Orchestration database.

If you followed the examples in this document, enter `csaoodbuser`.

e. Enter the 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. The embedded Operations Orchestration should not use the same port as other applications running on the system.

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

a. Enter the OO username. This is the name of the user used for provisioning topology designs. This user is given the ADMINISTRATOR and SYSTEM_ADMIN roles. The recommended

username is **admin**.

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

25. On the **Workflow Designer** screen, configure a Workflow Designer component. Depending on whether you wish to add a new database or reuse an existing one, select one of the following options, and click **Next**.

    - Option 1: No. I will provide new database information.
    - Option 2: Yes. Reuse configuration files from an existing node.

      Enter a comma separated list of number for selecting the required choice OR select the `default`.

      If this is standalone installation or first installation of clustered instance just hit **Enter** to choose default option which is option 1.

      In case of clustered installation choose option 2.

26. Based on the option you selected in the previous step, do one of the following:

- If you chose to provide new database information, specify the following details:

Field Name	Description
Database Host: MSSQL, Oracle, or PostgreSQL	The hostname or IP address of the server where the database is located.
Database Port: MSSQL, Oracle, or PostgreSQL	The database port number. For example, **1433:** (Microsoft SQL Server), **1521:** (Oracle), **5432:** (PostgreSQL).
Workflow Designer Database Name/ Oracle service name	The name of the database instance on which the CSA database schema will be installed. • If you are creating a new CSA database schema, this is the name of the database instance on which the CSA database components will be installed. • If you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version 4.80, this is the name of the database instance on which the CSA database schema exists. • For an Oracle database, this is the System ID (SID). **NOTE**: The database used by the embedded Workflow Designer must be the same type of database used by CSA (Oracle / Microsoft SQL Server / PostgreSQL) . Default: `ooddb`
Workflow Designer Database User Name	The user name of the database user you configured for the Workflow Designer database in the *Configure (Oracle / Microsoft SQL Server / PostgreSQL)* section of this guide (for example, csadbuser). Default: `oouser`
Workflow Designer Database Password	The password for the database user.

- If you chose to provide configuration files from an existing node, select the respective properties files available in an existing Workflow Designer to reuse the configuration values for the new installation by clicking the **Choose** button and navigating to the respective location of the properties file.

Following are the parameters representing configuration files on machine with finished installation:

`CSA_HOME/workflow-designer/designer/conf/database.properties`

`CSA_HOME/workflow-designer/designer/var/security/secured.properties`

`CSA_HOME/workflow-designer/designer/var/security/encryption.properties`

`CSA_HOME/workflow-designer/designer/var/security/encryption_repository`

where `CSA_HOME` is the directory in which CSA is installed.

27. Enter the **Workflow Designer Port number** click **Next**. The default port number is **8446**.
28. Verify the default endpoint details and click **Next**.

    You can change the endpoint details by clicking **Use a specific endpoint to connect to Workflow Designer**, and providing the required details.

    > **NOTE:** By default, there is no need to specify the **Workflow Designer** component endpoint as it is running on the same machine as HPE Cloud Service Automation. However, in case of a cluster installation, it is possible to connect to the component using a virtual IP (load balancer).

29. By default, sample content (service designs and the components and Operations Orchestration flows required by the designs) are installed with CSA. You can choose to deploy this content during installation (making the sample service designs available in the Design area of the Cloud Service Management Console) or deploy the content at a later time (see the *CSA/Codar Content at a Glance Guide* for more information).

    To deploy the sample content during the CSA installation process, type **1** (Install additional provider integration service designs, components and content) and select **Enter**.

    To deploy the sample content at a later time, type **2** (Skip content installation) and select **Enter**.

    If you choose to skip content installation, you can install the content at a later time by running the Cloud Content Capsule Installer. See the *CSA/Codar Content at a Glance Guide* or *Cloud Service Automation Configuration Guide* for more information.

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

30. Review your selections and select **Enter** to complete the installation or **Ctrl**-**c** to exit the installation.

31. When the installation completes, select **Enter** to exit the installer.
32. Define the CSA_HOME and JAVA_HOME environment variables for the csauser user. Set CSA_HOME to the location where CSA is installed. In a startup script for the csauser user (for example, `.bash_profile` (Red Hat Enterprise Linux)), add the following:

    ```
    export CSA_HOME=/usr/local/hpe/csa
    export JAVA_HOME=<csa_jre>$CSA_JRE_HOME
    ```

    where `<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed.
33. `. ./.bash_profile` (Red Hat Enterprise Linux)
34. Create an CSA service and HPE Marketplace Portal service to start and stop the CSA and Marketplace Portal processes.
    a. Log on as the root user.
    b. Go to the directory in which CSA is installed. For example:

    ```
    cd /usr/local/hpe/csa
    ```

    c. Copy the `csa` and `mpp` scripts to the `/etc/init.d` directory. Enter the following:

    ```
    cp ./scripts/csa /etc/init.d
    cp ./scripts/mpp /etc/init.d
    ```

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

    ```
    chmod 755 /etc/init.d/csa
    chmod 755 /etc/init.d/mpp
    ```

    e. Log off as the root user.
35. Log on as the csauser and start the CSA and HPE Marketplace Portal services. Enter the following:

    ```
    service csa start
    service mpp start
    ```
36. As csauser, restart the HPE Operations Orchestration Central service. Enter the following:

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

Restarting the CSA Service:

The CSA service must be running in order to access the Cloud Service Management Console. You can start this service by running the `service csa start` command . You can restart this service by

running the `service csa restart` command . You can stop the service by running the `service csa stop` command . You can check the status of the service by running the `service csa status` command.

The HPE Marketplace Portal service must be running in order to access the Marketplace Portal. You can start this service by running the `service mpp start` command . You can restart this service by running the `service mpp restart` command . You can stop the service by running the `service mpp stop` command . You can check the status of the service by running the `service mpp status` command.

The HPE Operations Orchestration Central service must be running in order to access Operations Orchestration Central. You can start this service by running the `/usr/local/hpe/csa/OO/central/bin/central start` command. You can stop this service by running the `/usr/local/hpe/csa/OO/central/bin/central stop` command.

Install Cloud Service Automation with Remote MPP for Windows

The following installation steps are for installing a remote instance of Marketplace Portal and CSA on Windows:

> **Note:** Installation log files are written to the `%CSA_HOME%\_CSA_4_80_0_installation\Logs\` directory.

> **Caution:** The memory requirements for any CSA installation are as follows:
>
> - A CSA installation with the External Operations Orchestration option requires a minimum of 4.5 GB *available* RAM.
> - A CSA installation with the Embedded Operations Orchestration option requires a minimum of 6 GB *available* RAM.
> - It is strongly recommended that you install CSA on a system with *at least* 16 GB RAM.
>
> For a complete listing of resource requirements and compatibility information, see the *Cloud Service Automation System and Software Support Matrix* for the relevant product release.

To install a remote instance of the Marketplace Portal, 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.zip` file.
   a. Navigate to the directory to which the files have been extracted.
   b. Run the `setup.bat` installation file.

   > **Note:** A command window (which will display until the script has completed) and a dialog that shows the progress of the installation preparation are displayed. Do not close either window.
   >
   > The installation preparation progress dialog disappears after the installation preparation has completed.
3. On the Introduction screen, read the information and click **Next**.
4. Read the license agreement and select **I accept the terms of the License Agreement**. Click

Next to continue with the installation.

If the following error message displays:

Another version of CSA is configured in the registry. However, CSA has been uninstalled (the CSA installation directory *%CSA_HOME%* does not exist). You must exit the installer and delete the entry in the registry before installing CSA. See the *Cloud Service Automation Installation Guide* for more information about deleting the registry entry.

Exit the installer. Locate the `C:\Program Files\Zero G Registry\.com.zerog.registry.xml` file (you may need to show hidden files), make a backup copy, delete all CSA entries from the `.com.zerog.registry.xml` file, and restart the installer.

5. Select **Marketplace Portal** and click **Next**.

   Selecting **CSA and Marketplace Portal** installs the entire CSA application, including the Cloud Service Management Console, Identity Management component, and Marketplace Portal, on the system.

   Selecting **Marketplace Portal** installs only the Marketplace Portal on the system.

   If you want to install CSA and the Marketplace Portal, go to the top of this document and click **Change** to change the selections you made to create this document. The tasks to install only the Marketplace Portal are different from the tasks to install both CSA and the Marketplace Portal.

6. Choose a location in which to install the Marketplace Portal and click **Next** (`CSA_HOME` is set to this location).

   The default location is `C:\Program Files\HPE\CSA`.

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

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

7. Define the instance on which the CSA is installed and the location of the CSA certificate that was copied to the local system. Enter the following information and click **Next**.

Field Name	Description
CSA Host	The **fully-qualified domain name** of the system on which CSA is installed.

Field Name	Description
CSA Port	The port number used to communicate with CSA.
CSA Certificate	The name and location of the CSA certificate file that was copied from the CSA system to the local system.

8. From the Hostname Configuration screen, enter the **fully-qualified domain name** of this system, the one on which you are installing the Marketplace Portal, and click **Next**.
9. Review your selections and click **Install** to complete the installation.
10. Click **Done** to exit the installer.
11. Verify that the HPE Marketplace Portal service has started by navigating to **Control Panel > Administrative Tools > Services**. If the service has not started, right-click on the service and select **Start**.

    The HPE Marketplace Portal service must be running in order to access the Marketplace Portal.

To start, stop, and restart the HPE Marketplace Portal service, navigate to **Control Panel > Administrative Tools > Services**, right-click on the HPE Marketplace Portal service, and select the desired action.

Install Cloud Service Automation with Remote MPP for Linux

The following installation steps are for installing a remote instance of the Marketplace Portal and CSA on Linux:

> **Note:** Installation log files are written to the `$CSA_HOME/_CSA_4_80_0_installation/Logs/` directory and are named `csa_*.txt`.

> **Caution:** The memory requirements for any CSA installation are as follows:
>
> - A CSA installation with the External Operations Orchestration option requires a minimum of 4.5 GB *available* RAM.
> - A CSA installation with the Embedded Operations Orchestration option requires a minimum of 6 GB *available* RAM.
> - It is strongly recommended that you install CSA on a system with *at least* 16 GB RAM.
>
> For a complete listing of resource requirements and compatibility information, see the *Cloud Service Automation System and Software Support Matrix* for the relevant product release.

To install HPE Cloud Service Automation (CSA), complete the following steps:

1. Log on to the system as the root user.
2. Install the unzip utility if it is not already installed and enter the following:

   ```
   apt-get install unzip
   ```

3. Create an installation directory for CSA (this document assumes that you will install the product in `/usr/local/hpe/csa` and all examples used in this document are based on this assumption). Enter the following:

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

4. For the installation directory, set the owner to csauser and the group to csagrp. Enter the following:

   ```
   chown -R csauser:csagrp /usr/local/hpe/csa
   ```

5. Log off as the root user and log on as the csauser.
6. Copy the CSA installation file (`setup.bin`) to the system and go to the directory in which it has been copied.

7. Verify that `setup.bin` is owned bythe csauser and csauser has full permissions to the file. If necessary, do the following:
   a. Log on as the root user
   b. Enter the following commands:

      ```
      chown csauser setup.bin
      chmod u+rwx setup.bin
      ```

   c. Log off as the root user and log on as csauser.
8. Run the `setup.bin` installation file (as the csauser).

   > **Note:** You must run `setup.bin` as the csauser. If you install CSA as another user, you may not be able to run CSA.

   As the csauser, enter `./setup.bin`
9. Read the **Introduction** and click **enter** to continue with the installation.
10. Read the license agreement. Click **enter** to scroll through the entire agreement.
11. Select **Y** and **enter** to accept the license agreement and continue with the installation. Select **N** and **enter** to exit the installation.

    If the following error message displays:

    Another version of CSA is configured in the registry. However, CSA has been uninstalled (the CSA installation directory *$CSA_HOME* does not exist). You must exit the installer and delete the entry in the registry before installing CSA. See the *Cloud Service Automation Installation Guide* for more information about deleting the registry entry.

    Exit the installer. Locate the `$CSA_HOME/.com.zerog.registry.xml` file, make a backup copy, delete all CSA entries from the `.com.zerog.registry.xml` file, and then restart the installer.
12. Select **Marketplace Portal** and select **Enter**.

    Selecting **CSA and Marketplace Portal** installs the entire CSA application, including the Cloud Service Management Console, Identity Management component, and Marketplace Portal, on the system.

    Selecting **Marketplace Portal** installs only the Marketplace Portal on the system.

    If you want to install CSA and the Marketplace Portal, go to the top of this document and click **Change** to change the selections you made to create this document. The tasks to install only the Marketplace Portal are different from the tasks to install both CSA and the Marketplace Portal.
13. Enter a location in which to install CSA (enter the absolute path to the location) and select **enter**.

Or, select **enter** to accept the default location.

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

> **Note:** If the directory in which you choose to install CSA is not empty, existing content in the directory may be overwritten or deleted when CSA 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. Define the instance on which the CSA is installed and the location of the CSA certificate that was copied to the local system. Enter the following information and select **Enter**.

Field Name	Description
CSA Host	The **fully-qualified domain name** of the system on which CSA is installed.
CSA Port	The port number used to communicate with CSA.
CSA Certificate	The name and location of the CSA certificate file that was copied from the CSA system to the local system.

15. From the **Hostname Configuration** screen, enter the **fully-qualified domain name** of this system, the one on which you are installing the Marketplace Portal, and click **Install** to complete the installation.
16. Review your selections and select **enter** to complete the installation or **ctrl**-**c** to exit the installation.
17. When the installation completes, select **enter** to exit the installer.
18. `export CSA_HOME=/usr/local/hpe/csa`

    Windows: `export JAVA_HOME=<csa_jre>`

    Linux: export JAVA_HOME=*$CSA_JRE_HOME*
    `export PATH=$PATH:/sbin`
19. Create the HPE Marketplace Portal service to start and stop the Marketplace Portal process.
    a. Log on as the root user.
    b. Go to the directory in which the Marketplace Portal is installed. For example:

       `cd /usr/local/hpe/csa`

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

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

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

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

e. Log off as the root user.

20. Log on as the csauser and start the HPE Marketplace Portal service. Enter the following:

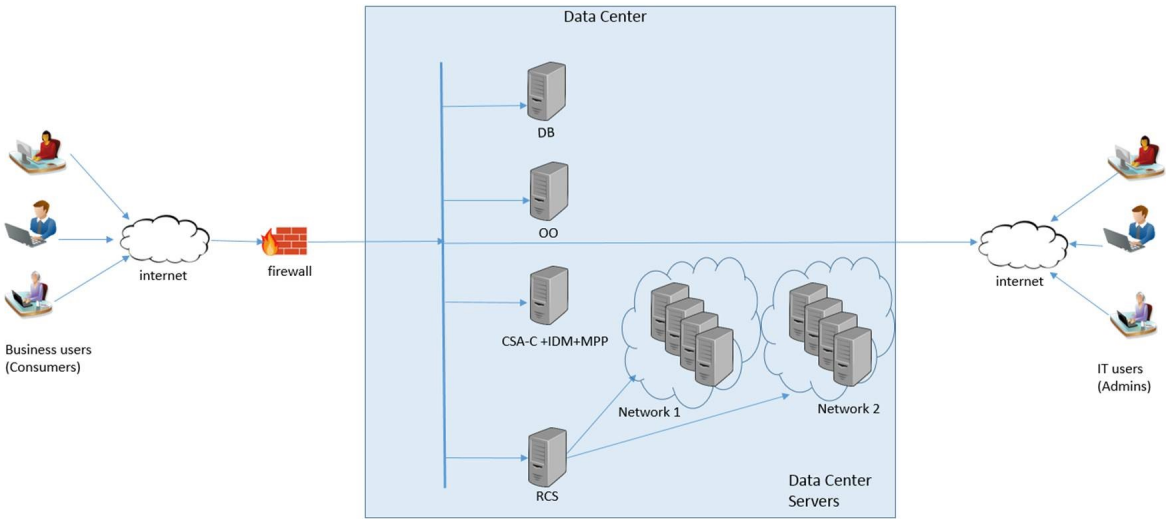
```
service mpp start
```

The HPEMarketplace Portal service must be running in order to access the Marketplace Portal. You can start this service by running the command `service mpp start`. You can restart this service by running the command `service mpp restart`. You can stop the service by running the command `service mpp stop`. You can check the status of the service by running the command `service mpp status`.

Install and Configure Remote Console Service

To provide the remote console access to subscribers for the provisioned servers, CSA remote console service should be installed and configured. A separate installer is provided for remote console service installation. Remote console service is supported only on CentOS platform and is not part of CSA installer.

The following diagram is a sample deployment architecture that demonstrates all the CSA components, which are CSA-Controller (CSA-C), Identity Management component (IDM), Marketplace Portal (MPP), and Remote Console Service (RCS). In this architecture, CSA-C, IDM and MPP are running on a single server and RCS is running on a different server. RCS has network access to MPP and also to the provisioned servers on different networks.



Installation through the Install Script

Prerequisites:

1. A separate machine with CentOS 6.8 installed.
2. Accessible Internet connection.

To install the remote console:

1. Log on as the root user.
2. Update the CentOS with the latest package. To do this, execute the following command:

   ```
   sudo yum update
   ```

   > **Note:** If the `sudo yum update` fails, then check the proxy related environment variables. Make sure the proxy settings are correct before proceeding with the installation.

3. Create the following user credentials:

Steps to configure the user and user credentials	Commands
a. Create a user group `hpegwrcs`	`groupadd hpegwrcs`
b. Create a user `hpegwuser`	`adduser hpegwuser`
c. Add `hpegwuser` to `hpegwrcs` group:	`usermod -aG hpegwrcs hpegwuser`
d. Add `hpegwuser` to `wheel` group	`usermod -aG wheel hpegwuser`
e. Add `hpegwuser` to `root` group	`usermod -aG root hpegwuser`
f. Check the user details (display group details)	`id hpegwuser`
g. Change the ownership of `/home/hpegwuser`	`chown hpegwuser:hpegwrcs \ /home/hpegwuser/`
h. Set the user password	`passwd hpegwuser`

4. Grant permissions to `hpegwuser` user:
   a. Add the following entries to `/etc/sudoers` at the end of the file:

   ```
   hpegwuser ALL=(ALL:ALL) ALL

   hpegwuser ALL=(ALL) NOPASSWD:ALL

   hpegwuser ALL = NOPASSWD: /usr/sbin/service /sbin/start-stop-daemon *

   Defaults env_keep += "HTTP_PROXY HTTPS_PROXY FTP_PROXY"

   Defaults env_keep += "http_proxy https_proxy ftp_proxy"
   ```

5. Log off as the root user.
6. Run the remote console installer:
   a. Log on as `hpegwuser`.
   b. Copy `hpecsarcs_centos-4.8.tar.gz` to `/home/hpegwuser`.

> **Note:** `hpecsarcs_centos-4.8.tar.gz` is available for download on the HPE Live Network at the following location:
>
> In the file repository at: https://hpln.hpe.com/contentoffering/hpe-csa-remote-console-access.

c. Untar `hpecsarcs_centos-4.8.tar.gz` file:

```
tar -xvzf hpecsarcs_centos-4.8.tar.gz
```

This creates a directory `hpecsarcs_centos-4.8`.

7. Install HPE's remote console service:
   a. Go to the directory `/home/hpegwuser/hpecsarcs_centos-4.8/`
   b. Configure the `input.properties` file for the following values:

Input property file parameters

Property: Value	Description
`guacd-port: 4822`	Default Port at which Guacamole server is running (non-configurable).
`rdp-port: 3389`	RDP port number (configurable).
`ssh-port: 22`	SSH port number (configurable).
`vnc-port: 5900`	VNC port number (configurable).
`auth-user: admin`	User name for the Guacamole log in.
`auth-pass:`	Password for the Guacamole log in. This is only for RCS internal use. The password is either blank or plain text. **Note:** This property is: i. **blank** if you do not enter a password manually in the `input.properties` file before executing `install.sh` script. In this case, you will be prompted to enter the password while executing `install.sh` script. This password gets encrypted and saved in the `/home/hpegwuser/.guacamole/guacamole.properties` file. ii. **plain text** if you enter a password manually in the `input.properties` file before executing `install.sh` script. In this case, you will **NOT** be asked to enter the password while executing `install.sh` script. As part of execution this password is encrypted and copied to

Input property file parameters, continued

Property: Value	Description
	/home/hpegwuser/.guacamole/guacamole.properties file. iii. **Weak Password** - If you have manually entered a password in the input.properties file which does not match the password strength criteria, you are prompted to re-enter the password during execution of install.sh script The encryption is done using the PasswordUtil tool available in /home/hpegwuser/hpecsarcs_centos-4.8/webapp/lib. The command for encrypting password is: java -cp passwordUtil-standalone.jar com.hp.csa.security.util.AESHelperWithMarkersStatic "<<sample password>>" where, <<sample password>> is the Guacamole password that you enter before encryption. This password should comply with the following password strength cafeteria: A minimum of 8 characters and at most X characters A minimum of 1 upper case letter (A-Z) A minimum of 1 lower case letter (a-z) A minimum of 1 non-alphanumeric character (For example: #, $, %) A minimum of 1 number (0-9)
socket-timeout: 15000	This is the socket timeout in milliseconds, to connect the socket (configurable).
api-session-timeout: 15	Time in minutes to keep the guacamole session alive (configurable).
mac-timeout: 30	Time in minutes, to keep the HMAC code valid (configurable).

c. Run the following command to grant execute permissions to install.sh script:

```
chmod 777 install.sh
```

d. Run the install.sh script:

```
sudo sh install.sh --file input.properties
```

e. Enter the password for Remote Console Service (RCS) user.

f. Enter **Y** if prompted for any download.

g. Select the option that provides 1.8.0 JVM version.

For example:

```
/usr/lib/jvm/jre-1.8.0-openjdk.x86_64/bin/java
```

8. After the installation is complete, check the service status of `hpercs` and `guacd` by entering the following commands:
   a. `sudo service hpercs status`
   b. `sudo service guacd status`

   If `hpercs` or `guacd` have stopped running, restart them. To do this, enter the following commands:
   a. `sudo service hpercs restart`
   b. `sudo service guacd restart`
9. To reflect `bashrc` changes execute the following command:

```
source ~/.bashrc
```

> **Note:** The guacamole configurable properties are available in `/home/hpegwuser/.guacamole/guacamole.properties` file.

> **Note:** The installer log file is available in the directory `/home/hpegwuser/hpecsarcs_centos-4.8/`
>
> The filename format is `rcs-0.9.9.DD-YY-MON.log`
>
> where: *DD* is the date, *YY* is the last two digits of the year, and *MON* is the month.
>
> For example: `rcs-installer-0.9.9.20-16-Dec.log` and `rcs-Uninstall-0.9.9-20-16-Dec.log`.
>
> The default guacamole URL will not be accessible directly from the browser.

Configure SSL for Remote Console Service

Configuring SSL certificate is a mandatory step for correct functioning of `hpercs` service.

To configure SSL for remote console service:

> **Note:** The location of `$CATALINA_HOME` is `/opt/hpercs`.

1. Log on as the `hpegwuser` user.
2. Create a directory with the name `certs` at the location `$CATALINA_HOME/conf` and change the directory to `certs`:

   ```
   sudo mkdir certs

   cd certs
   ```

3. Generate `Keystore` using `keytool`.
   a. Create a self-signed certificate by typing the following command (do not use copy and paste to duplicate the command):

   ```
   sudo $JAVA_HOME/jre/bin/keytool -genkey -alias guacamole -keyalg RSA \

   -validity 365 -keystore rcs.keystore
   ```

   > **Note:** If there are problems encountered due to incorrect Java path, execute the following commands:
   >
   > - Set the correct `JAVA_HOME` using the following commands:
   >
   >   ```
   >   export JAVA_HOME=`readlink -f /usr/bin/java | sed
   >   "s:/jre/bin/java::"`
   >
   >   export PATH="$PATH:$JAVA_HOME/bin"
   >   ```
   >
   > - Set the correct `CATALINA_HOME` using the command:
   >
   >   ```
   >   export CATALINA_HOME="/opt/hpercs"
   >   ```

   > **Note:** The certificate is valid for a default period of 90 days. To customize the validity period use the following command:
   >
   > ```
   > validity <number of days>
   > ```

   b. Enter the following details:
      i. Enter the keystore password. The password must be at least 6 characters in length.
      ii. Enter the first and last name details. It can be either an ipaddress or a domainname.
      iii. Enter the name of organizational unit. For example, CSA..
      iv. Enter the name of organization. For example, HPCSA.
      v. Enter the name of your City or Locality. For example, BLR.
      vi. Enter the name of your State or Province. For example, KA.
      vii. Enter the two-letter country code for this unit. For example, IN.

c. You are prompted to confirm if the entered details are correct. Verify and enter **Yes**.

4. Edit the `hpercs` configuration file:
   a. Stop `hpercs` service. To do this, execute the following command:

      ```
      sudo service hpercs stop
      ```

   b. Edit `$CATALINA_HOME/conf/server.xml`
   c. Configure SSL HTTP/1.1 Connector on port 8443.

      To do this, identify the SSL Connector element in the `server.xml` file.

      For example:

      ```
      <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
      maxThreads="150" scheme="https" secure="true"
      keystoreFile="${catalina.home}/conf/certs/rcs.keystore"
      keystorePass="changeit"
      clientAuth="false" sslProtocol="TLS" />
      ```

      where,

      `keystorePass` is the password you assigned to your keystore using the "`keytool`" command.

      `keystoreFile` is location of the generated keystore file. The location of generated keystore file is `${catalina.home}/conf/certs/rcs.keystore`.

   d. Restart `hpercs` service. To do this, execute the following command:

      ```
      sudo service hpercs restart
      ```

> **Note:** The remote console can be opened from the Marketplace Portal. If you encounter a browser certificate error while accessing remote console, then execute the following step.

5. Install the `HPE CSA Remote Console Service Self-Signed certificate`.
   a. **In Internet Explorer**
      i. Click the **Certificate Error** area next to the browsers address bar.
      ii. In the **Certificate Invalid** window displayed, click the **View certificates** link.
      iii. In the **Certificate** window displayed, click **Install Certificate** and then click **Next**.
      iv. Select **Place all certificates in the following store**, then click **Browse**.
      v. Select **Show physical stores** check box.
      vi. Select **Trusted Root Certificate Authorities –> Local Computer** and click **OK**.

vii. Click **Next -> Finish -> OK**

viii. Restart the Internet Explorer.

b. **In Google Chrome**

Export the certificate in to the browser, to do this:

i. Open Google Chrome.

ii. On the site that you want to add, right-click the *red lock icon* in the address bar.

iii. From the drop-down click the **Details** link. **Security Overview** pane opens.

iv. Click View Certificate. The **Certificate** window opens.

v. Click the **Details** tab.

vi. Click **Copy to File...** button. It opens the **Certificate Export Wizard**.

vii. Click Next.

viii. Select **DER encoded binary X.509 (.CER)** export file format.

ix. Click **Next**.

x. Click **Browse...**and save the file to your computer and name it.

xi. Click **Next**, then click **Finish**

Import certificate, to do this:

i. Open Google Chrome. Open the menu at the top right corner and select **Settings**.

ii. Scroll down and click **Show advanced settings…**.

iii. Go to **HTTP/SSL** and click **Manage certificates**.

iv. Click **Trusted Root Certification Authorities** tab.

v. Click **Import** to start the **Certificate Import Wizard**.

vi. Click **Next**.

vii. **Browse** to your Exported certificate file and click **Next**.

viii. Select **Place all certificates in the following store**.

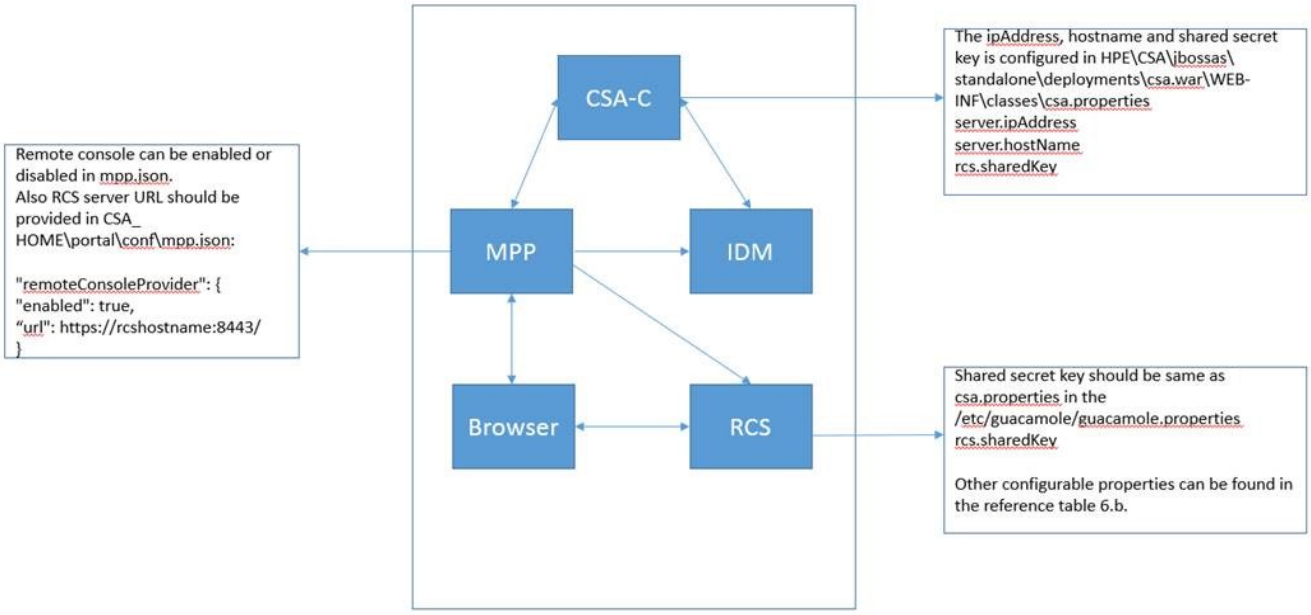
ix. Click **Next**, then click **Finish**.

Restart Chrome, to do this:

i. Type `chrome://restart` in the address bar.

ii. Press **Enter**.

The following block diagram shows the remote console service configuration based on components:



Configure Remote Console Service in CSA

To configure the remote console service in CSA *server*:

> **Note:** These configuration steps should be followed for all master and slave CSA nodes if CSA is running in a clustered environment.

1. Stop the CSA service `HPE Cloud Service Automation`. To do this:

   On Windows:

   Go to **Control Panel > Administrative Tools > Services**, right-click on the `HPE Cloud Service Automation`, and select **Stop**.

   On Linux:

   Run the command: `service csa stop`

2. Configure the following properties available in `HPE\CSA\jboss-`

as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties file:

Property	Description
server.hostName	Map IP Address (example: ip, ipaddr) field name used at the time of creating customized designs.
server.ipAddress	Map IP Address (example: ip, ipaddr) field name used at the time of creating customized designs.
rcs.sharedKey	Copy the value of rcs.sharedKey present in the /home/hpegwuser/.guacamole/guacamole.properties file from the remote console service server.

3. Start the CSA service HPE Cloud Service Automation. To do this:

   On Windows:

   Go to **Control Panel > Administrative Tools > Services**, right-click on the HPE Cloud Service Automation, and select **Start**.

   On Linux:

   Run the command: service csa start

Modify Remote Console Service default configurations

You can modify the default configuration for Remote Console Service. To do this, modify the following file:

/home/hpegwuser/.guacamole/guacamole.properties

Guacamole.properties file parameters

Property: Value	Description
guacd-port: 4822	Default Port at which Guacamole server is running (non-configurable).
rdp-port: 3389	RDP port number (configurable).
ssh-port: 22	SSH port number (configurable).

Guacamole.properties file parameters, continued

Property: Value	Description
`vnc-port: 5900`	VNC port number (configurable).
`auth-user: admin`	User name for the Guacamole log in.
`auth-pass:`	Password for the Guacamole log in. This is only for RCS internal use. The password is either blank or plain text. **Note:** This property is: 1. **blank** if you do not enter a password manually in the `input.properties` file before executing `install.sh` script. In this case, you will be prompted to enter the password while executing `install.sh` script. This password gets encrypted and saved in the `/home/hpegwuser/.guacamole/guacamole.properties` file. 2. **plain text** if you enter a password manually in the `input.properties` file before executing `install.sh` script. In this case, you will **NOT** be asked to enter the password while executing `install.sh` script. As part of execution this password is encrypted and copied to `/home/hpegwuser/.guacamole/guacamole.properties` file. 3. **Weak Password** - If you have manually entered a password in the `input.properties` file which does not match the password strength criteria, you are prompted to re-enter the password during execution of `install.sh` script The encryption is done using the `PasswordUtil` tool available in `/home/hpegwuser/hpecsarcs_centos-4.8/webapp/lib`. The command for encrypting password is: `java -cp passwordUtil-standalone.jar com.hp.csa.security.util.AESHelperWithMarkersStatic "<<sample password>>"` where, `<<sample password>>` is the Guacamole password that you enter before encryption. This password should comply with the following password strength cafeteria: A minimum of 8 characters and at most X characters A minimum of 1 upper case letter (A-Z) A minimum of 1 lower case letter (a-z) A minimum of 1 non-alphanumeric character (For example: #, $, %) A minimum of 1 number (0-9)

Guacamole.properties file parameters, continued

Property: Value	Description
`rcs.sharedKey`	Secret shared key. This is a shared key for secured communication between remote console service and Marketplace Portal. This key should be copied to `csa.properties` file on CSA Controller. **For Example** `rcs.sharedKey=ENC (e008rxEzmK/txtGmWGpaPFiaELkAt8GhSmRoknRCcsylDbOcjwh7L34uF9e//RjM9LatyOoYU6E=)`
`socket-timeout: 15000`	This is the socket timeout in milliseconds, to connect the socket (configurable).
`api-session-timeout: 15`	Time in minutes to keep the guacamole session alive (configurable).
`mac-timeout: 30`	Time in minutes, to keep the HMAC code valid (configurable).
`guacd-url`	This is the RCS URL. Example: https://<fqdn>:<port>

Restart `hpercs` and `guacd` services. To do this, execute the following commands:

1. `sudo service hpercs restart`
2. `sudo service guacd restart`

Modify Marketplace Portal default configuration for remote console service

To configure the remote console service in *Marketplace Portal*:

> **Note:** If there are multiple instances of Marketplace Portal installed. Then all the installed Marketplace Portal instances should be configured for remote console service.

1. Stop the Marketplace Portal service . To do this:

   On Windows:

Go to **Control Panel > Administrative Tools > Services**, right-click on the `hpemarketplaceportal`, and select **Stop**.

On Linux:

Run the command: `service mpp stop`

2. Configure the following properties available in `mpp.json` file at the location `CSA_HOME\portal\conf\mpp.json`:

> **Note:** Only the following properties should be configured in the `mpp.json` file.

Property	Description
`enabled`	This property is used to enable or disable the remote console service. When set to "true" it enables the remote console service. By default it is enabled, that is, it is set to "true". When this property is enabled, the console button is displayed for the server component.
`url`	This is the remote console service URL. Example: https://<rcsHost>:<rcsPort>

For example:

```
"remoteConsoleProvider": {
"enabled": true,
"url": "<rcs url>:<rcs port>" ,
}
```

3. Start the Marketplace Portal service. To do this:

On Windows:

Go to **Control Panel > Administrative Tools > Services**, right-click on the `hpemarketplaceportal`, and select **Start**.

On Linux:

Run the command: `service mpp start`

> **Note:** After the installation and configuration of remote console service, the open console button will be available for all the server components on the Service details page on the Marketplace Portal for all subscriptions.

Post Install Configuration

Enable RDP (Mandatory for Connect RDP option)

To connect to an RDP system from remote console you need to:

1. Click Window's **Start** button.
2. Right-click **This PC/Computer** icon and select **Properties**.
3. Select **Advanced system settings**, the **System Properties** window opens.
4. Go to **Remote** tab.
5. Un-check **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**.
6. Click **OK**.

> **Note:** Remote console service will not work with IPv6 addresses for RDP connections.

Uninstall Remote Console Service

To uninstall remote console service:

1. Change directory to `/home/hpegwuser/hpecsarcs_centos-4.8`:

   ```
   cd /home/hpegwuser/hpecsarcs_centos-4.8
   ```

2. Run the following command to grant execute permissions to `uninstall.sh` script:

   ```
   chmod 777 uninstall.sh
   ```

3. Run the uninstaller script:

   ```
   sudo sh uninstall.sh
   ```

> **Note:** The uninstall script does not remove all the dependent libraries.

> It is mandatory to run remote console service uninstaller before running remote console service installer again.

Secure the Marketplace Portal

For security reasons, the Marketplace Portal file system must be protected by the operating system. Do the following:

Windows:

1. Open an elevated command prompt (a command prompt that is run as the administrator). For example, navigate to **All Programs > Accessories**. Right-click on **Command Prompt** and select **Run as administrator**.
2. From the elevated command prompt, run the following command:

   ```
   attrib +s +h "%CSA_HOME%\portal" /S /D /L
   ```

   where
   `CSA_HOME` is the directory in which CSA is installed
3. Restart the CSA and HPE Marketplace Portal services.
   For example, navigate to **Start > Administrative Tools > Services**. Right-click the service and select **Restart**

Linux:

1. Log on as the root user.
2. Run the following commands:

   ```
   chown csauser:csagrp $CSA_HOME/portal
   chmod 700 $CSA_HOME/portal
   ```

   where csauser and csagrp are the user and group you configured for CSA when you installed CSA and
   `CSA_HOME` is the directory in which CSA is installed
3. Log off as root and log on as csauser.
4. Restart the csa and mpp services by running the following commands:

   ```
   service csa restart
   service mpp restart
   ```

Update and Redeploy the Service Manager Base Content Pack

Update and redeploy the `oo10-sm-cp-1.0.3.jar` base content pack. If you deployed an earlier version of the Service Manager base content pack, you must do the following (if this is a fresh installation of Operations Orchestration and you did not deploy an earlier version of the Service Manager base content pack, you do not have to complete these steps):

1. Stop the Operations Orchestration services:

   Windows:

   a. On the server that hosts Operations Orchestration, navigate to **Start** > **Administrative Tools** > **Services**.

   b. Right-click the HPE Operations Orchestration Central service and select **Stop**.

   c. If you installed the Remote Action Server (RAS), on all RAS systems (including localhost), navigate to **Start** > **Administrative Tools** > **Services**.

   d. Right-click the Operations Orchestration RAS service and select **Stop**.

   Linux:

   a. On the server that hosts Operations Orchestration, run the following command: `<HPEOOinstallation>/central/bin/central stop`

      For example, `/usr/local/hpe/csa/OO/central/bin/central stop`

   b. If you installed the Remote Action Server (RAS), on all RAS systems (including localhost), run the following command: `<HPEOOinstallation>/ras/bin/ras stop`

      For example,

      `/usr/local/hpe/csa/OO/ras/bin/ras stop`

2. Clear the Operations Orchestration Central cache by deleting the following folder:

   `<HPEOOinstallation>\central\var\cache`

   For example,

   Windows: `C:\Program Files\HPE\HP Operations Orchestration\central\var\cache`

   Linux: `/usr/local/hpe/csa/oo/central/var/cache`

3. If RAS is installed, clear the RAS artifact cache by deleting the following folder (on all RAS systems, including localhost):

   `<HPEOOinstallation>\ras\var\cache`

   For example,

   Windows: `C:\Program Files\HPE\HPE Operations Orchestration\ras\var\cache`

   Linux: `/usr/local/hpe/csa/oo/ras/var/cache`

4. Run the following SQL command against the Operations Orchestration database:

   ```
   DELETE from OO_ARTIFACTS where NAME =
   'org/apache/ws/security/wss4j/1.5.7/wss4j-1.5.7.pom' or NAME =
   'org/apache/ws/security/wss4j/1.5.7/wss4j-1.5.7.jar'
   ```

5. Start the Operations Orchestration services:

   Windows:

   a. On the server that hosts Operations Orchestration, navigate to **Start** > **Administrative Tools** > **Services**.

   b. Right-click the HPE Operations Orchestration Central service and select **Start**.

   c. If you installed the Remote Action Server (RAS), on all RAS systems (including localhost), navigate to **Start** > **Administrative Tools** > **Services**.

   d. Right-click the Operations Orchestration RAS service and select **Start**.

   Linux:

   a. On the server that hosts Operations Orchestration, run the following command: `<HPEOOinstallation>/central/bin/central start`

      For example, `/usr/local/hpe/csa/OO/central/bin/central start`

   b. If you installed the Remote Action Server (RAS), on all RAS systems (including localhost), run the following command: `<HPEOOinstallation>/ras/bin/ras start`

      For example, `/usr/local/hpe/csa/OO/ras/bin/ras start`

6. Redeploy the `oo10-sm-cp-1.0.3.jar` base content pack:

   a. Log on to Operations Orchestration Central and click **Content Management**.

   b. Click the **Content Packs** tab.

   c. Click the **Deploy New Content** icon.

d. In the Deploy New Content dialog, in the upper left corner, click the **+** (Add files for deployment) icon.

e. Navigate to the `CSA_HOME\oo\ooContentPack` directory and select **oo10-sm-cp-1.0.3.jar**.

f. Click **Deploy**.

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

g. Click **Close**.

What's next?

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

- Launch the Cloud Service Management Console (type the following URL in a supported Web browser: `https://<csahostname>:8444/csa`) and log on using the out-of-the-box user (admin) and password (cloud).
- Launch the default Marketplace Portal (type the following URL in a supported Web browser: `https://<csahostname>:8444/mpp`) and log on using the out-of-the-box user (consumer) and password (cloud).

Global Search

> **Note**: Global Search (i.e. elasticsearch) is turned on by default in CSA 4.80. After installing CSA and creating CSA content (Create Offerings, Services, and so on.) the global search window should be visible and functioning properly.

Install a new Operations Orchestration license

After 90 days, the Operations Orchestration license that is packaged with CSA expires and prompts you to install a new license.

You must contact HPE Customer Support to acquire the new license. After HPE Customer Support provides you with a new Operations Orchestration license, download it to your system.

To install your new Operations Orchestration license:

1. Log on to Operations Orchestration.
2. Click System Configuration on the left pane.
3. Click the System Settings tab.

4. On the License tab, click the Install License button.
5. You are prompted to select the license file. Browse to the path in which you downloaded and installed the license file and select it.
6. Click OK.

The Operations Orchestration license is now installed.

Configure CSA

To complete the configuration of CSA, see the following documents:

- *Cloud Service Automation Configuration Guide*: The configuration guide describes the process for preparing LDAP for the Cloud Service Management Console and for consumer organizations, requesting software licenses, configuring secure connections, customizing the Cloud Service Management Console, configuring CSA to be compliant with FIPS 140-2, and performing other CSA customizations. The configuration guide also describes the process of how to import the sample Operations Orchestration flows included with CSA.
- *Cloud Service Automation Cluster Configuration Guide Using a Load Balancer*: The cluster configuration guide describes how to configure the nodes in your clustered environment if you are using an Apache Web server or load balancer.
- *CSA/Codar Content at a Glance Guide*: This guide describes how to install and configure resource providers (such as Matrix OE, VMware vCenter, SiteScope, Universal CMDB, and Server Automation), how to deploy the sample Operations Orchestration flows included with CSA, how to deploy the sample resource offerings and service designs included with CSA that target these resource providers, and includes additional documentation on each of the out-of-the-box resource offerings and service designs. If you installed the additional provider integration service designs, components, and content during installation, the sample Operations Orchestration flows, resource offerings, and service designs have been deployed.

When you have completed the initial installation and configuration of the Marketplace Portal, you can begin familiarizing yourself with the capabilities of the Marketplace Portal.

Launch the default Marketplace Portal (type the following URL in a supported Web browser: `https://<csahostname>:8444/mpp`) and log on using the out-of-the-box user (consumer) and password (cloud).

For more information about the Marketplace Portal, see the online help.

Checksum-checker Tool

CSA provides a checksum-checker tool to verify the authenticity of CSA code files. This tool and a jarsigner tool that is included in Java JDK (but not in Java JRE) can be used to validate your CSA installation. The tool may uncover some modifications to CSA code files that may be malicious. It may be useful to run it after a breach is detected and mitigated to ensure that CSA code files has not been maliciously modified during a breach, or it can be useful for ordinary integrity check.

The tool is used post-installation.

Before Running the Checksum-checker Tool

Within your CSA installation, run a command line (Windows) or a shell (Linux) and navigate to the `CSA_HOME\Tools\Security` directory.

The first step is to verify that the checksum checker is signed. Execute the jarsigner command (available from Java JDK) in the specified directory:

```
jarsigner -verify checksum-checker.jar
```

You should get a response:

```
jar verified.
```

Once you verify the checksum-checker, you can use the tool to verify the rest of the CSA installation.

For complete assurance, you can run it with -verbose and -certs arguments to see if code signing certificate comes from HPE.

Once you verify the checksum-checker, you can use the tool to verify the rest of the CSA installation.

Using Checksum-checker

The tool can be used after mitigating potential security breach or just for plain file integrity validation.

To use the checksum-checker, follow these Steps (for plain file integrity validation without presence of adversary, you can skip directly to step 4):

1. Disconnect the systems from the network, to verify if the attacker has modified the CSA installation;
2. Check your OS to see if it is negatively affected;
3. Check the java files to verify if the Java is modified in any way;
4. Check checksum-checker with jarsigner (as described above);
5. Check to see if CSA code is modified via the checksum-checker. You can do this using the following command in the `CSA_HOME\Tools\Security` directory:

   ```
   java -jar checksum-checker.jar
   ```

   The tool will run through the files and give you the list of validated files. At the end of list there is a summary of files that did not pass the check.

   For example, let's see what would the checksum-checker.jar will report if the `provider-tool` file (in the `CSA_HOME\Tools\ProviderTool` directory) has been modified.

   The checksum-checker.jar will provide a message with the name of the file that has unexpected checksum at the end of its output like this:

   ```
   Files with wrong checksums:

   Tools/ProviderTool/provider-tool.jar
   ```

   > **Note:** The checksum-checker tool can only verify CSA code files, not configuration files. It verifies only known files and ignores unknown ones. Checksum-checker will report wrong checksums for CSA applied hotfixes; it can only validate full version installations, patch releases, and version updates within CSA installations. The checksum checker uses SHA-256 algorithm for checksums.

   The `checksum-checker.jar` can also run from different directory than `CSA_HOME\Tools\Security`, if the argument `--installdir` followed by the location of `CSA_HOME` directory is specified.

Appendix A: Install an Instance of the Marketplace Portal on a Remote System

This section describes how to install the Marketplace Portal on a remote system, a system that is not the same system on which the Cloud Service Management Console is installed. The remote system must meet the same system requirements for CSA.

See the *Cloud Service Automation System and Software Support Matrix*.
Guides are available on the HPE Software Support web site at: https://softwaresupport.hpe.com (this site requires a Passport ID). Select **Dashboards > Manuals**.

Complete the following tasks to install and configure the Marketplace Portal on a remote system:

- Copy the CSA certificate to the remote system.
- Configure a CSA Group and User.
- Install a JRE.
- Install CSA.
- Remove unneeded .war files.
- Configure the Marketplace Portal.
- Start the HPE Marketplace Portal service.
- Launch the Marketplace Portal.

> **Note:** In the following instructions, **Windows:** `%CSA_HOME%` and **Linux:** `$CSA_HOME` represent the directory in which the Marketplace Portal is installed.

Copy the CSA Certificate

From the system on which CSA is installed, copy the CSA certificate to the system on which the remote instance of the Marketplace Portal will be installed.

On the system on which CSA is installed, the CSA certificate is located in:

Windows: `%CSA_HOME%\jboss-as\standalone\configuration\jboss.crt`

Linux: `$CSA_HOME/jboss-as/standalone/configuration/jboss.crt`.

Copy this file to the system on which you are installing the remote instance of the Marketplace Portal. Remember the name and location to which you have copied this certificate as you will be asked for this information when you install the remote instance of the Marketplace Portal.

This file is needed for TLS verification which, by default, is enabled for the Marketplace Portal.

Install CSA for MPP for Windows

Click on the link for information in this guide on how to install CSA with Remote MPP for Windows.

Install CSA for MPP for Linux

Click on the link for information in this guide on how to install CSA with Remote MPP for Linux.

Secure the Marketplace Portal

For security reasons, the Marketplace Portal file system must be protected by the operating system. Do the following:

Windows:

1. Open an elevated command prompt (a command prompt that is run as the administrator). For example, navigate to **All Programs > Accessories**. Right-click on **Command Prompt** and select **Run as administrator**.
2. From the elevated command prompt, run the following command:

   ```
   attrib +s +h "%CSA_HOME%\portal" /S /D /L
   ```

   where
   `CSA_HOME` is the directory in which CSA is installed
3. Restart the CSA and HPE Marketplace Portal services.
   For example, navigate to **Start > Administrative Tools > Services**. Right-click the service and select **Restart**

Linux:

1. Log on as the root user.
2. Run the following commands:

   ```
   chown csauser:csagrp $CSA_HOME/portal
   chmod 700 $CSA_HOME/portal
   ```

   where csauser and csagrp are the user and group you configured for CSA when you installed CSA and
   `CSA_HOME` is the directory in which CSA is installed
3. Log off as root and log on as csauser.
4. Restart the csa and mpp services by running the following commands:

   ```
   service csa restart
   service mpp restart
   ```

Update the Marketplace Portal in the Cloud Service Management Console

The URL to launch the Marketplace Portal is displayed in the Cloud Service Management Console. Edit the `csa.properties` file to update this URL. Do the following:

1. On the system on which CSA and the Cloud Service Management Console are installed:
   - **Windows:** edit the `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file.
   - **Linux:** edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file.
2. Update the `csa.subscriber.portal.url` property value. Set the hostname to the fully-qualified domain name or IP address of the system on which the Marketplace Portal is remotely installed.
3. Save and exit the file.
4. Restart CSA.

   To restart CSA on Windows, complete the following steps:

   a. If you have configured CSA to be FIPS 140-2 compliant, create a CSA encryption keystore password file. The name and location of this file must match the value configured for the `keystorePasswordFile` property in the `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file.

The password file must contain only the following content: `keystorePassword=<CSA encryption keystore password>`

where `<CSA encryption keystore password>` is the CSA encryption keystore password in clear text.

This file is automatically deleted when the CSA service is started.

b. On the server that hosts CSA, navigate to **Start** > **Administrative Tools** > **Services**.

c. If global search is enabled, do the following:

   i. Right-click on the Elasticsearch 1.6.1 service and select **Restart**.

   ii. Wait for a minute for the Elasticsearch 1.6.1 service to restart, then right-click on HPE Search Service and select **Restart**.

   > **Note:** If global search is disabled, skip this step.

d. Right-click on the CSA service and select **Restart**.

e. Right-click on the HPE Marketplace Portal service and select **Restart**.

f. If you installed an embedded Operations Orchestration instance, right-click on the HPE Operations Orchestration Central service and select **Restart**.

To restart CSAon Linux, complete the following steps:

a. On the server that hosts CSA, type the following:

```
service csa restart
service mpp restart
```

b. If you installed an embedded Operations Orchestration instance, type:

```
<embeddedHPEOOinstallation>/central/bin/central stop
<embeddedHPEOOinstallation>/central/bin/central start
```

For example, type:

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

Launch the Marketplace Portal

Launch the default remote instance of a Marketplace Portal

Launch the default remote instance of the Marketplace Portal by typing one of the following URLs in a supported Web browser:

- `https://<csahostname>:8444/mpp`
- `https://<mpphostname>:8089`

where:

- *<csahostname>* is the fully-qualified domain name of the system on which CSA is installed and the URL in the `CSA_HOME\jboss-as\standalone\deployments\mpp.war\index.html` file (on the system on which CSA is installed) has been updated to `https://<mpphostname>:8089`.
- *<mpphostname>* is the fully-qualified domain name of the system on which the Marketplace Portal instance resides.

Examples:

- `https://csa_system.abc.com:8444/mpp`
- `https://mpp_system.abc.com:8089`

The organization associated with the default Marketplace Portal is defined in the `CSA_HOME\portal\conf\mpp.json` file (on the system on which the Marketplace Portal instance resides). By default, this is the sample organization that is installed with CSA (CONSUMER). To modify the organization associated with the default Marketplace Portal, modify the `defaultOrganizationName` property value by setting it to the *<organization_identifier>* of the desired organization, where *<organization_identifier>* is the unique name that CSA assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** menu of the Cloud Service Management Console).

Launch an organization-specific remote instance of a Marketplace Portal

Launch an organization's remote instance of the Marketplace Portal by typing the following URL in a supported Web browser:

`https://<mpphostname>:8089/org/<organization_identifier>`

where:

- *<mpphostname>* is the fully-qualified domain name of the system on which the Marketplace Portal instance resides.
- *<organization_identifier>* is the unique name that CSA assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** menu of the Cloud Service Management Console)

Example:

`https://mpp_system.xyz.com:8089/org/ORGANIZATION_A`

> **Caution:** Do not launch more than one organization-specific Marketplace Portal from the same browser session. For example, if you launch ORGANIZATION_A's Marketplace Portal in a browser, do not open a tab or another window from that browser and launch ORGANIZATION_B's Marketplace Portal. Otherwise, the user who has logged in to the Marketplace Portal launched for ORGANIZATION_A will start to see data for ORGANIZATION_B.
>
> Instead, start a new browser session to launch another organization's Marketplace Portal.

Start, Stop, or Restart the Marketplace Portal on the Remote System

Use the following instructions to start, stop, or restart the Marketplace Portal on the remote system.

Windows:

> **Note:** In Windows, this feature is referred to as the HPE Marketplace Portal service.

To start the HPE Marketplace Portal service, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).
2. Right-click the **HPE Marketplace Portal** service and select **Start**.

To stop the HPE Marketplace Portal service, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).
2. Right-click the **HPE Marketplace Portal** service and select **Stop**.

To restart the HPE Marketplace Portal service, do the following:

1. Navigate to the Services screen (**Control Panel > Administrative Tools > Services**).
2. Right-click the **HPE Marketplace Portal** service and select **Restart**.

Linux:

To stop Marketplace Portal, on the remote system, open a command prompt and type `service mpp stop`.

To restart Marketplace Portal, on the remote system, open a command prompt and type `service mpp restart`.

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 Guide (Cloud Service Automation 4.80)

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!