Cloud Service Automation

Software Version: 4.70

For Microsoft Windows and Linux operating systems

Upgrade Guide

Document Release Date: July 2016
Software Release Date: July 2016

Hewlett Packard Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

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

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

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

Documentation Updates

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

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

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

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

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

Support

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

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

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

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

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

Contents

Overview

The *Cloud Service Automation Upgrade Guide* is a document that provides the information necessary to upgrade your HPE Cloud Service Automation (CSA) solution from version 4.5x or 4.6x to version 4.70, based on the information you supply.

> **Note:** You can only upgrade from CSA version 4.5x or 4.6x to version 4.70. If you are running an earlier version, you must first upgrade to CSA version 4.5x or 4.6x. Refer to the *Cloud Service Automation Upgrade Guide* for CSA version 4.5x or 4.6x for more information on how to upgrade to version 4.5x or 4.6x.

You will need to supply the following information by selecting from the available options within the upgrade:

- CSA version from which to upgrade
- Operating system on which CSA is running
- Database used by CSA
- JRE used by CSA
- Operations Orchestration version with which CSA is integrated
- If CSA is configured to be compliant with FIPS 140-2
- System configuration (upgrading the Cloud Service Management Console or a remote Marketplace Portal)
- Configured Features

For general information about CSA, see the *Cloud Service Automation Concepts Guide*.

For information about the supported components and versions, see the *Cloud Service Automation System and Software Support Matrix* Guide.

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 Upgrade Prerequisites

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

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

- Supported database versions.
- Supported platforms.
- Supported middleware options.
- Recommended integration solutions.

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

> **Note:** It is important to verify that the connected OO instance is running before performing the CSA upgrade.

Upgrade a previous CSA Version

You can upgrade to CSA version 4.70 from the following versions:

CSA 4.50
CSA 4.60

> Note: if you want to upgrade from a version of CSA earlier than 4.5x, you must first upgrade to version 4.5x or 4.6x).

Operating System

The following operating systems are available for the CSA upgrade:

Windows
Linux, Red Hat Enterprise
HPE Linux

For the list of CSA supported operating systems, refer to the *Cloud Service Automation System and Software Support Matrix Guide*.

Database

The following databases are available for the CSA upgrade:

Oracle
Microsoft SQL Server
PostgreSQL

Java Runtime Environment (JRE)

You must select a JRE for the CSA instance to function properly after the upgrade. You can choose from the following:

- OpenJDK JRE
- Oracle JRE

For a list of supported JREs, refer to the *Cloud Service Automation System and Software Support Matrix Guide*.

FIPS 140-2 Compliance

During the upgrade process, the FIPS 140-2 compliance option is detected and upgraded automatically. After the CSA upgrade installer finishes, you can use the *CSA 4.70 FIPS 140-2 Configuration Guide* for further configuration options.

FIPS 140-2 is only supported on Windows using a Microsoft SQL Server database and Oracle JRE.

Global Search

> **Note**: Global Search (i.e. elasticsearch) is enabled by default in CSA 4.70. After upgrading CSA and creating CSA content (Create Offerings, Services, etc.) the global search window should be visible and functioning properly.

Configured Features

These are the current configured features available for the CSA upgrade:

- Cloud Service Management Console: properties
- Cloud Service Management Console: dashboard tile(s)

- Cloud Service Management Console: import large archives
- Cloud Service Management Console: session timeout
- Cloud Service Management Console: title
- Cloud Service Management Console: custom files (dynamic query scripts and custom graphics)
- Cloud Service Management Console: Marketplace Portal redirection
- CSA tools
- CSA database user
- CSA seeded users
- Marketplace Portal themes
- Marketplace Portal widgets
- ArcSight Logger
- Common access card
- Identity Management component
- IPv6
- JBoss password vault
- Oracle RAC
- CA SiteMinder
- Other single sign-on solution

If you want to configure, customize, or use any of these features for the first time, after you have completed the upgrade, refer to one or more of the guides listed below:

> **Caution:** For more information about the listed features, refer to one or more of the following guides:
>
> - *Cloud Service Automation Configuration Guide*
> - *Cloud Service Management Console Help*

- *Cloud Service Automation Content Archive Tool*
- *Cloud Service Automation Provider Configuration Tool*
- *Cloud Service Automation Customizing the Marketplace Portal*
- *Cloud Service Automation Integration with ArcSight Logger*
- *Configuring CSA to Work with Oracle RAC*

Directories Affected by the Upgrade

When CSA is upgraded, new directories (and content) are added and existing directories (and content) are preserved, backed up, or updated.

The following is a list of the affected directories, where

Windows: `%CSA_HOME%`

Or

Linux:`$CSA_HOME`

is the directory in which CSA is installed, for example:

Windows: `C:\Program Files\HPE\CSA`

Or

Linux: `/usr/local/hpe/csa`).

New directories and content (Windows)

- `%CSA_HOME%\_CSA_4_70_0_installation`

Preserved directories and content (Windows)

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

- `%CSA_HOME%\CSAKit`
- `%CSA_HOME%\CSAKit-3.01`
- `%CSA_HOME%\CSAKit-3.10`
- `%CSA_HOME%\CSAKit-3.20`
- `%CSA_HOME%\CSAKit-4.00`
- `%CSA_HOME%\CSAKit-4.01`
- `%CSA_HOME%\CSAKit-4.10`

- %CSA_HOME%\CSAKit-4.20
- %CSA_HOME%\CSAKit-4.50
- %CSA_HOME%\CSAKit-4.60
- %CSA_HOME%_CSA_3_0_0_installation
- %CSA_HOME%_CSA_3_0_1_installation
- %CSA_HOME%_CSA_3_1_0_installation
- %CSA_HOME%_CSA_3_2_0_installation
- %CSA_HOME%_CSA_4_0_0_installation
- %CSA_HOME%_CSA_4_0_1_installation
- %CSA_HOME%_CSA_4_1_0_installation
- %CSA_HOME%_CSA_4_2_0_installation
- %CSA_HOME%_CSA_4_5_0_installation
- %CSA_HOME%_CSA_4_60_0_installation

Backed up directories and content (Windows)

- %CSA_HOME%\node.js
  (backed up to %CSA_HOME%_CSA_4_70_0_installation\Backup\node.js)
- %CSA_HOME%\portal
  (backed up to %CSA_HOME%_CSA_4_70_0_installation\Backup\portal)
- %CSA_HOME%\Tools
  (backed up to %CSA_HOME%_CSA_4_70_0_installation\Backup\Tools\)
- %CSA_HOME%\jboss-as\standalone\deployments*.war
  (backed up to %CSA_HOME%_CSA_4_70_0_installation\Backup\standalone*.war)

New directories and content (Linux)

- $CSA_HOME/_CSA_4_70_0_installation

Preserved directories and content (Linux)

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

- `$CSA_HOME/CSAKit-3.10`
- `$CSA_HOME/CSAKit-3.20`
- `$CSA_HOME/CSAKit-4.00`
- `$CSA_HOME/CSAKit-4.01`
- `$CSA_HOME/CSAKit-4.10`
- `$CSA_HOME/CSAKit-4.20`
- `$CSA_HOME/CSAKit-4.50`
- `$CSA_HOME/CSAKit-4.60`
- `$CSA_HOME/_CSA_3_1_0_installation`
- `$CSA_HOME/_CSA_3_2_0_installation`
- `$CSA_HOME/_CSA_4_0_0_installation`
- `$CSA_HOME/_CSA_4_0_1_installation`
- `$CSA_HOME/_CSA_4_1_0_installation`
- `$CSA_HOME/_CSA_4_2_0_installation`
- `$CSA_HOME/jre` or
  `$CSA_HOME/openjre`

Backed up directories and content (Linux)

- `$CSA_HOME/node.js`
  (backed up to `$CSA_HOME/_CSA_4_70_0_installation/Backup/node.js`)
- `$CSA_HOME/portal`
  (backed up to `$CSA_HOME/_CSA_4_70_0_installation/Backup/portal`)
- `$CSA_HOME/Tools`
  (backed up to `$CSA_HOME/_CSA_4_70_0_installation/Backup/Tools/`)
- `$CSA_HOME/jboss-as/standalone/deployments/*.war`
  (backed up to `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/*.war`)

- >$CSA_HOME/jboss-as/domain/servers/*<server_name>*/deployments/*.war (backed up to $CSA_HOME/_CSA_4_70_0_installation/Backup/domain/*.war)

Customized Files Affected by the Upgrade

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

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

> **Note:** You must recustomize CSA for the features configured, customized, or used prior to the upgrade *only* (complete *only* the tasks for features that were already configured, customized, or used prior to the upgrade).

If you want to configure, customize, or use any of these features for the first time, refer to the following guides for more information:

- *Cloud Service Automation Configuration Guide*
- *Cloud Service Management Console Help*
- *Cloud Service Automation Provider Configuration Tool*
- *Cloud Service Automation Customizing the Marketplace Portal*
- *Cloud Service Automation Integration with ArcSight Logger*
- *Configuring CSA to Work with Oracle RAC*

For files listed by feature and the actions to perform, refer to Recustomize CSA. For a list of customized files that must be manually backed up, refer to Initial Setup.

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

Customized Files Listed by Location

Windows: %CSA_HOME%\jboss-as\bin\

Linux: $CSA_HOME/jboss-as/bin/

File	Action

Windows: standalone.conf.bat **Linux:** standalone.conf	Automatically backed up, manually restore
Windows: vault.bat **Linux:** vault.sh	Automatically restored

Windows: %CSA_HOME%\jboss-as\standalone\configuration\

Linux: $CSA_HOME/jboss-as/standalone/configuration/

File	Action
*.crt	Automatically restored
.keystore	Automatically restored
standalone.xml	Automatically backed up; however, you must manually restore this file (for all features).

Windows: %CSA_HOME%\jboss-as\standalone\deployments\csa.war\custom\

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/custom/

File	Action
message.properties	Automatically restored

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

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/custom-content/

File	Action
index.jsp	Automatically restored

Windows: %CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/

File	Action
config.json	Automatically backed up, manually restore

Windows: %CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\messages\dashboard\

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/messages/dashboard/

File	Action
message.properties	Automatically backed up, manually restore

Windows: %CSA_HOME%\jboss-as\standalone\deployments\csa.war\images\

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/images/

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

Windows: %CSA_HOME%\jboss-as\standalone\deployments\csa.war\propertysources\

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/propertysources/

File	Action
*.jsp	Automatically backed up, manually restore

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

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/

File	Action

applicationContext-security.xml	Automatically backed up, manually restore (for the following feature(s): single sign-on, common access card, CSA seeded users, SiteMinder)
web.xml	Automatically backed up, manually restore (for the following feature(s): Cloud Service Management Console: session timeout , SiteMinder)

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

Linux: $CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/

File	Action
csa.properties	Automatically restored
log4j.properties	Automatically backed up, manually restore to `log4j2.xml`

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

Linux: $CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/

File	Action
csa-consumer-users.properties	Automatically backed up, manually restore
provider-users.properties	Automatically backed up, manually restore
integrationusers.properties	Automatically backed up, manually restore

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

Linux: $CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/

File	Action

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

Windows: %CSA_HOME%\jboss-as\standalone\deployments\mpp.war\

Linux: $CSA_HOME/jboss-as/standalone/deployments/mpp.war/

File	Action
index.html	Automatically restored

Windows: %CSA_HOME%\jboss-as\standalone\log\

Linux: $CSA_HOME/jboss-as/standalone/log/

File	Action
*	Automatically backed up, manually restore

Windows: %CSA_HOME%\portal\conf\

Linux: $CSA_HOME/portal/conf/

File	Action
*	Automatically restored

Windows: %CSA_HOME%\portal\node_modules\mpp-ui\dist\

Linux: $CSA_HOME/portal/node_modules/mpp-ui/dist/

File	Action
*	Automatically backed up, manually restore

Windows: %CSA_HOME%\portal\node_modules\mpp-ui\dist\locales*\

Linux: $CSA_HOME/portal/node_modules/mpp-ui/dist/locales/*/

File	Action
rb.json	Automatically backed up, manually restore

Windows: %CSA_HOME%\Tools\ContentArchiveTool\

Linux: $CSA_HOME/Tools/ContentArchiveTool/

File	Action
config.properties	Automatically backed up, manually restore

Windows: %CSA_HOME%\Tools\DBPurgeTool\

Linux: $CSA_HOME/Tools/DBPurgeTool/

File	Action
config.properties	Automatically backed up, manually restore

Windows: <*csa_jre*>\lib\security\

Linux: <*csa_jre*>/lib/security/

File	Action

cacerts	manually back up, manually restore
java.security	manually back up, manually restore

<user-specified location>

File	Action
*.jar (for dynamic queries)	manually back up, manually restore
*.jsp (custom for the CSA dashboard defined in the configuration file: **Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json`	manually back up, manually restore
keystore file (defined by the certificate-key-file property of the connector attribute in: **Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\standalone.xml` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml`)	manually back up, manually restore

Initial Setup

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

1. The following files must be manually backed up outside of **Windows:** `%CSA_HOME%`; or **Linux:** `$CSA_HOME` (these files are not automatically restored nor backed up by the upgrade installer):
   - **Windows:** `<csa_jre>\lib\security\`; and <*csa_jre*>\lib\security\ .
   - **Linux:** `< csa_jre>/lib/security/cacerts`; and `<csa_jre>/lib/security/java.security` .
   - The keystore file defined by the certificate-key-file property of the connector attribute in **Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\standalone.xml; or` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` if you are not using the default keystore file (the default keystore file, **Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\.keystore`**Linux:** `$CSA_HOME/jboss-as/standalone/configuration/.keystore`, is automatically backed up and restored)
   - Any `.jar` files used by dynamic query scripts.
   - Any Java server page (`.jsp`) files created for the CSA dashboard and saved in a directory within the 4.5x or 4.6x CSA installation but not in a directory whose content is backed up by the upgrade installer (the directory where the Cloud Service Management Console expects to find these files is defined in the **Windows:**`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\;or` **Linux:**`$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` configuration file).
2. You MUST back up all files that you have created, customized, or manually installed in the **Windows:** `%CSA_HOME%`; or **Linux:** `$CSA_HOME` installation directory that are not automatically restored or backed up by the upgrade installer (see Customized Files Affected by the Upgrade for a list of customized files and the action performed during the upgrade). These files should be backed up outside of **Windows:** `%CSA_HOME%`; or **Linux:** `$CSA_HOME`.

   > **Caution:** You MUST back up all files that you have customized with undocumented changes in the **Windows:** `%CSA_HOME%`; or **Linux:**`$CSA_HOME` installation directory. Files with undocumented customizations may not be backed up and must be manually restored.

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

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

> **Note:** If you are not sure what files may have been created, customized, or manually installed in the CSA installation directory, back up the entire **Windows:** `%CSA_HOME%;or` **Linux:** `$CSA_HOME` directory.

> **Caution:** Back up files outside of the CSA installation directory (**Windows:**`%CSA_HOME%`;or **Linux:**`$CSA_HOME`). The existing CSA installation directory and all of its contents are deleted during upgrade.

> **Caution:** Do not remove any directories in **Windows:**`%CSA_HOME%`;or **Linux:** `$CSA_HOME`. Doing so may cause the upgrade to fail.

3. Back up the database.If you have not already done so, back up the database used by CSA4.5x or 4.6x

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

4. If it exists, back up the registry file (outside of **Windows:** `%CSA_HOME%`).;or **Linux:** `$CSA_HOME`). The registry file name and location is:

   Windows: `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`

   Linux: `/home/csauser/.com.zerog.registry.xml` or `/var/.com.zerog.registry.xml`

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

5. If you mounted a file system within the CSA installation directory (for example, within `$CSA_HOME`), you must unmount the file system. The upgrade installer cannot remove the mounted file system during the upgrade.

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

6. The user should ensure that there are no files owned by the `root` in the Operations Orchestration installation folder or in any sub-folder. If there are any such files, you should change the ownership and group to match the ownership and group of the other files. For example, If files with `root` ownership exist, then the upgrade will fail, destroying the Operations Orchestration installation without the possibility to rollback the changes.

7. Create a database instance and user for the embedded Operations Orchestration:

a. **PostgreSQL:** Log in to psql as the postgres user. Enter the following:

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

When prompted, enter the password for the postgres user.

b.
   i. Create a schema for the embedded Operations Orchestration by creating a database user (for example, csaoodbuser).

   ii. Grant the following privileges to the user:

   - CONNECT
   - CREATE VIEW
   - CREATE SEQUENCE
   - CREATE TABLE
   - CREATE PROCEDURE

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

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

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

Create an Operations Orchestration database user (for example, `csaoodbuser`). The Operations Orchestration database user, used by the embedded Operations Orchestration, is required. This user should inherit rights from parent roles and have superuser privileges.

From the psql prompt, enter the following:

```
create role csaoodbuser login password '<csaoodbuser_password>' superuser
inherit;
```

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

c. Work with the database administrator to create a database that is used by the embedded Operations Orchestration. Refer to the *Operations Orchestration Database Guide* for more

information about database requirements for Operations Orchestration.

You must provide the service (global database) name of this database when prompted for the Operations Orchestration database information during the installationupgrade of CSA.

i. Create a new database for Operations Orchestration (for example, csaoodb).

   As of the release date of the CSA software (listed at the top of this guide), the mandatory database options for the Microsoft SQL Server for Operations Orchestration are:

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

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

ii. Create a new user for the Operations Orchestration database (for example, `csaoodbuser`) with the following roles. You can use the existing database login you created for the CSA database (for example, `csadbuser`) or you may create a new database login for the Operations Orchestration database (for example, `csaoodbuser`).

   - db_datareader
   - db_datawriter
   - db_owner

   For example, run the following commands to create the `csaoodbuser` login and user with the specified roles:

   Microsoft SQL Server 2012

```
USE csaoodb;
CREATE LOGIN csaoodbuser WITH PASSWORD = '<csaoodbuser_password>';
CREATE USER csaoodbuser FOR LOGIN csaoodbuser;
ALTER ROLE db_datareader ADD MEMBER csaoodbuser;
ALTER ROLE db_datawriter ADD MEMBER csaoodbuser;
ALTER ROLE db_owner ADD MEMBER csaoodbuser;
```

Create a new database for Operations Orchestration. Grant the Operations Orchestration database user all rights to this database. Refer to the *Operations Orchestration Database Guide* for more information about database requirements for Operations Orchestration.

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

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

```
create database csaoodb with owner=csaoodbuser connection limit=-1;
 grant all on database csaoodb to csaoodbuser;
```

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

d. **PostgreSQL:** Exit psql. From the psql prompt, enter the following:

```
\q
```

You must provide this database instance, username, and password when prompted for the Operations Orchestration database configuration during the upgrade of CSA.

8. Stop CSA:

Before upgrading to CSA 4.70 for Windows, you need navigate to Windows Services and stop the following services:

- Elasticsearch
- HPE CSA
- HPE Marketplace Portal
- HPE Search

Windows:

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

   ```
   jboss-cli.bat --connect command=:shutdown
   ```

3. Close the command prompt.
4. Navigate to **Start** > **Administrative Tools** > **Services**.
5. Right-click on each service and select **Stop**.
6. Close the Control Panel.

Linux:

1. Open a command prompt.
2. Run the following commands:

```
service csa stop
service mpp stop
```

3. Close the command prompt.

5. Verify that you have upgraded to the latest versions of software components required for CSA version 4.70. For example, for some resource providers, you may need to install a hotfix or service pack. See the *Cloud Service Automation System and Software Support Matrix* for the latest versions of software components required for CSA version 4.70.
6. Install Operations Orchestration to the correct version and patch level. See *Cloud Service Automation System and Software Support Matrix* for version requirements, available on the HPE Software Support site
7. If you have upgraded Operations Orchestration, you may need to upgrade your content packs. Refer to the Operations Orchestration release notes for more information.
8. Complete this step for Operations Orchestration 10.50 only.

   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:

   a. On the system running Operations Orchestration, open a command prompt and change to the directory where Operations Orchestration is installed.
   b. 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).

   c. 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.
9. Export the certificate from the truststore of Operations Orchestration as it is needed during the upgrade process. Do the following:

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

b. Run the following command:

Windows: `"<csa_jre>\bin\keytool" -exportcert -keystore "C:\Program Files\Hewlett-Packard\Operations Orchestration\central\var\security\key.store" -alias tomcat -file .\<filename> -storepass changeit`

Linux: `$CSA_JRE_HOME/bin/keytool -exportcert -keystore /usr/local/hpe/csa/OO/central/var/security/key.store -alias tomcat -file ./<filename> -storepass changeit`

> **Note**: <CSA_JRE_HOME> or $CSA_JRE_HOME is the directory in which the JRE that is used by CSA is installed.

where *<filename>* is a unique filename given to the certificate file that will be imported into CSA version 4.70 later during the upgrade process.

1. Close all instances of Windows Explorer and any command prompts, and exit all programs that are running on the system.

> **Caution:** The upgrade will fail if any program is accessing a CSA file or directory.

Run the Upgrade Installer

> **Note:** Upgrade log files are written to the **Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Logs`; or the **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Logs` directory.

> **Note:** In the case of a failed upgrade process using the installer, the installer will detect the failed execution step, terminate the installation process, and provide an explanation in the log file. Rerun the installer; the installer allows you to continue the installation from the last successfully implemented step (prior to the failure point).

Instructions for Windows:

1. Unzip the `setup.zip` file. Go to the directory to which the files have been extracted and run the `setup.exe` upgrade file.
2. On the Introduction screen, read the information and click **Next**.
3. Read the license agreement and select **I accept the terms of the License Agreement**. Click **Next** to continue with the installation.
4. Verify that you want to upgrade to CSA version 4.70 and click **OK**.
5. Select the JRE used by CSA.
   - Use OpenJDK JRE if you want to use the JRE that is installed with CSA version 4.70.
   - Use Oracle JRE if you want to use an Oracle JRE. You must manually export the CSA certificate from the existing truststore and import it into the Oracle JRE truststore.

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

   For a list of supported JREs, refer to the *Cloud Service Automation System and Software Support Matrix* Guide, available on the HPE Software Support WebSite.
6. Install CSA database components onto the database instance to create the CSA database schema, if it does not exist.

   Select **Yes** to install CSA database components and upgrade the CSA database schema, then click **Next**. When you select this option, the CSA service automatically starts when you exit the installer.

   Select **No** if you are using an existing CSA database schema that was created as part of a prior successful installation of CSA version 4.70. When you select this option, you cannot use the installer to deploy sample content, you cannot create a new database schema, and the CSA service does not start when 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 upgrade, the CSA installer will populate the database and migrate the organizations automatically; however, if you selected **No** during the upgrade, you will need to populate the database and migrate organizations manually using CSA tools.

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

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

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

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

Windows:

- `Go to <CSA_HOME>\Tools\SchemaInstallationTool\`
- `Run <JAVA_HOME>\bin\java.exe –jar schema-installation-tool.jar`

Linux:

- `Go to <CSA_HOME>/Tools/SchemaInstallationTool/`
- `Run <JAVA_HOME>/bin/java –jar schema-installation-tool.jar`

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

Windows:

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

Linux:

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

Refer to the end of this section for information on how to start and stop the CSA service.

7. Select the environment in which CSA is running and click **Next**.

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

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

8. Verify that you have stopped the CSA services and click **OK**.
9. Enter the CSA database user password and click **Next**.
10. If you configured a reporting database user, enter the reporting database user and password and click **Next**. If you did not configure a reporting database user, click **Next**.
11. Define the Identity Management component database instance and click **Next**.

Field Name	Description
Identity Management component Database Host	The hostname or IP address of the server where the Identity Management component database is located.
Identity Management component Database Name	The service name of the database used by Identity Management component.
Identity Management component Database Port	The Identity Management component database port number, for example: **1433:** (Microsoft SQL Server),**1521:** (Oracle), **5432:** (PostgreSQL).
Identity Management component Database User Name	The user name of the database user you configured for the Identity Management component database.
Identity Management component Database Password	The password for the Identity Management component database user.

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

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

12.
    - Stop the **Operations Orchestration Central** service (Windows)

- Issue the command " `OO-install-dir/central/bin/central stop` " (Linux)
- Clear the database schema used for the Operations Orchestration installation;
- Finally, restart the installer and resume installation.

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

Field Name	Description
OO Hostname	The OO Hostname is the fully-qualified domain name or IP address of the server where Operations Orchestration is located. Specify the hostname that was used to generate Operations Orchestration's certificate. The hostname is used for TLS validation and to build the URL that the 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]`.
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.
OO User	The name of the user who logs in to Operations Orchestration Central. HP recommends that you use the `admin` userIf you followed all the steps documented in the *Install Operations Orchestration* section of this guide, this is the `admin` user. This is the user that was configured for provisioning topology designs (typically, admin).
OO Password	The password used by the OO user to log in to Operations Orchestration Central. If you followed all the steps documented in the *Install Operations Orchestration* section of this guide, use the password `cloud`.
OO Certificate File	The filename 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 this guide for more information) (see the *Initial Setup* section in this guide for more information).

Note: This information is used to set the Operations Orchestration properties in the `csa.properties` file and import Operations Orchestration's certificate into CSA's truststore.

> Refer to the *Cloud Service Automation Configuration Guide* for more information about these properties.

14. Enter the OO installation folder. This is the location in which to install the embedded Operations Orchestration.

15. Define the user and port used by the embedded Operations Orchestration. Enter the following information and click **Next**.

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

16. Define the database instance used by the embedded Operations Orchestration. Enter the following information and click **Next**.

Field Name	Description
Database Host: Microsoft SQL Server, Oracle, PostgreSQL	This is the hostname or IP address of the server where the embedded Operations Orchestration database is located.
Database Port: Microsoft SQL Server, Oracle, PostgreSQL	This is the embedded Operations Orchestration database port number: **1433** : (Microsoft SQL Server) **1521**: (Oracle) **5432**: (PostgreSQL)
OO Database Name Oracle OO service name	This is the service (global database) name of the database instance used by the embedded Operations Orchestration.

Field Name	Description
OO Database User Name	This is the username of the database user you configured for the Operations Orchestration database.
OO Database Password	This is the password for the Operations Orchestration database user.

17. By default, sample content (service designs and the components and Operations Orchestration flows required by the designs) can be installed with CSA. You can choose to deploy this content during upgrade (making the sample service designs available in the Designs area of the Cloud Service Management Console) or deploy the content at a later time (refer to the *Cloud Service Automation Content Pack User's Guide* or *Cloud Service Automation Configuration Guide* for more information).

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

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

    If you choose to skip content installation, you can install the content at a later time by running the Cloud Content Capsule Installer. Refer to the *Cloud Service Automation Content Pack User's 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.

18. Review your selections and click **Install** to complete the upgrade.
19. Review the system information and click **Next** to continue.
20. Review the system and database information and click **Install** to complete the upgrade.
21. Click **Done** to exit the installer.

Instructions for Linux:

1. Log in to the system as the root user.
2. Check the owner and group of `$CSA_JRE_HOME/lib/security/cacerts`, where `<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed.

    If the owner is not `csauser` or the group is not `csagrp`, reset the owner or group. For example, enter the following:

    ```
    chown csauser:csagrp $CSA_JRE_HOME/lib/security/cacerts
    ```

3. Log out as the `root user` and log in as `csauser`.
4. Check the values of the CSA_HOME, PS1, and TITLEBAR environment variables. If they are set,

verify that they do not contain any escape sequences. If any of these variables contain an escape sequence, the variable will cause the installer to fail. The variable must either be reset to a value that does not contain an escape sequence or must be unset.

5. Source the startup file in which you set the CSA_HOME and PATH environment variables. If you edited RHELinux: `.bash_profile`, enter the following: **RHELinux:** `. .bash_profile`

   Linux: `.bashrc`

6. Copy the CSA upgrade 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 in as the root user
   b. Enter the following commands:

      ```
      chown csauser setup.bin
       chmod 755 setup.bin
      ```

   c. Log out as the `root user` and then log in as `csauser`.
8. Run the `setup.bin` upgrade file as the `csauser`.

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

   As the `csauser`, enter the following:

   ```
   ./setup.bin
   ```

9. *Introduction*

   Read the Introduction and click **enter** to continue with the installation.

10. *License Agreement*

    Read the license agreement. Click **enter** after reading each page to scroll through the entire agreement.

11. *DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT?*

    Select **Y** and **enter** to accept the license agreement and continue with the installation. Type **N** and **enter** if you do not accept the license agreement and to exit the installation.

12. *Stop CSA*

    Verify that you have stopped CSA version 4.5x or 4.6x and click **enter**.

13. *CSA Installation Detected*

    Select the environment in which CSA is running.

    This selection determines the file from which the database instance information is read. For example, if you select standalone, the database instance information is read from the JBoss server's `standalone.xml` file (`$CSA_HOME/jboss-as/standalone/configuration/standalone.xml`). If you select cluster, the database instance information is read from the JBoss server's `domain.xmlstandalone-full-ha.xml` file (`$CSA_HOME/jboss-as/standalone/configuration/domain.xmlstandalone-full-ha.xml`).The installer detects if you are upgrading a remote installation of the Marketplace Portal. Click **enter** to continue.

14. *Select appropriate JRE*

    Select the JRE used by CSA and click **Enter**.

    Select OpenJDK JRE if you want to use the JRE that is installed with CSA version 4.70.

    Select Oracle JRE if you want to use an Oracle JRE. Then, select the location in which you installed this JRE. You must manually export the CSA certificate from the existing truststore and import it into the Oracle JRE truststore.

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

    For a list of supported JREs, refer to the *Cloud Service Automation System and Software Support Matrix* Guide.

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

    > **Note:** Use the existing JRE to continue using the JRE that was used with your previous CSA version. No additional configuration is required if you use the existing JRE.

15. *CSA Installation Detected*

    Verify the database instance information and click **enter**.

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

16. *CSA Database User Password*

    Enter the CSA database user password and click **enter**.

17. *Reporting User*

    Enter the CSA reporting database user and click **enter**. If you did not configure a reporting database user, click **enter** to continue.

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

18. *Install Database Components?*

    Type **1** (Yes) to install CSA database components and upgrade the CSA database schema then click **enter**.

19. *Operations Orchestration Configuration*

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

    > **Note**: if you have chosen to install a new version of the Embedded OO during the CSA upgrade, and the upgrade fails, do the following:

    - Stop the **Operations Orchestration Central** service (Windows)
    - Issue the command `" OO-install-dir/central/bin/central stop "` (Linux)
    - Clear the database schema used for the Operations Orchestration installation;
    - Finally, restart the installer and resume installation.

20. Define the Operations Orchestration 10.50 instance with which CSA is to be integrated. Enter the following information (select **Enter** after each entry).

    a. Enter the Operations Orchestration hostname. This is the fully-qualified domain name or IP address of the server where Operations Orchestration is located. Specify the hostname that was used to generate Operations Orchestration's certificate.

       The hostname is used for TLS validation and to build the URL that the 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 Operations Orchestration port. This 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 Operations Orchestration user. This is the name of the user who logs in to Operations Orchestration Central. HP recommends that you use the `admin` userIf you followed all the steps documented in the *Install Operations Orchestration* section of this guide, this is the `admin` user. This is the user that was configured for provisioning topology designs (typically, admin).

d. Enter the Operations Orchestration password. This is the password used by the OO user to log in 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. Enter the Operations Orchestration certificate file. This is the filename 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 this guide for more information) (see the *Initial Setup* section in this guide for more information).

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

21. *Operations Orchestration Installation Folder*

    Enter the Operations Orchestration installation folder. This is the location in which to install the embedded Operations Orchestration.

22. *Operations Orchestration Database Configuration*

    Configure the database instance used by the embedded Operations Orchestration. Enter the following information (select **Enter** after each entry).

    a. Enter the database hostname. This is the hostname 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 Operations Orchestration database name or Oracle Operations Orchestration service name. This is the service (global database) name of the database instance used by the embedded Operations Orchestration.

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

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

23. *Operations Orchestration Port*

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

24. *Operations Orchestration User*

    Enter the Operations Orchestration user. 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**.

25. *Operations Orchestration Password* and *Confirm Password*

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

26. *Pre-Installation Summary*

    Review your selections and click **enter** to complete the installation or **ctrl**-**c** to exit the installation.

27. When the installation completes, click **enter** to exit the installer.

28. Upgrade the CSA services to start and stop the CSA process and the Marketplace Portal process.

    a. Log in as the root user.

    b. Remove the old version of the CSA scripts. Enter the following:

    ```
    rm /etc/init.d/csa
    rm /etc/init.d/mpp
    ```

    c. Go to the directory in which CSA is installed. For example:

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

    d. Copy the new scripts to the `/etc/init.d` directory. Enter the following:

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

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

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

Update and Restart CSA

The following tasks must be completed before CSA can be restarted:

- Recustomize SSL/security
- Import certificates into CSA's truststore
- Recustomize manually configured files
- Remount shared file systems
- Upgrade all organization's *5recentWidget* mashup
- Restart the CSA Services

Recustomize SSL/Security

If you generated or copied SSL certificates that are used by CSA, you must copy these files to the appropriate directory in CSA 4.70.

> **Note:** If the automatically generated self-signed certificate for CSA has expired, you may still be able to use the Cloud Service Management Console. However, you will not be able to use the Marketplace Portal or Identity Management component unless you disable the `strictSSL` attribute in the Marketplace Portal's configuration file. If SSL must be enabled, you can generate another self-signed certificate or a Certificate Authority-signed certificate. If you generate a new certificate, you MUST import that certificate into CSA's JRE. Refer to the *Configure SSL for Client Browsers* section in the *Cloud Service Automation Configuration Guide* for more information.

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

File	Action
certificate files	**Required.** Manually copy certificate files that do not use the .crt extension that are used by CSA from the backup directory to the CSA 4.70 directory (see table below for more information).
cacerts	**Required.**
Keystore file defined by the `certificate-key-file` property of the connector attribute in `standalone.xml`	**Required** (if not using the default keystore file). Manually copy the custom keystore file back from the location outside of the **Windows:** `%CSA_HOME%` or the **Linux:** `$CSA_HOME` installation directory where you manually backed it up.

File	Action
standalone.xml	**Required** (if not using the default keystore file). Manually copy the custom keystore file back from the location outside of the **Windows:**`%CSA_HOME%`; or the **Linux:** `$CSA_HOME` installation directory where you manually backed it up.

Files, Actions, and Locations

certificate files	
Action	**Required.** Manually copy certificate files that do not use the .crt extension that are used by CSA from the backup directory to the CSA 4.70 directory. Files that use the .crt extension are automatically restored. If you saved .crt files in a different directory, you must manually copy these files back after upgrade.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\security\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/security/`

cacerts	
Action	**Required.** `<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed
File Location in CSA 4.70	**Windows:** `<csa_jre>\lib\security\` **Linux:** `<csa_jre>/lib/security/` where `<csa_jre>` is the directory in which the JRE (used exclusively by CSA) is installed.
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	This file is not backed up.

Keystore file defined by the `certificate-key-file` property of the connector attribute in `standalone.xml`	
Action	**Required** (if not using the default keystore file). Manually copy the keystore file back from the location outside of the **Windows:** `%CSA_HOME%`; or the **Linux:** `$CSA_HOME` installation directory where you manually backed it up. If you are using the default keystore file (**Windows:** `C:\Program Files\HPE\CSA\jboss-as\standalone\configuration\.keystore; or` **Linux:**`/usr/local/hpe/csa/jboss-`

Keystore file defined by the `certificate-key-file` property of the connector attribute in `standalone.xml`	
File Location in CSA 4.70	The file and its location are determined by the value defined by `certificate-key-file`. By default, the value is: **Windows:** `C:\Program Files\HPE\CSA\jboss-as\standalone\configuration\.keystore` ; or **Linux:** `/usr/local/hpe/csa/jboss-as/standalone/configuration/.keystore`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	If you are using a custom keystore file, this file is not backed up. The default keystore file is backed up to: **Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\security\keystores\`; or **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/security/keystores/`

standalone.xml	
Action	If this file was customized, manually copy the custom keystore file back from the location outside of the CSA installation directory where you manually backed it up.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\configuration\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/configuration/` Backup - **Windows:** `C:\csabackup\` **Windows:** `/tmp/csabackup/`

Import Certificates into CSA's Truststore

Prior to running the upgrade installer, you should have exported the SSL certificate from the truststore of CSA version 4.5x or 4.6x. Import this certificate and other application's certificates into the truststore of CSA version 4.70. Do the following:

1. If you did not export the SSL certificate from the truststore of CSA version 4.5x or 4.6x, the truststore has been backed up to the directory:

   Windows:`%CSA_HOME%\_CSA_4_70_0_installation\Backup\security\keystores\`

   Linux:`$CSA_HOME/_CSA_4_70_0_installation/Backup/security/keystores/`

Follow the instructions in the *Initial Setup* section of this document to export CSA's SSL certificate from the backed up truststore (you will need to modify the location of the truststore in the command).

2. Import the CSA certificate into the new CSA truststore. Do the following:

   a. Run the following commands:

   Windows:

   ```
   <csa_jre>\bin\keytool -importcert -keystore <csa_jre>\lib\security\cacerts
   -alias <alias> -file <filename>  -storepass changeit
   ```

   ```
   %CSA_HOME%\openjre\bin\keytool -importcert -keystore %CSA_
   HOME%\openjre\lib\security\cacerts -alias <alias> -file <filename>
   -storepass changeit
   ```

   Linux:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -keystore $CSA_JRE_
   HOME/lib/security/cacerts -alias <alias> -file <filename> -storepass
   changeit
   ```

   ```
   $CSA_HOME/openjre/bin/keytool -importcert -keystore $CSA_
   HOME/openjre/lib/security/cacerts -alias <alias> -file <filename> -storepass
   changeit
   ```

   where `<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed, *<alias>* is the name used by the CSA server keystore to identify the SSL certificate, and *<file_name>* is the filename given to the certificate file to be imported.

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

   Windows:

   ```
   <csa_jre>\bin\keytool -importcert -keystore <csa_jre>\lib\security\cacerts
   -alias csa -file .\csa.cert -storepass changeit
   ```

   ```
   %CSA_HOME%\openjre\bin\keytool -importcert -keystore <csa_
   jre>\openjre\lib\security\cacerts -alias csa -file .\csa.cert -storepass
   changeit
   ```

   Linux:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -keystore $CSA_
   HOME/lib/security/cacerts -alias csa -file ./csa.cert -storepass changeit
   ```

```
$CSA_HOME/openjre/bin/keytool -importcert -keystore $CSA_
HOME/openjre/lib/security/cacerts -alias csa -file ./csa.cert -storepass
changeit
```

b. At the prompt to import the certificate, type **yes**.

3. Import the Operations Orchestration certificate into the new CSA truststore. Do the following:

   a. If the root certificate of Operations Orchestration's Certificate Authority is stored in a file on this system, import that file. Otherwise, export Operations Orchestration's certificate from Operations Orchestration's truststore:

      i. On the system running Operations Orchestration, open a command prompt and change the directory to `%ICONCLUDE_HOME%` (Windows) or `$ICONCLUDE_HOME` (Linux).

      ii. Run the following command:

      Windows:

      ```
      .\jre1.6\bin\keytool exportcert alias pas file C:\oo.crt keystore
      .\Central\conf\rc_keystore storepass bran507025
      ```

      Linux:

      ```
      ./jre1.6/bin/keytool -exportcert -alias pas -file /tmp/oo.crt -keystore
      ./Central/conf/rc_keystore -storepass bran507025
      ```

      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).

      iii. 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 (in this example, the file is copied to **Windows:** `C:\` **Linux:** `/tmp`).

   b. On the system running CSA, run the following commands:

      Windows:

      ```
      <csa_jre>\bin\keytool -importcert -alias pas -file C:\oo.crt -keystore <csa_
      jre>\lib\security\cacerts -storepass changeit
      ```

      ```
      %CSA_HOME%\openjre\bin\keytool -importcert -alias pas -file C:\oo.crt
      -keystore %CSA_HOME%\openjre\lib\security\cacerts -storepass changeit
      ```

      Linux:

      ```
      $CSA_JRE_HOME/bin/keytool -importcert -alias pas -file /tmp/oo.crt -keystore
      $CSA_JRE_HOME/lib/security/cacerts -storepass changeit
      ```

```
$CSA_HOME/openjre/bin/keytool -importcert -alias pas -file /tmp/oo.crt
-keystore $CSA_HOME/openjre/lib/security/cacerts -storepass changeit
```

where
`<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed

c. When prompted to trust the certificate, type **yes**.

> **Important Note:** The manual certificate import procedure is mandatory, especially when one or more Operations Orchestration instances are used by CSA for sequence designs. These particular Operations Orchestration instances are not specified during the CSA installation or upgrade process.
>
> The import of any certificate used by an Operations Orchestration instance which was specified during installation is performed automatically by installer.

4. If other applications, such as the database, LDAP, SMTP, Operations Orchestration Load Balancer, or Continuous Delivery Automation require SSL, and/or you have installed an instance of the Marketplace Portal on a remote system, you must import these applications' certificates into the truststore of CSA version 4.70.

Recustomize Manually Configured Files

If you customized CSA files that are not documented as being customizable or customized CSA files with undocumented customizations, you will need to manually recustomize those files.

> **Caution:** All files that you have customized with undocumented changes in the **Windows:** `%CSA_HOME%` or the **Linux:**`$CSA_HOME` installation directory **MUST BE MANUALLY RESTORED**. If you followed all the steps in the *Initial Setup* section of this guide, you should have backed up these files before upgrading CSA.

Remount Shared File Systems

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

Upgrade all Organization's *5recentWidget* Mashup

For security purposes, you must manually update the *5recentWidget* mashup and every copy of this mashup for every organization that existed prior to upgrade. Do the following:

1. Log in to the Cloud Service Management Console as an administrator.
2. Click **Organizations**.
3. Create a temporary organization:
   a. In the left navigation frame, click the **Create Organization** button.
   b. Enter an organization name.
   c. Click **Create**.
4. Copy the content of the *5recentWidget* mashup from the temporary organization:
   a. In the left navigation frame, select the temporary organization.
   b. In the organization's navigation frame, select **Dashboard Widgets**.
   c. Select the *5recentWidget* mashup and click **edit**.
   d. Copy the text from the Content field.
5. For every organization (except the temporary organization you just created), do the following:
   a. Select the organization.
   b. In the organization's navigation frame, select **Dashboard Widgets**.
   c. For the *5recentWidget* mashup and every mashup that is a copy of the *5recentWidget* mashup that has not been customized, do the following:
      i. Select the mashup and click **edit**.
      ii. If you have not customized the *5recentWidget* mashup, paste the content from the temporary organization's *5recentWidget* mashup to this organization's *5recentWidget* mashup. If you made a copy of the organization's *5recentWidget* mashup but did not customize it, paste the contents from the temporary organization's *5recentWidget* mashup to this mashup.
      iii. If you have customized the *5recentWidget* mashup or made a copy of the *5recentWidget* mashup and customized it, do the following:
         A. Locate the `render` function.
         B. Locate every occurrence of `data[i].name` in the function and change every occurrence of `data[i].name` to **htmlEncode(data[i].name)** (except variable

declarations). In the uncustomized *5recentWidget* mashup, this content appears three times, but only two occurrences need to be updated (do not update the variable declaration).

C. Add the following functions to the mashup (the content can be copied from the temporary organization's *5recentWidget* mashup):

```
function htmlEncode(value){
   //create a in-memory div, set its inner text (which jQuery
automatically encodes)
   //then grab the encoded contents back out. The div never exists
on the page.
   return $('<div/>').text(value).html();
}
function htmlDecode(value){
   return $('').html(value).text();
}
```

iv. Click **Update**.

6. After you have updated all organizations, delete the temporary organization:

   a. In the left navigation frame, select the temporary organization.

   b. In the temporary organization's navigation frame, select **General Information**.

   c. Click **Delete**.

   d. In the **Delete Organization?** dialog, click **Yes** to delete the temporary organization.

Restart the CSA Services

To start CSA on Windows, complete the following steps:

1. 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 Cloud Service Automation service is started.

2. On the server that hosts CSA, navigate to **Start** > **Administrative Tools** > **Services**.
3. If global search is enabled, do the following:
   a. Right-click on the Elasticsearch 1.6.1 service and select **Restart**.
   b. 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.
4. Right-click on the CSA service and select **Start**.
5. Right-click on the Marketplace Portal service and select **Start**.
6. If you installed an embedded Operations Orchestration instance, right-click on the Operations Orchestration Central service and select **Start**.

To start CSA on Linux, complete the following steps:

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

```
service csa start
service mpp start
```

1. If elasticsearch is enabled (by default, elasticsearch is enabled; refer to the `csa.provider.es.exists` property in Properties for more information), type the following:

```
service elasticsearch start
```

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

   `<embeddedHPOOinstallation>/central/bin/central start`

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

Recustomize CSA

> **Note:** You must recustomize CSA for the features configured, customized, or used prior to the upgrade *only* (complete *only* the tasks for features that were already configured, customized, or used prior to the upgrade).

If you want to configure, customize, or use any of these features for the first time, refer to the following guides for more information:

- *Cloud Service Automation Configuration Guide*
- *Cloud Service Management Console Help*
- *Cloud Service Automation Provider Configuration Tool*
- *Cloud Service Automation Customizing the Marketplace Portal*
- *Cloud Service Automation Integration with ArcSight Logger*
- *Configuring CSA to Work with Oracle RAC*

The following page lists files you may have customized in previous CSA installations and the necessary actions to complete for the CSA upgrade:

- Configure the Cloud Service Management Console properties
- Recustomize the Cloud Service Management Console dashboard
- Configure the Cloud Service Management Console to import large archives
- Recustomize the Cloud Service Management Console session timeout
- Recustomize the Cloud Service Management Console dashboard title
- Add custom graphic files or dynamic query scripts
- Recustomize the CSA tools
- Recustomize the CSA database user
- Recustomize the CSA seeded users
- Add Marketplace Portal themes
- Add Marketplace Portal widgets
- Configure ArcSight Logger
- Integrate CSA with a common access card

- Configure the Identity Management component
- Configure IPv6
- Configure the JBoss Password Vault
- Configure Oracle RAC
- Configure CSA to use a Single Sign-On
- Integrate CSA with CA SiteMinder
- Delete the sample consumer organization
- Upgrade shortcuts
- Marketplace Portal configuration

Configure the Cloud Service Management Console Properties

The following is the file that you may have customized for the Cloud Service Management Console and the actions required when you upgrade CSA:

File	Action
csa.properties	No action required.

File, Actions, and Locations

csa.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/classes/`

Recustomize the Cloud Service Management Console Dashboard

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

File	Action
*.jsp	**Required.** Manually copy the JSP files from the backup directory to the appropriate directory in CSA 4.70 directory (see table below for more information).
config.json	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
messages.properties	**Required.** Manually copy the file from the backup directory to the CSA 4.70 directory (see table below for more information).
index.jsp	No action required.

Files, Actions, and Locations

***.jsp**	
Action	**Required.** If you created custom Java server page (JSP) files for the CSA dashboard and saved them in a directory within the CSA 4.5x or 4.6x installation but not in a directory whose content is backed up by the upgrade installer, you should have backed up these files to preserve them. Otherwise, they will be deleted by the upgrade installer. Manually copy the JSP files from the backup directory to the appropriate directory in CSA 4.70 directory.
File Location in CSA 4.70	The directory where the Cloud Service Management Console expects to find these files, defined in the `config.json` dashboard configuration file.
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	The directory to which the JSP files were backed up, either manually or by the upgrade installer, depending on where the files were located in CSA 4.5x or 4.6x.

config.json	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\dashboard\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/csa.war/dashboard/`

messages.properties	
Action	**Required.** Manually copy the file from the backup directory to the CSA 4.70 directory.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\dashboard\messages\dashboard\` **Linux:**`$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/messages/dashboard/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**`%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\dashboard\messages\dashboard\` **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/csa.war/dashboard/messages/dashboard/`

index.jsp	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\custom-content\` **Linux:**`$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom-content/`

index.jsp	
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**`%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\deployments\csa.war\custom-content\` **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/deployments/csa.war/custom-content/`

Configure the Cloud Service Management Console to Import Large Archives

The following is the file that you customized to import large archives using the Cloud Service Management Console or REST API and the actions required when you upgrade CSA:

File	Action
Windows: standalone.conf.bat **Linux:**standalone.conf	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File, Action, and Locations

Windows:standalone.conf.batLinux:standalone.conf	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\bin\`**Linux:** `$CSA_HOME/jboss-as/bin/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/`

Recustomize the Cloud Service Management Console Session Timeout

The following file may have been customized if you updated the Cloud Service Management Console session:

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

File, Action, and Locations

web.xml	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/`

Recustomize the Cloud Service Management Console Dashboard Title

The following file may have been customized if you updated the Cloud Service Management Console dashboard title:

File	Action
messages.properties	**Required.** Manually copy the file from the backup directory to the CSA 4.70 directory (see table below for more information).

File, Action, and Locations

messages.properties	
Action	**Required.** Manually copy the file from the backup directory to the CSA 4.70 directory.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\custom\` **Linux:**`$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**`%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\custom\` **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/csa.war/custom/`

Add Custom Graphic Files or Dynamic Query Scripts

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

File	Action
*.jsp (dynamic query scripts)	**Required.** Manually copy any custom dynamic query scripts from the backup directory to the CSA 4.70 directory (see table below for more information).
*.jar (dynamic query scripts)	**Required.** Manually copy any custom dynamic query scripts from the manual backup copies you made before running the upgrade installer.
*.jpg, *.jpeg, *.gif, *.png	No action required.

Files, Actions, and Locations

*.jsp (dynamic query scripts)	
Action	**Required.** Manually copy any custom dynamic query scripts from the backup directory to the CSA 4.70 directory.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\propertysources\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/propertysources/`
Backed Up CSA 4.5x or	**Windows:** `%CSA_HOME%\_CSA_4_70_0_`

*.jsp (dynamic query scripts)	
4.6x File Location in CSA 4.70	`installation\Backup\standalone\csa.war\propertysources\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/csa.war/propertysources/`

*.jar (dynamic query scripts)	
Action	**Required.** Manually copy any custom dynamic query scripts from the manual backup copies you made before running the upgrade installer.
File Location in CSA 4.70	*<user-specified location>*
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	*<user-specified location>*

*.jpg, *.jpeg, *.gif, *.png	
Action	No action required. All custom graphics of the listed types in the associated directory are automatically restored.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\images\` **Linux:**`$CSA_HOME/jboss-as/standalone/deployments/csa.war/images/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**`%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\images\` **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/csa.war/images/`

Recustomize the CSA Tools

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

File	Action
config.properties (Content Installer, Health Tool, Purge Tool, Provider Configuration Tool)	**Required.** Manually copy any custom configuration files from the backup directory to the CSA 4.70 directory (see table below for more information).

File	Action
provider.xml (Provider Configuration Tool)	**Required.** Manually copy any custom input files from the backup directory to the CSA 4.70 directory (see table below for more information).

Files, Actions, and Locations

config.properties	
Action	**Required.** Manually copy any custom configuration files from the backup directory to the CSA 4.70 directory. This is the generic name of the configuration file used in some examples for the Content Archive Tool, Purge Tool, and Provider Configuration Tool. If you used a different name for the configuration file, copy that file instead.

File Location in CSA 4.70	**Windows:**
	`%CSA_HOME%\Tools\DBPurgeTool\`
	`%CSA_HOME%\Tools\ProviderTool\`
	Linux:/
	`$CSA_HOME/Tools/DBPurgeTool/`
	`$CSA_HOME/Tools/ProviderTool/`

Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**
	`%CSA_HOME%\_CSA_4_70_0_installation\Backup\Tools\DBPurgeTool\`
	`%CSA_HOME%\_CSA_4_70_0_installation\Backup\Tools\ProviderTool\`
	Linux:
	`$CSA_HOME/_CSA_4_70_0_installation/Backup/Tools/DBPurgeTool/`
	`$CSA_HOME/_CSA_4_70_0_installation/Backup/Tools/ProviderTool/`

provider.xml	
Action	**Required.** Manually copy any custom provider input files from the backup directory to the CSA 4.70 directory. This is the generic name of the input file used in some examples for the Provider Configuration Tool. If you used a different name for the provider input file, copy that file instead.
File Location in CSA 4.70	**Windows:**`%CSA_HOME%\Tools\ProviderTool\` **Linux:**`$CSA_HOME/Tools/ProviderTool/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:**`%CSA_HOME%\_CSA_4_70_0_installation\Backup\Tools\ProviderTool\` **Linux:**`$CSA_HOME/_CSA_4_70_0_installation/Backup/Tools/ProviderTool/`

Recustomize the CSA Database User

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

File	Action
standalone.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

Files, Actions, and Locations

standalone.xml	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\configuration\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/configuration/` Backup - **Windows:** `C:\csabackup\` **Windows:** `/tmp/csabackup/`

Recustomize the CSA Seeded Users

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

File	Action
applicationContext-security.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
csa-consumer-users.properties	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
provider-users.properties	

File	Action
integrationusers.properties	
applicationContext.properties	**Required.** If this file was customized, you must recustomize this file (see table below for more information.

Files, Actions, and Locations

applicationContext-security.xml	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/`

csa-consumer-users.properties	
Action	**Required.** If you customized the roles of a seeded user, you must manually restore those roles. If you customized the password of a seeded user, the password is automatically restored. If you deleted a seeded user, the seeded user is automatically restored and you must manually remove that user. If you added a custom user, that user is automatically restored. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70.No action required.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/`
Backed Up CSA 4.5x	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/idm-service.war/WEB-`

csa-consumer-users.properties	
or 4.6x File Location in CSA 4.70	`INF/classes/`

provider-users.properties	
Action	**Required.** If you customized the roles of a seeded user, you must manually restore those roles. If you customized the password of a seeded user, the password is automatically restored. If you deleted a seeded user, the seeded user is automatically restored and you must manually remove that user. If you added a custom user, that user is automatically restored. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/idm-service.war/WEB-INF/classes/`

integrationusers.properties	
Action	**Required.** If you customized the roles of a seeded user, you must manually restore those roles. If you customized the password of a seeded user, the password is automatically restored. If you deleted a seeded user, the seeded user is automatically restored and you must manually remove that user. If you added a custom user, that user is automatically restored. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/`
Backed Up CSA 4.5x or	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\classes\`

integrationusers.properties	
4.6x File Location in CSA 4.70	**Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/idm-service.war/WEB-INF/classes/`

applicationContext.properties	
Action	**Required.** If you customized the password of a seeded user, the password is automatically restored. If you deleted a seeded user, the seeded user is automatically restored and you must manually remove that user. If you added a custom user, that user is automatically restored. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. **Note:** The parameter `idm.csa.hostname` has to be fixed to contain the correct value (you can use the corrected value from the previous version of CSA).
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

Add Marketplace Portal Themes

The following are directories where you may have added customized themes for the Marketplace Portal and the action required when you upgrade CSA:

Directory	Action
<theme_directory>	**Required.** If you created a customized theme for the Marketplace Portal, you must manually copy these directories (one for the Marketplace Portal and one for the Identity Management component) and their content from the backup directory to the CSA 4.70 directory (see table below for more information).

Directories, Actions, and Locations

<theme_directory> (Marketplace Portal)	
Action	**Required.** If you created a customized theme for the Marketplace Portal, you must manually copy this directory and its content from the backup directory to the CSA 4.70 directory.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\portal\node_modules\mpp-ui\dist\bower_components\mpp-*theme\` **Linux:** `$CSA_HOME/portal/node_modules/mpp-ui/dist/bower_components/mpp-*theme/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\portal\node_modules\mpp-ui\dist\bower_components\mpp-*theme\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/bower_components/mpp-*theme/`

<theme_directory> (Identity Management Component)	
Action	**Required.** If you created a customized theme for the Marketplace Portal, you must recreate this theme by creating a new directory in the CSA 4.70 directory : `idm-service.war/ui/bower_components`. • This directory contains the HPE Enterprise and HPE Playful themes. • The default theme is in the `idm-service.war/ui/styles` directory. • The backup directory contains the previous versions of your themes; however, due to changes in the Identity Management component, that CSS is no longer applicable.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\themes\bower_components` **Linux:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\themes\bower_components`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\themes\` **Linux:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\themes\`

Add Marketplace Portal Widgets

The following is the directory where you may have added customized widgets for the Marketplace Portal and the action required when you upgrade CSA:

Directory	Action
<iFRAME_URL_structure>	**Required.** If you created a customized widget that uses an iFRAME that serves HTML pages for the Marketplace Portal, you must manually copy its URL structure and contents from the backup directory to the CSA 4.70 directory (see table below for more information).

Directory, Action, and Locations

<iFRAME_URL_structure>	
Action	**Required.** If you created a customized widget that uses an iFRAME that serves HTML pages for the Marketplace Portal, you must manually copy its URL structure and contents from the backup directory to the CSA 4.70 directory.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\portal\node_modules\mpp-ui\dist\` **Linux:** `$CSA_HOME/portal/node_modules/mpp-ui/dist/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\portal\node_modules\mpp-ui\dist\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/`

Configure ArcSight Logger

The following is the file that you may have customized if you integrated with the ArcSight Logger and the actions required when you upgrade CSA:

File	Action
log4j.xml properties	**Required.** You must recustomize the `log4j2.xml` file (see table below for more information).

File, Actions, and Locations

log4j.xml properties	
Action	**Required.** You must recustomize the `log4j2.xml` file. Refer to the *Cloud Service Automation Integration with ArcSight Logger* whitepaper for more information.

log4j.xml properties	
	Caution: Do NOT copy the backed up file over the new file. The logger has been upgraded in CSA 4.70 and the backed up file is not compatible with the current version.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/classes/`

Integrate CSA with a Common Access Card

> **Note**: the CSA Upgrade will detect the current Common Access Card (CAC) configuration and load it from the current JBoss directory during the pre-install phase via an InstallAnywhere context. This configuration is then later used to configure CAC during the post-install phase.

> See the *Cloud Service Automation Configuration Guide* for more information on configuring CAC.

The following is a list of files that you customized when integrating CSA with a Common Access Card (CAC) and the actions required when you upgrade CSA:

File	Action
applicationContext.xml (Cloud Service Management Console)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
applicationContext.xml (Identity Management component)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
applicationContext-security.xml (Identity Management component)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
applicationContext-v0.xml (Identity Management component)	**Required.** This is a new file that must be customized (see table below for more information).
csa.properties	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File	Action
java.security	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
standalone.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File	Action
rb.json	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
main.css (default)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
main.css (pilot)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
main.css (custom theme)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
java.security	No action required.

Files, Actions, and Locations

applicationContext.xml (Cloud Service Management Console)	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version. No action required.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/`

applicationContext.xml (Identity Management Component)	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation). No action required.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

applicationContext-security.xml (Identity Management Component)	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. > **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version. No action required.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\`

applicationContext-security.xml (Identity Management Component)	
	Linux: `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

applicationContext-v0.xml (Identity Management Component)	
Action	**Required.** This is a new file that requires customization. Refer to the *Cloud Service Automation Configuration Guide* for more information.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	N/A

csa.properties	

Action	User has to validate or add the following properties in `csa.properties`:
	`csaKeystore=C:/Program Files/HPE/CSA/jboss-as/standalone/configuration/.keystore`
	`csaKeystorePassword=ENC(oreBTzwQRoHyaKoELUqpHLOzganbIkQg)`

File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\classes\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/classes/`

java.security	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed

java.security	
	up copy and compare it to the file installed with CSA 4.70. **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** `<csa_jre>\lib\security\` **Linux:** `<csa_jre>/lib/security/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	This file is not backed up. You should have manually backed this file up prior to running the upgrade installer.

standalone.xml	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\configuration\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/configuration/` Backup - **Windows:** `C:\csabackup\` **Windows:** `/tmp/csabackup/`

Configure the Identity Management Component

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

File	Action
applicationContext.xml (Identity Management component)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File	Action
applicationContext.properties	No action required.
applicationContext-common.xml	No action required.

Files, Actions, and Locations

applicationContext.xml (Identity Management Component)	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

applicationContext.properties	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

applicationContext-common.xml	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\idm-service.war\WEB-INF\spring\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/idm-service.war/WEB-INF/spring/`

Configure IPv6

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

File	Action
standalone.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File, Actions, and Locations

standalone.xml	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. > **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`

standalone.xml	
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\configuration\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/configuration/` Backup - **Windows:** `C:\csabackup\` **Windows:** `/tmp/csabackup/`

Configure the JBoss Password Vault

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

File	Action
Windows: vault.bat**Linux:**vault.sh	**Required.** If this file was customized, you must recustomize this file (see table below for more information.

File, Actions, and Locations

Windows:vault.batLinux:vault.sh	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\bin\` **Linux:** `$CSA_HOME/jboss-as/bin/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/`

Configure Oracle RAC

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

File	Action
standalone.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

File, Actions, and Locations

standalone.xml	
Action	**Required.** If this file was customized, you must recustomize this file. The customization required for this file is different from the previous release. Refer to the *Cloud Service Automation Configuration Guide* for more information. **Caution:** Do NOT copy the backed up file over the new file. The file has changed in CSA 4.70 and the backed up file is different from the current version.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\configuration\` **Linux:** `$CSA_HOME/jboss-as/standalone/configuration/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\configuration\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/configuration/` Backup - **Windows:** `C:\csabackup\` **Windows:** `/tmp/csabackup/`

Configure CSA to Use a Single Sign-On

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

File	Action
applicationContext.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
applicationContext-security.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
hpssoConfiguration.xml	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
main.css (default)	**Required.** If this file was customized, you must recustomize this file (see

File	Action
	table below for more information).
main.css (pilot)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
main.css (custom theme)	**Required.** If this file was customized, you must recustomize this file (see table below for more information).
rb.json	**Required.** If this file was customized, you must recustomize this file (see table below for more information).

Files, Actions, and Locations

applicationContext.xml	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation). No action required.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/`

applicationContext-security.xml	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in	**Windows:** `%CSA_HOME%\jboss-`

applicationContext-security.xml	
CSA 4.70	`as\standalone\deployments\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/csa.war/WEB-INF/`

hpssoConfiguration.xml	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	`%CSA_HOME%\jboss-as\standalone\deployments\csa.war\WEB-INF\`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	`%CSA_HOME%\_CSA_4_70_0_installation\Backup\standalone\csa.war\WEB-INF\`

main.css (<theme_directory>)	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\portal\node_modules\mpp-ui\dist\themes\<theme_directory>\styles\` **Linux:** `$CSA_HOME/portal/node_modules/mpp-ui/dist/themes/<theme_directory>/styles/`
Backed Up CSA 4.5x or 4.6x	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\portal\node_modules\mpp-ui\themes\<theme_`

main.css (<theme_directory>)	
File Location in CSA 4.70	directory>\styles\ **Linux:** $CSA_HOME/_CSA_4_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/themes/<theme_directory>/styles/

rb.json	
Action	**Required.** If this file was customized, you must recustomize this file. If you do not remember the customizations you made to the file, refer to the backed up copy and compare it to the file installed with CSA 4.70. > **Note:** Port property has to be verified to contain a custom port, if such a port is used (or you can use the property from the backup of the previous CSA installation).
File Location in CSA 4.70	**Windows:** %CSA_HOME%\portal\node_modules\mpp-ui\dist\locales\<locale>\ **Linux:** $CSA_HOME/portal/node_modules/mpp-ui/dist/locales/<locale>/
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** %CSA_HOME%_CSA_4_70_0_installation\Backup\portal\node_modules\mpp-ui\dist\locales\<locale>\ **Linux:** $CSA_HOME/_CSA_4_70_0_installation/Backup/portal/node_modules/mpp-ui/dist/locales/<locale>/

Delete the Sample Consumer Organization

If you deleted the sample consumer organization on your CSA 4.5x or 4.6x system, you should delete the sample consumer organization (if it still exists) if you are no longer using it, if you are moving the application to production, or if you are upgrading a production system. See the *Cloud Service Automation Configuration Guide* for more information if you are deleting this organization for the first time.

Upgrade Shortcuts

If you created CSA shortcuts in the default directory (for example, C:\Users\<*user*>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Hewlett-

`Packard\Cloud Service Automation`), these shortcuts are automatically upgraded. If you created CSA shortcuts and saved them to another directory other than the default directory (for example, in a Program Group, in the Start Menu, on the desktop, or in the Quick Launch Bar), you should delete these shortcuts as they will no longer work. Optionally, you can change the target of the shortcuts to `%CSA_HOME%\_CSA_4_70_0_installation\Change HPE Cloud Service Automation Installation.exe`.

Marketplace Portal Configuration

If you customized the Marketplace Portal configuration file, the customizations have been merged with the upgraded file. Refer to the *Cloud Service Automation Configuration Guide* for more information about the configurable properties in this file.

File	Action
mpp.json	No action required. If this file was customized, the customizations have been merged with the upgraded file.
index.html	No action required. If this file was customized, the customizations have been restored.

Files, Actions, and Locations

mpp.json	
Action	No action required. If this file was customized, the customizations have been merged with the upgraded file.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\portal\conf\` **Linux:** `$CSA_HOME/portal/conf/`
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** `%CSA_HOME%\_CSA_4_70_0_installation\Backup\portal\conf\` **Linux:** `$CSA_HOME/_CSA_4_70_0_installation/Backup/portal/conf/`

index.html	
Action	No action required. If this file was customized, the customizations have been restored.
File Location in CSA 4.70	**Windows:** `%CSA_HOME%\jboss-as\standalone\deployments\mpp.war\` **Linux:** `$CSA_HOME/jboss-`

index.html	
	as/standalone/deployments/mpp.war/
Backed Up CSA 4.5x or 4.6x File Location in CSA 4.70	**Windows:** %CSA_HOME%_CSA_4_70_0_installation\Backup\standalone\mpp.war\ **Linux:** $CSA_HOME/_CSA_4_70_0_installation/Backup/standalone/mpp.war/

Update and Redeploy the Service Manager Base Content Pack

Important Note: During the CSA upgrade, make sure there are no apostrophe characters (`'`) in any base content pack filename. If your content pack filename contains an apostrophe, the upgrade installation may fail.

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 on the 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 on the Operations Orchestration RAS service and select **Stop**.

   Linux:

   a. On the server that hosts Operations Orchestration, run the following command: `<HPOOinstallation>/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: `<HPOOinstallation>/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:

   `<HPOOinstallation>\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):

   `<HPOOinstallation>\ras\var\cache`

   For example,

   Windows: `C:\Program Files\HPE\HP 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 on the 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 on the Operations Orchestration RAS service and select **Start**.

   Linux:

   a. On the server that hosts Operations Orchestration, run the following command: `<HPOOinstallation>/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: `<HPOOinstallation>/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 in 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**.

Run the Cloud Content Capsule Installer

If you did not install the sample content during the upgrade or if the sample content deployment failed, you can run the Cloud Content Capsule Installer to install the sample content. Refer to the *CSA Content Installation Guide* and *Cloud Service Automation Content Pack User's Guide* for more information.

Update CSA Flows for Topology Designs

Install CSA flows for sequential designs and deploy a content pack for topology designs. If you have not installed flows for sequential designs before, you should configure Operations Orchestration for sequential designs instead. Refer to the *Configure Operations Orchestration for Sequential Designs* section in the *Cloud Service Automation Configuration Guide* for more information.

Deploy a Content Pack for Topology Designs

If you upgraded CSA that uses an existing external Operations Orchestration version 10.50, you must manually deploy a content pack for topology designs.

To deploy the content pack, do the following from the system on which CSA is installed:

1. Log in to Operations Orchestration Central (version 10.50) and click the **Content Management** button.
2. Click the **Content Packs** tab.
3. Click the **Deploy New Content** icon.
4. Click the **Add files for deployment** icon.
5. Navigate to the **Windows:** `%CSA_HOME%\Tools\ComponentTool\contentpacks\; or the` **Linux:**`$CSA_HOME/Tools/ComponentTool/contentpacks/` directory.

1. Select the **CSA-SA-CP-04.70.0000** content pack, and click **Open**.

   > **Note:** You do not need to select the other content packs in this directory. The other content packs were automatically deployed during the upgrade.

2. Click **Deploy**.

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

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

Install CSA Flows for Sequential Designs

Install CSA flows on the system running Operations Orchestration:

1. If CSA and Operations Orchestration are running on different systems, from the CSA system, copy the `%CSA_HOME%\CSAKit-4.7\OO Flow Content\9X\CSA-4_10-ContentInstaller.jar` file to the Operations Orchestration 9.07 system and `%CSA_HOME%\CSAKit-4.7\OO Flow Content\10X\oo10-csa-cp-4.70.000.jar$CSA_HOME/CSAKit-4.7/OO Flow Content/>9X/CSA-4_10-ContentInstaller.jar` file to the Operations Orchestration 9.07 system and `$CSA_HOME/CSAKit-4.7/OO Flow Content/10X/oo10-csa-cp-4.70.000.jar` file to the Operations Orchestration 10.20 system.
2. On the system running Operations Orchestration, open a command prompt and change to the directory where the `CSA-4_10-ContentInstaller.jar`/`oo10-csa-cp-4.70.000.jar` file is located.
3. From the command prompt, run the following command:

   Windows (9.07): **"<*location_of_OO_jre*>\bin\java" -jar CSA-4_10-ContentInstaller.jar -centralPassword <*OOAdminPassword*>**
   Windows (10.20): **"<*location_of_OO_jre*>\bin\java" -jar oo10-csa-cp-4.70.000.jar -centralPassword <*OOAdminPassword*>**

   Linux (9.07): **<*location_of_OO_jre*>/bin/java -jar CSA-4_10-ContentInstaller.jar -centralPassword <*OOAdminPassword*>**
   Linux (10.20): **<*location_of_OO_jre*>/bin/java -jar oo10-csa-cp-4.70.000.jar -centralPassword <*OOAdminPassword*>**

   where `<location_of_OO_jre>` is the location of the JRE installed for Operations Orchestration. For example, `"%ICONCLUDE_HOME%\jre1.6"` or `$ICONCLUDE_HOME/jre1.6` on the 9.07 system and `"%ICONCLUDE_HOME%\java"` or `$ICONCLUDE_HOME/java` on the 10.20 system.

Import Service Designs

Import the CSA 4.70 sample service designs:

1. Log in to the Cloud Service Management Console. You must be assigned the Service Designer or CSA Administrator role in order to import service designs.
2. Click the **Designs** tile.
3. If you are importing a sequential design, do the following:
   a. Click the **Sequenced** tile, which takes you to the **All Designs** area for sequenced designs.
   b. In the lower, right pane of the **All Designs** area, click **Import**.
4. If you are importing a topology design, do the following:
   a. Click the **Topology** tile.
   b. From **Browse Designs**, click **Import**.
5. Navigate to **Windows:** `%CSA_HOME%\CSAKit-4.7\Content Archives,` ; or the **Linux:** `$CSA_HOME/CSAKit-4.7/Content Archives,` select a zip file from one of the directories, and click **Open**.
6. Repeat steps 3, 4, and 5 for every zip file in the `Content Archives` directory and its subdirectories.

> **Note:** HPE recommends that you start using the CSA 4.70 versions of the service designs immediately.

Refer to the *CSA Integration Pack* whitepaper and *CSA Service Design Guide* for more information about the CSA service designs.

Upgrade Resource Providers

Refer to the README file of the resource provider to verify if it requires and upgrade. The README file can be found in the following locations:

- **Windows:** `%CSA_HOME%\CSAKit-4.7\Lib\<resource_provider>\`
- **Linux:** `$CSA_HOME/CSAKit-4.7/Lib/<resource_provider>/`

Clear the Web Browser Cache

It may be necessary to clear your Web browser cache on systems that previously accessed the Cloud Service Management Console prior to upgrading to CSA 4.70. To clear your Web browser cache:

- If you are using a Chrome Web browser:
  a. Open the browser.
  b. Select **<Ctrl>+<Shift>+<Delete>**.
  c. For **Obliterate the following items from**, select **the beginning of time**.
  d. Select only **Empty the cache**. Unselect all other items.
  e. Click **Clear browsing data**.
- If you are using a Firefox Web browser:
  a. Open the browser.
  b. Select **<Ctrl>+<Shift>+<Delete>**.
  c. For **Time range to clear**, select **Everything**.
  d. Expand **Details**.
  e. Select only **Cache**. Unselect all other items.
  f. Click **Clear Now**.
- If you are using a Windows IE Web browser:
  a. Open the browser.
  b. Select **<Ctrl>+<Shift>+<Delete>**.
  c. Select only **Temporary Internet Files**. Unselect all other items.
  d. Click **Delete**.

Restart CSA

To start CSA on Windows, complete the following steps:

1. 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 Cloud Service Automation service is started.

2. On the server that hosts CSA, navigate to **Start** > **Administrative Tools** > **Services**.
3. If global search is enabled, do the following:
   a. Right-click on the Elasticsearch 1.6.1 service and select **Restart**.
   b. 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.
4. Right-click on the CSA service and select **Start**.
5. Right-click on the Marketplace Portal service and select **Start**.
6. If you installed an embedded Operations Orchestration instance, right-click on the Operations Orchestration Central service and select **Start**.

To start CSA on Linux, complete the following steps:

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

```
service csa start
service mpp start
```

1. If elasticsearch is enabled (by default, elasticsearch is enabled; refer to the `csa.provider.es.exists` property in Properties for more information), type the following:

```
service elasticsearch start
```

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

```
<embeddedHPOOinstallation>/central/bin/central start
```

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

Appendix A: Remote MPP for CSA

The following sections are important for operating a remote Marketplace Portal on CSA:

- Backup CSA
- Update CSA directories and certificates
- Start the MPP Service

Back Up CSA

Before you back up and upgrade your remote installation of the Marketplace Portal, on the system running the Cloud Service Management Console, upgrade to CSA 4.70, if you have not already done so.

On the remote system, do the following:

1. Create a directory named: **Windows:** `C:\csabackup\`. or **Linux:** `/tmp/csabackup/`.
2. Copy the **Windows:** `%CSA_HOME%\portal\` or the **Linux:**`$CSA_HOME/portal/` directory to **Windows:** `C:\csabackup\`; or **Linux:** `/tmp/csabackup/`.
3. Copy the **Windows:** `%CSA_HOME%\jre\lib\security\cacerts` or **Linux:** `$CSA_HOME/jre/lib/security/cacerts` file to the **Windows:** `C:\csabackup\`; or **Linux:** `/tmp/csabackup/`.
4. **[Oracle]**: Copy the JDBC drivers from the system running the Cloud Service Management Console:

   Windows:

   ```
   %CSA_HOME% \jboss-as\modules\system\layers\base\com\oracle\ojdbc6\main;
   ```

   Linux:

   ```
   %CSA_HOME% /jboss-as/modules/system/layers/base/com/oracle/ojdbc6/main;
   ```

   to the remote system (to a directory outside of the **Windows:** `%CSA_HOME%` or **Linux:**`$CSA_HOME` directory).

For example, copy `ojdbc*.jar` and `ora*.jar` to **Windows:** `C:\csabackup\jdbc\`; **Linux:**or `/tmp/csabackup/jdbc/`.

Update CSA Directories and Certificates

Complete the following tasks:

- Remove the JBoss directory
- Restore `cacerts`

Remove the JBoss Directory

If it exists, remove the **Windows:** `%CSA_HOME%\jboss-as`; or the **Linux:** `$CSA_HOME/jboss-as` directory.

Restore cacerts

To restore certificates, do the following:

Windows: Restore the `C:\csabackup\cacerts` to `<csa_jre>\lib\security\cacerts`; or

Linux: Restore the `/tmp/csabackup/cacerts` to `<csa_jre>/lib/security/cacerts` (overwrite the existing file) where `<CSA_JRE_HOME>` is the directory in which the JRE that is used by CSA is installed.

Start the Marketplace Portal Service

To start the Marketplace Portal service:

Windows:

1. On the system running the remote Marketplace Portal, navigate to **Start** > **Administrative Tools** > **Services**.

2. Start the Marketplace Portal service.

   Linux:

3. On the system running the remote Marketplace Portal, type `service mpp start`.

Send documentation feedback

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

Feedback on Upgrade Guide (Cloud Service Automation 4.70)

Just add your feedback to the email and click send.

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

We appreciate your feedback!