HP Cloud Service Automation

Software Version: 4.50
Linux operating system

Configuration Guide

Document Release Date: August 2015
Software Release Date: July 2015

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link 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 HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP 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 web site 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 sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Overview

This document provides information on how to set up the Cloud Service Management Console and HP Cloud Service Automation (HP CSA) in order to enable users to log in and use the Cloud Service Management Console and Marketplace Portal. Some tasks must be completed before you can start using HP CSA.

The user who sets up HP CSA should have knowledge of or work with someone who has knowledge of LDAP, TLS, HP Operations Orchestration, and the resource providers that will be integrated with HP CSA.

The following information is provided in this document:

Getting Started. Before setting up the Cloud Service Management Console, you may need to complete some initial configuration such as preparing LDAP, configuring HP CSA truststore properties, and requesting a software license.

Secure Connections. Many of the components that interact with HP CSA may require communication over a secure connection. You may want to replace the HP CSA self-signed certificate or configure a secure connection for LDAP, SMTP, the Oracle Database, the Microsoft SQL Server, or the HP Operations Orchestration Load Balancer.

HP Operations Orchestration. A process engine whose flows are executed by HP CSA, HP Operations Orchestration must be integrated with HP CSA and sample flows must be imported before the flows can be executed.

The Cloud Service Management Console. To set up the Cloud Service Management Console so that users can log in, you must configure the provider organization. In order to start using the Cloud Service Management Console, you must add a software license. You may wish to import the sample service designs provided with HP CSA, configure a proxy, or enable or customize tiles in the Cloud Service Management Console.

Common HP CSA Tasks. Common tasks include launching the Cloud Service Management Console and Marketplace Portal, starting, stopping, or restarting HP CSA and the Marketplace Portal, encrypting an HP CSA password, and uninstalling HP CSA.

The Marketplace Portal. The Marketplace Portal's password utility is different from the one used by HP CSA. This section explains how to encrypt passwords used by the Marketplace Portal. Configuring the Marketplace Portal is completed using the Cloud Service Management Console. Refer to the *HP Cloud Service Management Console Help* for information about configuring the Marketplace Portal.

User Administration. User administration includes tasks such as changing the out-of-the-box users.

IPv6 Configuration. Configure HP CSA to support IPv6 (both dual-stack and IPv6-only).

Common Access Card. Common access cards are used for user authentication and allow users to log in to HP CSA using a Personal Identity Verification card.

Single Sign-On. Enable or disable HP Single Sign-On that is included with HP CSA. Single sign-on can also be configured for the Cloud Service Management Console and Marketplace Portal with almost any single sign-on solution and a specific solution for CA SiteMinder is provided.

Database Administration. Database administration includes any task that might involve the database, such as configuring the HP CSA reporting database user if you did not configure it during installation, updating HP CSA database system or users and passwords, importing large archives, purging service subscriptions, installing the HP CSA database schema, and configuring HP CSA to mitigate frequently dropped database connections.

Cloud Service Management Console Properties. This is a reference to the Cloud Service Management Console configurable properties.

Marketplace Portal Attributes. This is a reference to the Marketplace Portal configurable attributes.

HP Operations Orchestration Settings. This is a reference to the HP Operations Orchestration configurable settings applicable to HP CSA.

Identity Management Configuration. This is a reference to the Identity Management component configurable settings applicable to HP CSA.

HP Operations Orchestration Manual Configuration for Designs. The steps needed to configure HP Operations Orchestration for topology and sequential designs without using the HP Cloud Content Capsule Installer.

Cross-Product Upgrade Between HP Codar and HP CSA. The upgrade result when existing HP CSA 4.2x installations use the HP Codar 1.50 installer, and when existing HP Codar 1.00 installations use the HP CSA 4.50 installer.

Refer to the following guides for more information about:

- HP CSA: *HP Cloud Service Automation Concepts Guide*
- Supported components and versions: *HP Cloud Service Automation System and Software Support Matrix*
- Installation: *HP Cloud Service Automation Installation Guide*
- Cloud Service Management Console: *HP Cloud Service Management Console Help*
- Automated, on-demand cloud services creation: *HP Cloud Service Automation Service Design Guide*
- Sample service designs and resource offerings: *HP Cloud Service Automation Content Pack User's Guide*

These guides are available from the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Chapter 2: Getting Started

This chapter provides information for common setup tasks that need to be completed for HP CSA.

Tasks include:

- "Prepare LDAP for HP CSA" below (required)
- "Configure the HP CSA Truststore Properties" on the next page (required)
- "Request Software Licenses" on page 17 (required)
- "Enable TLS on Your Web Browser" on page 18 (required)
- "Configure the Provider Organization" on page 19 (required)
- "Add a Software License" on page 20 (required)
- "Proxy Configuration for Resource Providers Outside the Internal Network" on page 21 (optional)

Prepare LDAP for HP CSA

HP CSA supports limited authentication out-of-the-box and has a fixed set of user names (and associated passwords) that can be used to log in. This basic form of authentication can be used for initial setup and experimentation with the product, but in a production environment, authentication should be configured to occur against a directory service.

HP CSA can be configured to authenticate against a Lightweight Directory Access Protocol (LDAP) server. Users can then log in with a pre-existing user name (such as an enterprise email address) and password combination. LDAP authenticates the login credentials by verifying that the user name and password match an existing user in the LDAP directory.

In HP CSA, LDAP is used to:

- Authenticate a user's login to the Cloud Service Management Console and Marketplace Portal
- Authenticate a user's access to information
- Authorize a user's access to information
- Retrieve information about a user's manager for approvals
- Retrieve information about a user's group membership for approvals

These functions are configured when you configure LDAP and access control for an organization.

Before you configure LDAP for the Cloud Service Management Console or Marketplace Portal, you should be familiar with your enterprise LDAP server and LDAP configuration tasks.

Note: The user object configured in LDAP that is used to log in to HP Cloud Service Automation and by which users can be identified should be configured to contain the following attribute types:

- User Email - Required. This attribute type designates the email address of the user to which to send email notifications. Common LDAP attribute names for email include **mail**, **email**, and **userPrincipalName**. If the value for this attribute in the user object in LDAP is empty or not valid, the user for whom the value is empty or not valid does not receive email notifications.
- Manager Identifier - Required. This attribute type identifies the manager of the user. A common LDAP attribute name for a user's manager is **manager**. If the value for this attribute in the user object in LDAP is empty or not valid, approval policies that use the User Context Template will fail.
- Manager Identifier Value - Required. This attribute type describes the value of the manager identifier. A common value for the manager identifier in LDAP is the **dn** (distinguished name) of the manager's user object. If the manager's user object cannot be located based on the values for manager identifier and manager identifier value, approval policies that use the User Context Template will fail.

The group object configured in LDAP must contain the following attribute type:

- Group Membership - Required. This attribute type identifies a user as belonging to the group. Common LDAP attribute names that convey group membership include **member** and **uniqueMember**.

The attribute names configured in your LDAP directory for these attribute types are used when configuring an organization's LDAP in the Cloud Service Management Console.

Note: Do not create users in your LDAP directory that match the out-of-the-box users provided by HP Cloud Service Automation (the out-of-the-box users are `admin`, `cdaInboundUser`, `csaCatalogAggregationTransportUser`, `csaReportingUser`, `csaTransportUser`, `idmTransportUser`, and `ooInboundUser`). Creating the same users in LDAP may allow the out-of-the-box users unintended access to the Cloud Service Management Console or give the LDAP users unintended privileges.

Configure the HP CSA Truststore Properties

You must configure information about the HP CSA's keystore. Do the following:

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor.
2. Enter values for the `csaTruststore` and `csaTruststorePassword` properties.

Property	Description
csaTruststore	Required. The HP Cloud Service Automation keystore that stores trusted Certificate Authority certificates. **Note:** Use only forward slashes (/) as your path separators.
csaTruststorePassword	Required. The encrypted password of the HP Cloud Service Automation keystore (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

For more information about these properties, refer to "Cloud Service Management Console Properties" on page 218.

3. Save and exit the file.

4. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Location of the HP CSA Truststore

The location of the HP CSA truststore depends on the JRE you are using with HP CSA and where the JRE has been installed.

The following are examples of where the HP CSA truststore may be located.

- If you are using the JRE that is installed with HP CSA (OpenJDK JRE), the truststore is located in the following location:

  `$CSA_HOME/openjre/lib/security/cacerts`

  For example: `/usr/local/hp/csa/openjre/lib/security/cacerts`

- If you are using an Oracle JRE, the truststore may be found in the following location:

  `<JRE_HOME>/lib/security/cacerts`

  For example, if you installed the Oracle JRE in `/usr/local/bin`, the truststore may be located at: `/usr/local/bin/jre1.7.0_71/lib/security/cacerts`

Request Software Licenses

HP CSA version 4.50 requires a software license. HP CSA licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP CSA version 4.50, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

After upgrade to HP CSA version 4.50, when you log in to the Cloud Service Management Console, all HP CSA version 4.10 or 4.2x licenses are valid and are automatically added.

> **Note:** HP CSA version 4.50 licenses are not compatible with HP CSA versions 4.01 or 4.10. That is, you cannot add HP CSA version 4.50 licenses to HP CSA versions 4.01 or 4.10.

The following topics are covered in this section:

- Request a software license
- Request a software license for a clustered environment
- Request a software license for a system with an updated IP address
- Request an emergency key

For information on how to view, add, or delete a license, refer to the *HP Cloud Service Management Console Help*.

Request a Software License

If you received an Electronic Delivery Receipt, use the link to the licensing portal located in the receipt and follow the online instructions to request a software license. Otherwise, to access the licensing portal, go to http://www.hp.com/software/licensing, enter your Entitlement Order Number, and follow the online instructions to request a software license.

Refer to the *Software License Activation Quick Start Guide* for more information about requesting a software license.

IP Address Limitations

When you request a software license, you must supply the IP address (IPv4 or Ipv6) of the system on which HP CSA is installed.

Do NOT use the following IP addresses when requesting a software license:

- Loopback address - 127.0.0.1 (IPv4) or ::1 (IPv6)

Request a Software License for a Clustered Environment

If you are configuring HP CSA in a clustered environment, use the IP address of the load balancer (in the examples given in the *Configuring an HP CSA Cluster for High Availability Using an Apache Web Server*, this is the APACHE_IP_ADDR; in the examples given in the *Configuring an HP CSA Cluster for High Availability Using a Load Balancer*, this is the LOAD_BALANCER_IP_ADDR). The license should be installed on only one node in the clustered environment.

Request a Software License for a System with an Updated IP Address

If you change the IP address of the system on which HP CSA is running, you must request a new software license.

If you immediately add the new license without restarting HP CSA, the license will not be accepted. You must restart HP CSA before adding the new license. To restart CSA, see "Restart HP CSA" on page 129. For more information about managing software licenses, refer to the *HP Cloud Service Management Console Help*.

Enable TLS on Your Web Browser

The Cloud Service Management Console is configured to require https (http over a secure connection) for client browsers. Specifically, the Cloud Service Management Console is configured to use the TLS protocol. You must enable TLS 1.0 as the required minimum protocol for the browser, and, if applicable, disable the SSL protocols.

Enable your Web browser to use the TLS protocol:

Chrome, Ubuntu

1. Exit or kill all Chrome sessions.
2. Edit the `/usr/share/applications/google-chrome.desktop` file.
3. For every line that starts with `Exec`, add the following argument:

   --ssl-version-min=tls1

4. Save and exit the file.

Chrome, Red Hat Enterprise Linux

1. Exit or kill all Chrome sessions.
2. When invoking the browser from the command line, add the following argument:

--ssl-version-min=tls1

Microsoft Internet Explorer

1. Open the **Tools** menu (click on the tools icon or type Alt - x) and select **Internet options**.
2. Select the **Advanced** tab.
3. Scroll down to the bottom of the **Settings** section.
4. If TLS is not enabled, select the checkboxes next to **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**.
5. Disable SSL 2.0 and SSL 3.0, if enabled (recommended). Unselect the checkbox next to **Use SSL 2.0** and/or **Use SSL 3.0**.
6. Click **OK**.

Firefox

1. Launch the Firefox browser.
2. In the Location Bar (address bar), enter **about:config** and press **Enter**.
3. In the Search box, enter **security.tls** and press **Enter**.
4. Double-click **security.tls.version.min**.
5. Set the value to **1** and click **OK**.

Configure the Provider Organization

1. Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

   Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

2. Log in to the Cloud Service Management Console as a CSA Administrator (refer to the *HP Cloud Service Automation Concepts Guide* and HP Cloud Service Management Console Help for more information about the CSA Administrator role).
3. Click the **Organizations** tile.

In the left-navigation frame, the provider organization icon (((•))) appears to the right of the provider organization that is automatically set up (CSA-Provider). You may modify the provider organization, as needed. However, you cannot delete it. There can be only one provider organization.

4. In the left-navigation frame, select the provider organization.

5. Configure the provider organization by selecting and entering information into each section of the organization's navigation frame (General Information, LDAP, Access Control, Email Notifications, and Catalogs). Refer to the *HP Cloud Service Management Console Help*, which is available in a printable PDF format, for more information about the fields in each section. This document is available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Add a Software License

HP CSA version 4.50 requires a software license. HP CSA licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP CSA version 4.50, when you log in to the Cloud Service Management Console, a temporary 90-day trial license is activated. Once the trial license expires, you are limited to 25 OSIs. If you created more than 25 OSIs during the trial period, you cannot create any additional OSIs. You can add more licenses at any time to increase your OSI capacity.

After upgrade to HP CSA version 4.50, when you log in to the Cloud Service Management Console, all HP CSA version 4.10 or 4.2x licenses are valid and are automatically added.

> **Note:** HP CSA version 4.50 licenses are not compatible with HP CSA versions 4.01 or 4.10. That is, you cannot add HP CSA version 4.50 licenses to HP CSA versions 4.01 or 4.10.

Before you can add a software license, you must request a license using the licensing portal. See "Request Software Licenses" on page 17 for more information.

To add a software license, log in to the Cloud Service Management Console as the CSA Administrator. From the **Options** menu, select **Licensing**. For more detailed information about adding a license, refer to the *HP Cloud Service Management Console Help*.

For information on how to view or delete a license, refer to the *HP Cloud Service Management Console Help*.

Proxy Configuration for Resource Providers Outside the Internal Network

If you are using a network proxy server to communicate with a resource provider outside of the internal network (the resource provider's service access point is located outside of the internal network), configure HP CSA and HP Operations Orchestration to use this proxy server.

If you are using a network proxy server to communicate with a resource provider outside of the internal network, proxy configuration is required in the following situations:

- HP CSA - Validating the accessibility of a resource provider's URL. When a resource provider is created or modified, accessibility of the provider URL is validated with an HTTP or HTTPS GET call.
- HP Operations Orchestration - Contacting a resource provider. When an HP Operations Orchestration workflow provisioning step is executed, HP Operations Orchestration attempts to contact the resource provider.

If you do not configure the proxy server, you may see a Provider Validation Failed message when creating or updating a resource provider whose service access point is located outside of the internal network. Or, provisioning of a design fails when HP Operations Orchestration is unable to communicate with a resource provider that is located outside of the internal network.

To configure the proxy server for HP CSA and HP Operations Orchestration, do the following:

1. On the system running HP CSA, open the `$CSA_HOME/jboss-as/bin/standalone.conf` file in a text editor.
2. After the last uncommented line that sets the JAVA_OPTS property, add the following lines:

   ```
   # HTTP Proxy Settings
   JAVA_OPTS= "$JAVA_OPTS -Dhttp.proxyHost=<proxy.company.com>
   -Dhttp.proxyPort=<proxy_port>"

   # HTTPS Proxy Settings
   JAVA_OPTS= "$JAVA_OPTS -Dhttps.proxyHost=<proxy.company.com>
   -Dhttps.proxyPort=<proxy_port>"

   # HTTP/HTTPS hosts not handled by the proxy
   JAVA_OPTS= "$JAVA_OPTS -Dhttp.nonProxyHosts=mycsaserver\|localhost\|127.*\|10.*
   "
   ```

   where <*proxy.company.com*> is the fully-qualified domain name of the proxy server, <*proxy_port*> is the port used to communicate with the proxy server, and `\|` is the separator used when defining more than one non-proxy host.
3. Save and exit the file.

4. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

5. If you have integrated with HP Operations Orchestration version 9.07, do the following:

   a. Log in to HP Operations Orchestration Studio.

   b. Open the **Configuration** folder.

   c. Right-click the **System Properties** folder and select **New**.

   d. In the dialog, enter **CSA_Proxy_Host** and click **OK**.

   e. Set the **Property Value** to the fully-qualified domain name of the proxy server and click **OK**.

   f. Right-click the **System Properties** folder and select **New**.

   g. In the dialog, enter **CSA_Proxy_Port** and click **OK**.

   h. Set the **Property Value** to the port used to communicate with the proxy server and click **OK**.

6. If you have integrated with HP Operations Orchestration version 10.21.0001, do the following:

   a. Log in to HP Operations Orchestration Central.

   b. Click the **Content Management** button.

   c. Select **Configuration Items** > **System Properties**.

   d. Click the **Add** icon.

   e. Enter the following information if it is not already configured:

Field	Description
Name	CSA_Proxy_Host
Override Value	The fully-qualified domain name of the proxy server.
Name	CSA_Proxy_Port
Override Value	The port used to communicate with the proxy server.

   f. Click **Save**.

Chapter 3: Secure Connections

This chapter provides general information about configuring secure connections between HP CSA and some commonly used components of HP CSA and securing internal communication. You should consult your security expert for more detailed information about configuring secure connections in your environment.

> **Note:** HP CSA only accepts secure connections using the TLSv1 protocol. If you are integrating with an application and are using secure connections, you must configure the application to use the TLSv1 protocol with HP CSA.

Information includes:

- "Configure Secure Connections for Client Browsers" on the next page (required when the HP CSA self-signed certificate expires)
- "Configure Secure Connections for LDAP" on page 49 (required if the LDAP server requires a secure connection)
- "Configure Secure Connections for SMTP" on page 49 (required if the SMTP server requires a secure connection)
- "Configure Secure Connections for an Oracle Database" on page 50 (required if the Oracle database requires a secure connection)
- "Configure Secure Connections for Microsoft SQL Server" on page 53 (required if Microsoft SQL Server requires a secure connection)
- "Configure Secure Connections for HP Operations Orchestration Load Balancer" on page 54 (required if you are running the HP OO LB server and it requires a secure connection)
- "Configure Secure Internal Communication" on page 56 (recommended)

The function of http over a secure connection is configured by the `com.hp.csa.service.ssl.certificate.validation` property in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file and the `strictSSL` attribute in the `$CSA_HOME/portal/conf/mpp.json` file. That is, http over a secure connection can be configured to encrypt the connection only or http over a secure connection can be configured to encrypt the connection, validate the certificate's expiration date, verify the certificate's hostname, and authenticate the certificate. Refer to the *Secure Connections* section in "Cloud Service Management Console Properties" on page 218 for more information about the `com.hp.csa.service.ssl.certificate.validation` property and the *Provider Attributes* and *Identity Management Component Attributes* sections in "Marketplace Portal Attributes" on page 255 for more information about the `strictSSL` attribute.

Configure Secure Connections for Client Browsers

The Cloud Service Management Console is configured to require https (http over a secure connection) for client browsers. For a secure connection to be established, a certificate must first be installed on the HP Cloud Service Automation (HP CSA) server.

A self-signed certificate is created and configured when HP CSA is installed and is configured with the fully-qualified domain name that was entered during the installation. This self-signed certificate is used when https browser requests are issued for the Cloud Service Management Console and expires 120 days after HP CSA is installed.

When client browsers connect to the Cloud Service Management Console in this default configuration, the client browser will usually issue warnings that the certificate was not issued by a trusted authority. The end user can choose to continue to the Web site or close the browser.

Although the self-signed certificate can be used in production, HP recommends that you replace this certificate. You can configure a trusted third-party Certificate Authority-signed or subordinate Certificate Authority-signed certificate (see "Configure HP CSA to Use a Trusted Certificate Authority-Signed or Subordinate Certificate Authority-Signed Certificate" on page 26) or configure an internal Certificate Authority-signed certificate (see "Configure HP CSA to Use an Internal Certificate Authority-Signed Certificate" on page 36). If the self-signed certificate expires before you are ready to move to production, you can replace the expired self-signed certificate by configuring a new self-signed certificate (see "Configure HP CSA to Use a Self-Signed Certificate" on page 40).

The following sections describe some common scenarios of configuring secure connections for HP CSA and the Marketplace Portal:

- "Configure HP CSA to Use a Trusted Certificate Authority-Signed or Subordinate Certificate Authority-Signed Certificate" on page 26
- "Configure HP CSA to Use a Certificate Authority-Signed Certificate and a Certificate Authority-Provided Keystore" on page 32
- "Configure HP CSA to Use an Internal Certificate Authority-Signed Certificate" on page 36
- "Configure HP CSA to Use a Self-Signed Certificate" on page 40

Note: Certificate chains require additional configuration and general information about importing a chain of certificates is provided in this section. However, you should consult your security expert for more detailed information when using certificate chains in your environment.

Wildcard certificates do not require special configuration.

If one of these scenarios does not match your situation, follow these general guidelines:

1. Obtain a root certificate and signed certificate and/or keystore. The root certificate is used to authenticate the signed certificate. The keystore stores the signed certificate. If you are

generating a self-signed certificate, the self-signed certificate is used as the root certificate. If you need to create a certificate signing request to obtain this information, look for the steps to "Create a Keystore and Self-Signed Certificate" and "Create a Certificate Signing Request" for more detailed information.

2. Import the root certificate into the JRE's truststore. Look for the step to "Import the Certificate Authority's Root Certificate" for detailed instructions on how to import the root certificate into the JRE's keystore.

3. Complete one of the following steps, based on if you have a signed certificate only, a keystore only, or if you have both a signed certificate and keystore.

   - If you have a signed certificate only, do the following:

     i. Create and import the certificate into a JKS keystore. Look for the step to "Import the Internal Certificate Authority-Signed Certificate" for more detailed information on how to create and import the certificate into a JKS keystore.

        If the signed certificate contains a chain of certificates, you must copy the root certificate and each intermediate certificate in the chain to a separate certificate file and import each certificate file into the keystore in the following order (each certificate must have a unique alias):

        - root certificate

        - intermediate or subordinate certificate(s) in hierarchical order

        - primary or end-user certificate

        Use the signed certificate as the primary certificate. You will use the alias of the primary certificate when you configure the Web server. Work with your security expert to determine if the signed certificate contains a chain of certificates and to copy each certificate to a separate file.

     ii. Configure the Marketplace Portal. This step includes converting the JKS keystore into a PKCS#12 keystore used by the Marketplace Portal. Look for the step to "Configure the Marketplace Portal" for more detailed information.

   - If you have a keystore only, do the following:

     i. Determine the type of keystore you have. You must have two keystore types: JKS and PKCS#12 (HP CSA and the Marketplace Portal use two different types of keystores). Convert the existing keystore into the type that you need. Look for the step to "Convert the Certificate Authority-Provided Keystore" for more detailed information on how to generate both of the required keystores.

     ii. Export the certificate from the keystore. You will need to provide the name and location of the certificate file when configuring the Marketplace Portal. Look for the step to "Export the Self-Signed Certificate" for more detailed information on how to export a certificate from a keystore.

iii. Configure the Marketplace Portal. You can skip the steps to convert the keystore to PKCS#12 format as you have already completed these steps. Look for the step to "Configure the Marketplace Portal" for more detailed information.

- If you have both the signed certificate and keystore, do the following:

  i. Determine the type of keystore you have. You must have two keystore types: JKS and PKCS#12 (HP CSA and the Marketplace Portal use two different types of keystores). Convert the existing keystore into the type that you need. Look for the step to "Convert the Certificate Authority-Provided Keystore" for more detailed information on how to generate both of the required keystores.

  ii. Configure the Marketplace Portal. You can skip the steps to convert the keystore to PKCS#12 format as you have already completed these steps. Look for the step to "Configure the Marketplace Portal" for more detailed information.

4. Configure the Web server. This step configures HP CSA to use the JKS keystore. Look for the step to "Configure the Web Server" for more detailed information.

5. Configure client browsers. This step is optional and tests whether or not the browser on a client system is configured to trust certificates signed by your Certificate Authority. Look for the step to "Configure Client Browsers" for more detailed information.

6. Test secure connections to the Cloud Service Management Console. Test the connection to the Cloud Service Management Console. Look for the step to "Test Secure Connections" for more detailed information.

Configure HP CSA to Use a Trusted Certificate Authority-Signed or Subordinate Certificate Authority-Signed Certificate

This section describes the process you should follow to obtain, install, and configure a trusted third-party Certificate Authority-signed or subordinate Certificate Authority-signed certificate for use by HP CSA. The process by which you acquire a certificate depends on your organization. If you are obtaining a certificate from a trusted third-party Certificate Authority, such as Verisign, perform the following general steps, which are described in detail below. If you are generating and/or obtaining a certificate from an internal Certificate Authority, such as a corporate Certificate Authority, you should perform the general steps in "Configure HP CSA to Use an Internal Certificate Authority-Signed Certificate" on page 36.

1. Create a keystore and a self-signed certificate

2. Create a certificate signing request

3. Submit the certificate signing request to a Certificate Authority

4. Import the Certificate Authority's root certificate

5. Import the Certificate Authority-signed certificate

6. Configure the Marketplace Portal

7. Configure the Web server

8. Configure client browsers

9. Test the secure connection

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed (for example, `/usr/local/hp/csa`) and the `keytool` utility is included with the JRE.

Also, the following instructions are applicable for subordinate Certificate Authorities. Wherever the Certificate Authority is mentioned, the subordinate Certificate Authority is implied. For example, if the content states to submit the certificate to a Certificate Authority, you may also submit the certificate to a subordinate Certificate Authority.

Step 1: Create a Keystore and Self-Signed Certificate

Create a self-signed certificate to send with your request to a Certificate Authority by doing the following:

1. Open a command prompt and change directories to `$CSA_HOME`.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -genkeypair -alias csa_ca_signed
   -validity 365 -keyalg rsa -keysize 2048 -keystore
   ./jboss-as/standalone/configuration/.keystore_ca_signed
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

   You can use different values for `-alias`, `-validity`, `-keysize` and `-keystore`. These instructions assume that you will use the `-alias` and `-keystore` values recommended here; you will have to adjust the commands accordingly if you use different values.

3. Enter a keystore password.

   This password is used to control access to the keystore. This password must be the same as the password you enter for the key later in this procedure.

4. When you are prompted for your first and last name, enter the fully qualified domain name of the HP CSA server.

5. Follow the prompts to enter the remaining organization and location values.

6. Enter the keystore password you supplied earlier to use as the key password.

   Although `keytool` allows you to enter different passwords for the keystore and the key, the two passwords must be the same to work with HP CSA.

Step 2: Create a Certificate Signing Request

To enable a Certificate Authority to sign the self-signed certificate, you will need to create a Certificate Signing Request using the following procedure:

1. Open a command prompt and change directories to `$CSA_HOME`.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -certreq -alias csa_ca_signed
   -file /tmp/csacsr.txt -keystore ./jboss-as/standalone/configuration/.keystore_
   ca_signed
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When you are prompted for a password, enter the password you supplied for the keystore and key when you created the keystore and self-signed certificate in step 1.

Step 3: Submit the Certificate Signing Request to a Certificate Authority

Submit the Certificate Signing Request to the Certified Authority following the procedure used by your organization or the third-party provider. After the submission has been processed, you will receive a Certificate Authority-signed certificate and a root certificate for the Certificate Authority.

In our example, we will assume the Certificate Authority's root certificate is named `csaca.crt`, the Certificate Authority-signed certificate is named `csa_ca_signed.crt`, and that both are located in /tmp.

Step 4: Import the Certificate Authority's Root Certificate

This step configures the JRE so it trusts the Certificate Authority that has signed your certificate. The JRE ships with a list of common, trusted Certificate Authority certificates that are stored in a keystore named `cacerts`. If the Certificate Authority used to sign your certificate is well known, it is likely that this root certificate is already present in the `cacerts` keystore. It is recommended that you perform the following steps even if you suspect that the certificate is already installed. The `keytool` command will detect if the certificate is already present, and you can exit the import process if the certificate exists.

1. Open a command prompt.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias csaca -file /tmp/csaca.crt -
   trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When prompted for the keystore password, enter `changeit`.

4. Enter `yes` when prompted to trust the certificate.

Step 5: Import the Certificate Authority-Signed Certificate

1. The Certificate Authority-signed certificate (`csa_ca_signed.crt`) contains a chain of certificates and you must copy the root and any intermediate certificates in the chain to separate files. Work with your security expert to copy each certificate to a separate file.

2. Open a command prompt and change directories to `$CSA_HOME`.

3. Import the certificate file(s):

   You must import each separate file in the following order (each certificate must have a unique alias):

   - root certificate

   - intermediate or subordinate certificate(s) in hierarchical order

   - primary or end-user certificate

   For example, if the Certificate Authority-signed certificate contains three certificates (root, intermediate, and primary) and you copied the root certificate to `/tmp/root.crt` and the intermediate certificate to `/tmp/intermediate.crt` (you will use the Certificate Authority-signed certificate as the primary certificate), run the following commands in the following order to import each certificate:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias csa_ca_signed_root -file
   /tmp/root.crt -trustcacerts -keystore
   ./jboss-as/standalone/configuration/.keystore_ca_signed
   ```

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias csa_ca_signed_intermediate -file
   /tmp/intermediate.crt -trustcacerts -keystore
   ./jboss-as/standalone/configuration/.keystore_ca_signed
   ```

```
$CSA_JRE_HOME/bin/keytool -importcert -alias csa_ca_signed -file /tmp/csa_ca_
signed.crt -trustcacerts -keystore
./jboss-as/standalone/configuration/.keystore_ca_signed
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Use the alias of the primary certificate (`csa_ca_signed`) and keystore name (`$CSA_HOME/jboss-as/standalone/configuration/.keystore_ca_signed`) when you configure the Web server.

4. When prompted, enter the password for the key and keystore.

   Use this password when you configure the Web server.

Step 6: Configure the Marketplace Portal

This step converts the HP CSA keystore to a PKCS#12 archive and configures the Marketplace Portal to use the Certificate Authority-signed certificate.

1. Open a command prompt and navigate to `$CSA_HOME`.

2. Convert the HP CSA keystore to a PKCS#12 archive. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importkeystore -srckeystore
   ./jboss-as/standalone/configuration/.keystore_ca_signed -deststoretype PKCS12 -
   destkeystore ./portal/conf/.mppkeystore_ca_signed
   ```

3. When prompted, enter the password for the PKCS#12 archive. You will need this password when you configure the `passphrase` attribute later in this section.

4. When prompted, enter the password for the HP CSA keystore (changeit).

5. Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.

6. Update the `ca` attribute value for the provider. Enter the path to the certificate file that you imported in step 5. For example, `/tmp/csa_ca_signed.crt`. If you imported a chain of certificates, use the certificate file of the primary certificate.

7. Update the `ca` attribute value for the idmProvider. Enter the path to the certificate file that you imported in step 5. For example, `/tmp/csa_ca_signed.crt`. If you imported a chain of certificates, use the certificate file of the primary certificate.

8. Update the `pfx` attribute value. Enter the name of the PKS#12 archive you created earlier. For example, `../conf/.mppkeystore_ca_signed`.

9. Update the `passphrase` attribute value. Enter the encrypted password used to access the `.mppkeystore_ca_signed` archive (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

10. Save and exit the file.

Step 7: Configure the Web Server

1. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

2. Locate the following entry:

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
   keystore-password="changeit"/>
   ```

3. Set the `path` attribute to the keystore you used in step 5, set the `password` attribute to the value that corresponds to the password you selected for the keystore, and add the `alias` attribute and set it to the alias you used in step 5.

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore_ca_
   signed" keystore-password="keystorePassword" alias="csa_ca_signed"/>
   ```

   Note: If you imported a chain of certificates, use the alias of the primary certificate.

   Note: This example stores the password in clear text. If you want to use an encrypted password, see "Masking Passwords in standalone.xml Using the JBoss vault Script" on page 45 for information about creating a password vault for JBoss.

4. Restart the HP Cloud Service Automation service.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

5. After the service has started, review the log files in `$CSA_HOME/jboss-as/standalone/log/` and verify that no TLS or keystore errors are present.

Step 8: Configure Client Browsers

The client browser must be configured to trust certificates that are signed by the Certificate Authority. In most situations, this step will already have occurred. Client browsers are likely to already trust well-known third-party Certificate Authorities, or will have previously accessed and trusted Web sites that use internal Certificate Authority root certificates.

To test whether or not the browser on a client system is configured to trust certificates signed by your Certificate Authority, open a supported Web browser and navigate to `https://<csahostname>:8444/csa`. If you do not see a certificate warning, then the browser is configured properly.

If client browsers need to be configured to trust certificates signed by your Certificate Authority, then you will need to make the root certificate available to clients so it can be installed in the browser. The process of installing the root certificate will vary based on the browser.

- **Microsoft Internet Explorer** and **Chrome**: From Windows Explorer, double-click on the `.crt` file to begin the import process. Install the certificate in the Trusted Root Certification Authorities store. For information on how to import the certificate, refer to the browser's online documentation.
- **Firefox**: To begin the import process, select **Tools > Options**, select **Advanced**, select the **Encryption** tab, and click **View Certificates**. Import the root certificate into the Authorities tab. For information on how to import the certificate, refer to the browser's online documentation.

Step 9: Test Secure Connections

To test the connection to the Cloud Service Management Console, on a client system, open a supported Web browser and navigate to `https://`*`<csahostname>`*`:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system that was used when the certificate was created. If the client browser is configured to accept the Certificate Authority's root certificate and the Web application opens without a certificate warning, then you have successfully configured HP Cloud Service Automation to use a Certificate Authority-signed certificate. If a certificate warning is displayed, review steps 1-8 to be sure they were followed as documented.

Configure HP CSA to Use a Certificate Authority-Signed Certificate and a Certificate Authority-Provided Keystore

This section describes the process you should follow to install and configure a root certificate, Certificate Authority-signed certificate, and Certificate Authority-provided keystore for use by HP CSA. In this example, the Certificate Authority provides you with a root certificate, signed certificate, and a keystore containing the signed certificate. A Certificate Authority may provide you with a keystore if you are using a wildcard certificate.

Perform the following general steps, which are described in detail below:

1. Import the Certificate Authority's root certificate
2. Convert the Certificate Authority-provided keystore
3. Determine the alias for the certificate from the JKS keystore
4. Configure the Marketplace Portal
5. Configure the Web server
6. Configure client browsers
7. Test the secure connection

> **Note:** In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed (for example, `/usr/local/hp/csa`) and the `keytool` utility is included with the JRE.

In this example, we will assume you are given a Certificate Authority-signed certificate (referred to as `csa_ca_signed.crt`), a Certificate Authority's root certificate (referred to as `ca_root.crt`), and a keystore provided by the Certificate Authority that contains the Certificate Authority-signed certificate (referred to as `.keystore_caprovided`). All files are located in /tmp.

Step 1: Import the Certificate Authority's Root Certificate

This step configures HP CSA's JRE so it trusts the Certificate Authority that has signed the certificate by importing the Certificate Authority's root certificate into a keystore named `cacerts` that is shipped with the JRE. The JRE ships with a list of common, trusted Certificate Authority certificates that are stored in this keystore. If the Certificate Authority used to sign the certificate is well known, it is likely that this root certificate is already present in this keystore. It is recommended that you perform the following steps even if you suspect that the certificate is already installed. The keytool command will detect if the root certificate is already present, and you can exit the import process if the certificate exists.

1. Open a command prompt.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias csaca -file /tmp/ca_root.crt -
   trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When prompted for the keystore password, enter `changeit`.

4. Enter `yes` when prompted to trust the certificate.

Step 2: Convert the Certificate Authority-Provided Keystore

The keystore used by HP CSA must be in JKS format. The keystore used by the Marketplace Portal must be in PKCS#12 format. You will need to provide both types of keystores. This section provides the tasks to convert a JKS keystore to a PKCS#12 keystore and a PKCS#12 keystore to a JKS keystore. If your Certificate Authority provided you a keystore in another format, ask your Certificate Authority how to convert it to either the JKS or PKCS#12 format. Then, complete the tasks in this step to create both required keystore formats.

1. Determine the format of the Certificate Authority-provided keystore. If you do not know the format, ask the Certificate Authority for this information. If your Certificate Authority provided you a keystore in a format other than JKS or PKCS#12, ask your Certificate Authority how to convert it to either the JKS or PKCS#12 format.

2. Open a command prompt and change directories to `$CSA_HOME`.

3. To convert a JKS keystore to a PKCS#12 keystore, run the following command:

```
$CSA_JRE_HOME/bin/keytool -importkeystore -srckeystore /tmp/.keystore_
caprovided -deststoretype PKCS12 -destkeystore /tmp/.keystore_mpp
```

To convert a PKCS#12 keystore to a JKS keystore, run the following command:

```
$CSA_JRE_HOME/bin/keytool -importkeystore -srckeystore /tmp/.keystore_
caprovided -deststoretype JKS -destkeystore /tmp/.keystore_csa
```

4. When prompted, enter the password for the destination and source keystores. For simplicity, use the same passwords.

   Use this password when you configure the Marketplace Portal and the Web server.

Step 3: Determine the Alias for the Certificate from the JKS Keystore

Determine the alias for the certificate from the JKS keystore. You will need this alias when you configure the Web server.

If the Certificate Authority provided a JKS keystore, run the following command:

```
$CSA_JRE_HOME/bin/keytool -list -keystore /tmp/.keystore_caprovided
```

If you converted the Certificate Authority-provided keystore to JKS, run the following command:

```
$CSA_JRE_HOME/bin/keytool -list -keystore /tmp/.keystore_csa
```

If there is more than one entry displayed, contact the Certificate Authority and ask which alias to use for the certificate. If a certificate chain is being used, typically you would use the alias of the primary certificate.

Step 4: Configure the Marketplace Portal

This step configures the Marketplace Portal to use the root certificate and the PKCS#12 keystore.

1. Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.

2. Update the `ca` attribute value for the provider. Enter the path to the root certificate file. For example, `/tmp/ca_root.crt`.

3. Update the `ca` attribute value for the idmProvider. Enter the path to the root certificate file. For example, `/tmp/ca_root.crt`.

4. Update the `pfx` attribute value. Enter the name of the PKCS#12 keystore you created earlier. For example, if the Certificate Authority provided a PKCS#12 keystore, `/.keystore_caprovided`. If you converted the Certificate Authority-provided keystore to PKCS#12, `./.keystore_mpp`.

5. Update the `passphrase` attribute value. Enter the encrypted password used to access the PKCS#12 keystore (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. This is the password from step 2 (Convert

the Certificate Authority-Provided Keystore).

6. Save and exit the file.

Step 5: Configure the Web Server

1. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

2. Locate the following entry:

```
<keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
keystore-password="changeit"/>
```

3. Set the `path` attribute to the JKS keystore, set the `keystore-password` to the value that corresponds to the password you selected for the JKS keystore, and add the `alias` and set it to the alias you determined in step 3 (Determine the Alias for the Certificate from the JKS Keystore).

   For example, if the Certificate Authority provided a JKS keystore, update the entry to:

```
<keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore_
caprovided" keystore-password="keystorePassword" alias="<alias_from_step3>"/>
```

   For example, if you converted the Certificate Authority-provided keystore to JKS, update the entry to:

```
<keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore_csa"
keystore-password="keystorePassword" alias="<alias_from_step3>"/>
```

   > **Note:** This example stores the password in clear text. If you want to use an encrypted password, see "Masking Passwords in standalone.xml Using the JBoss vault Script" on page 45 for information about creating a password vault for JBoss.

4. Restart the HP Cloud Service Automation service.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

5. After the service has started, review the log files in `$CSA_HOME/jboss-as/standalone/log/` and verify that no TLS or keystore errors are present.

Step 6: Configure Client Browsers

The client browser must be configured to trust certificates that are signed by the Certificate Authority. In most situations, this step will already have occurred. Client browsers are likely to already trust well-known third-party Certificate Authorities, or will have previously accessed and trusted Web sites that use internal Certificate Authority root certificates.

To test whether or not the browser on a client system is configured to trust certificates signed by your Certificate Authority, open a supported Web browser and navigate to `https://<csahostname>:8444/csa`. If you do not see a certificate warning, then the browser is configured properly.

If client browsers need to be configured to trust certificates signed by your Certificate Authority, then you will need to make the root certificate available to clients so it can be installed in the browser. The process of installing the root certificate will vary based on the browser.

- **Microsoft Internet Explorer** and **Chrome**: From Windows Explorer, double-click on the `.crt` file to begin the import process. Install the certificate in the Trusted Root Certification Authorities store. For information on how to import the certificate, refer to the browser's online documentation.
- **Firefox**: To begin the import process, select **Tools > Options**, select **Advanced**, select the **Encryption** tab, and click **View Certificates**. Import the root certificate into the Authorities tab. For information on how to import the certificate, refer to the browser's online documentation.

Step 7: Test Secure Connections

To test the connection to the Cloud Service Management Console, on a client system, open a supported Web browser and navigate to `https://`*`<csahostname>`*`:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system that was used when the certificate was created. If the client browser is configured to accept the Certificate Authority's root certificate and the Web application opens without a certificate warning, then you have successfully configured HP Cloud Service Automation to use a Certificate Authority-signed certificate. If a certificate warning is displayed, review steps 1-6 to be sure they were followed as documented.

Configure HP CSA to Use an Internal Certificate Authority-Signed Certificate

This section describes the process you should follow to install and configure an internal root and internal Certificate Authority-signed certificate for use by HP CSA. An internal certificate is one that is generated by an internal Certificate Authority, such as a corporate or government Certificate Authority. For an internal Certificate Authority, you do not have to generate a self-signed certificate nor create a certificate signing request. The internal Certificate Authority should provide you with a root certificate and signed certificate.

Perform the following general steps, which are described in detail below:

1. Import the internal Certificate Authority's root certificate
2. Import the internal Certificate Authority-signed certificate
3. Configure the Marketplace Portal
4. Configure the Web server
5. Configure client browsers
6. Test the secure connection

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed (for example, `/usr/local/hp/csa`) and the `keytool` utility is included with the JRE.

In this example, we will assume you are given an internal Certificate Authority-signed certificate (referred to as `csa_internalca_signed.crt`), an internal Certificate Authority's root certificate (referred to as `csainternalca.crt`), and both certificates are located in /tmp.

Step 1: Import the Certificate Authority's Root Certificate

This step configures the JRE so it trusts the internal Certificate Authority that has signed your certificate by importing the internal Certificate Authority into a keystore named `cacerts` that is shipped with the JRE.

1. Open a command prompt.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias csainternalca -file
   /tmp/csainternalca.crt -trustcacerts -keystore $CSA_JRE_
   HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When prompted for the keystore password, enter `changeit`.

4. Enter `yes` when prompted to trust the certificate.

Step 2: Import the Internal Certificate Authority-Signed Certificate

1. The internal Certificate Authority-signed certificate (`csa_internalca_signed.crt`) contains a chain of certificates and you must copy the root and any intermediate certificates in the chain to separate files. Work with your security expert to copy each certificate to a separate file.

2. Open a command prompt and change directories to `$CSA_HOME`.

3. Import the certificate file(s):

   You must import each separate file in the following order (each certificate must have a unique alias):

   - root certificate
   - intermediate or subordinate certificate(s) in hierarchical order
   - primary or end-user certificate

For example, if the internal Certificate Authority-signed certificate contains three certificates (root, intermediate, and primary) and you copied the root certificate to `/tmp/root.crt` and the intermediate certificate to `/tmp/intermediate.crt` (you will use the internal Certificate Authority-signed certificate file as the primary certificate), run the following commands in the following order to import each certificate:

```
$CSA_JRE_HOME/bin/keytool -importcert -alias csa_internalca_signed_root -file
/tmp/root.crt -trustcacerts -keystore
./jboss-as/standalone/configuration/.keystore_internalca_signed
```

```
$CSA_JRE_HOME/bin/keytool -importcert -alias csa_internalca_signed_intermediate
-file /tmp/intermediate.crt -trustcacerts -keystore
./jboss-as/standalone/configuration/.keystore_internalca_signed
```

```
$CSA_JRE_HOME/bin/keytool -importcert -alias csa_internalca_signed -file
/tmp/csa_internalca_signed.crt -trustcacerts -keystore
./jboss-as/standalone/configuration/.keystore_internalca_signed
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Use the alias of the primary certificate (`csa_internalca_signed`) and keystore name (`$CSA_HOME/jboss-as/standalone/configuration/.keystore_internalca_signed`) when you configure the Web server.

4. When prompted, enter the password for the key and keystore.

   Use this password when you configure the Web server.

Step 3: Configure the Marketplace Portal

This step converts the HP CSA keystore to a PKCS#12 archive and configures the Marketplace Portal to use the internal Certificate Authority root certificate.

1. Open a command prompt and navigate to `$CSA_HOME`.

2. Convert the HP CSA keystore to a PKCS#12 archive. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importkeystore -srckeystore
   ./jboss-as/standalone/configuration/.keystore_internalca_signed -deststoretype
   PKCS12 -destkeystore ./portal/conf/.mppkeystore_internalca_signed
   ```

3. When prompted, enter the password for the PKCS#12 archive. You will need this password when you configure the `passphrase` attribute later in this section.

4. When prompted, enter the password for the HP CSA keystore (changeit).

5. Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.

6. Update the `ca` attribute value for the provider. Enter the path to the certificate file that you imported in step 2. For example, `/tmp/csa_internalca_signed.crt`. If you imported a chain of certificates, use the certificate file of the primary certificate.

7. Update the `ca` attribute value for the idmProvider. Enter the path to the certificate file that you imported in step 2. For example, `/tmp/csa_internalca_signed.crt`. If you imported a chain of certificates, use the certificate file of the primary certificate.

8. Update the `pfx` attribute value. Enter the name of the PKS#12 archive you created earlier. For example, `../conf/.mppkeystore_internalca_signed`.

9. Update the `passphrase` attribute value. Enter the encrypted password used to access the `.mppkeystore_internalca_signed` archive (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

10. Save and exit the file.

Step 4: Configure the Web Server

1. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

2. Locate the following entry:

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
   keystore-password="changeit"/>
   ```

3. Set the `path` attribute to the keystore you used in step 2, set the `keystore-password` attribute to the value that corresponds to the password you selected for the keystore, and add the `alias` attribute and set it to the alias you used in step 2.

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore_
   internalca_signed" keystore-password="keystorePassword" alias="csa_internalca_
   signed" />
   ```

   Note: If you imported a chain of certificates, use the alias of the primary certificate.

   Note: This example stores the password in clear text. If you want to use an encrypted password, see "Masking Passwords in standalone.xml Using the JBoss vault Script" on page 45 for information about creating a password vault for JBoss.

4. Restart the HP Cloud Service Automation service.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

5. After the service has started, review the log files in `$CSA_HOME/jboss-as/standalone/log/` and verify that no TLS or keystore errors are present.

Step 5: Configure Client Browsers

The client browser must be configured to trust certificates that are signed by the Certificate Authority. In most situations, this step will already have occurred. Client browsers are likely to already trust well-known third-party Certificate Authorities, or will have previously accessed and trusted Web sites that use internal Certificate Authority root certificates.

To test whether or not the browser on a client system is configured to trust certificates signed by your Certificate Authority, open a supported Web browser and navigate to `https://<csahostname>:8444/csa`. If you do not see a certificate warning, then the browser is configured properly.

If client browsers need to be configured to trust certificates signed by your Certificate Authority, then you will need to make the root certificate available to clients so it can be installed in the browser. The process of installing the root certificate will vary based on the browser.

- **Microsoft Internet Explorer** and **Chrome**: From Windows Explorer, double-click on the `.crt` file to begin the import process. Install the certificate in the Trusted Root Certification Authorities store. For information on how to import the certificate, refer to the browser's online documentation.

- **Firefox**: To begin the import process, select **Tools > Options**, select **Advanced**, select the **Encryption** tab, and click **View Certificates**. Import the root certificate into the Authorities tab. For information on how to import the certificate, refer to the browser's online documentation.

Step 6: Test Secure Connections

To test the connection to the Cloud Service Management Console, on a client system, open a supported Web browser and navigate to `https://`*`<csahostname>`*`:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system that was used when the certificate was created. If the client browser is configured to accept the Certificate Authority's root certificate and the Web application opens without a certificate warning, then you have successfully configured HP Cloud Service Automation to use a Certificate Authority-signed certificate. If a certificate warning is displayed, review steps 1-5 to be sure they were followed as documented.

Configure HP CSA to Use a Self-Signed Certificate

This section describes the process you should follow to obtain, install, and configure a self-signed certificate for use by HP CSA.

In general, HP recommends that you replace HP CSA's self-signed certificate with a Certificate Authority-signed certificate. However, you may consider replacing HP CSA's self-signed with a self-signed certificate you create in the following situations:

- HP CSA's self-signed certificate has expired and you do not want to configure a Certificate Authority-signed certificate at this time.
- The hostname that you entered when you installed HP CSA has changed (the hostname you entered during installation is used to configure HP CSA's self-signed certificate).
- You entered an IP address instead of the fully-qualified domain name when HP CSA was installed.
- Obtaining a Certificate Authority-signed certificate is not an option in your environment.

You should perform the following general steps, which are described in detail below:

1. Create a keystore and a self-signed certificate
2. Export the self-signed certificate
3. Import the self-signed certificate as a trusted certificate
4. Configure the Marketplace Portal
5. Configure the Web server
6. Configure client browsers (optional)
7. Test the secure connection

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed (for example, `/usr/local/hp/csa`) and the `keytool` utility is included with the JRE.

Step 1: Create a Keystore and Self-Signed Certificate

Create a self-signed certificate by doing the following:

1. Open a command prompt and change directories to `$CSA_HOME`.
2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -genkeypair -alias csa_self_signed
   -validity 365 -keyalg rsa -keysize 2048
   -keystore ./jboss-as/standalone/configuration/
   .keystore_self_signed [-ext san=ip:<ip_address>]
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed and `-ext san=ip:<ip_address>` is the option to specify the IP address of the system on which HP CSA is installed. This option is required if you specified an IP address instead of the fully-qualified domain name when you installed HP CSA. If you specified the fully-qualified domain name during installation, you may omit this option.

You can use different values for `-alias`, `-validity`, `-keysize` and `-keystore`. These instructions assume that you will use the `-alias` and `-keystore` values recommended here; you will have to adjust the commands accordingly if you use different values.

3. Enter a keystore password.

   This password is used to control access to the keystore. This password must be the same as the password you enter for the key later in this procedure.

4. When you are prompted for your first and last name, enter the fully qualified domain name of the HP CSA server.

5. Follow the prompts to enter the remaining organization and location values.

6. Enter the keystore password you supplied earlier to use as the key password.

   Although `keytool` allows you to enter different passwords for the keystore and the key, the two passwords must be the same to work with HP CSA.

Step 2: Export the Self-Signed Certificate

Export the self-signed certificate using the following procedure:

1. Open a command prompt and change directories to `$CSA_HOME`.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -export -alias csa_self_signed
   -file /tmp/csa_self_signed.crt
   -keystore ./jboss-as/standalone/configuration/
   .keystore_self_signed
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When you are prompted for a password, enter the keystore password used in step 1.

Step 3: Import the Self-Signed Certificate as a Trusted Certificate

This step configures the JRE so it trusts the self-signed certificate.

1. Open a command prompt.

2. Run the following command:

```
$CSA_JRE_HOME/bin/keytool -importcert -alias csa_self_signed
-file /tmp/csa_self_signed.crt -trustcacerts
-keystore $CSA_JRE_HOME/lib/security/cacerts
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. When prompted for the keystore password, enter `changeit`.

4. Enter `yes` when prompted to trust the certificate.

Step 4: Configure the Marketplace Portal

This step converts the HP CSA keystore to a PKCS#12 archive and configures the Marketplace Portal to use the self-signed certificate.

1. Open a command prompt and navigate to `$CSA_HOME`.

2. Convert the HP CSA keystore to a PKCS#12 archive. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importkeystore -srckeystore
   ./jboss-as/standalone/configuration/.keystore_self_signed -deststoretype PKCS12
   -destkeystore ./portal/conf/.mppkeystore_self_signed
   ```

3. When prompted, enter the password for the PKCS#12 archive. You will need this password when you configure the `passphrase` attribute later in this section.

4. When prompted, enter the password for the HP CSA keystore (changeit).

5. Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.

6. Update the `ca` attribute value for the provider. Enter the path to the certificate file that you imported in step 2. For example, `/tmp/csa_self_signed.crt`.

7. Update the `ca` attribute value for the idmProvider. Enter the path to the certificate file that you imported in step 2. For example, `/tmp/csa_self_signed.crt`.

8. Update the `pfx` attribute value. Enter the name of the PKS#12 archive you created earlier. For example, `../conf/.mppkeystore_self_signed`.

9. Update the `passphrase` attribute value. Enter the encrypted password used to access the `.mppkeystore_self_signed` archive (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

10. Save and exit the file.

Step 5: Configure the Web Server

1. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

2. Locate the following entry:

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
   keystore-password="changeit"/>
   ```

3. Set the `path` attribute to the keystore you used in step 2, set the `keystore-password` attribute to the value that corresponds to the password you selected for the keystore, and add the `key-alias` attribute and set it to the alias you used in step 2.

   ```
   <keystore path="$CSA_HOME/jboss-as/standalone/
   configuration/.keystore_self_signed" keystore-password="keystorePassword"
   alias="csa_self_signed"/>
   ```

   > **Note:** This example stores the password in clear text. If you want to use an encrypted password, see "Masking Passwords in standalone.xml Using the JBoss vault Script" on the next page for information about creating a password vault for JBoss.

4. Restart the HP Cloud Service Automation service.

   To restart HP CSA, on the server that hosts HP CSA, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop` `<embeddedHPOOinstallation>/central/bin/central start`.

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

5. After the service has started, review the log files in `$CSA_HOME/jboss-as/standalone/log/` and verify that no TLS or keystore errors are present.

Step 6: Configure Client Browsers (Optional)

Because the self-signed certificate is not signed by a Certificate Authority, when accessing the Cloud Service Management Console, warning messages are displayed in the browser (these messages do not affect normal operations of HP CSA). To avoid these warning messages, import the `csa_self_signed.crt` file or add an exception.

- **Microsoft Internet Explorer** and **Chrome**: From Windows Explorer, double-click on the `csa_self_signed.crt` file to begin the import process. Install the certificate in the Trusted Root Certification Authorities store. For information on how to import the certificate, refer to the browser's online documentation.

- **Firefox**: Add an exception by opening the browser and navigating to `https://<csahostname>:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system on which HP CSA is running. When the **This Connection is Untrusted** page opens, select **I Understand the Risks**, click the **Add Exception** button, verify the Server Location, and click **Confirm Security Exception**. For information on how to import the certificate, refer to the browser's online documentation.

Step 7: Test Secure Connections

To test the connection to the Cloud Service Management Console, on a client system, open a supported Web browser and navigate to `https://`*`<csahostname>`*`:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system that was used when the certificate was created. If the client browser is configured to accept the self-signed certificate (that is, you have completed step 6) and the Web application opens without a certificate warning, then you have successfully configured HP CSA to use a self-signed certificate. If you did not complete step 6, verify that the only certificate warning relates to the certificate not being issued by a trusted authority. If any other certificate warning is displayed, review steps 1-6 to be sure they were followed as documented.

Masking Passwords in standalone.xml Using the JBoss vault Script

JBoss provides a script that allows passwords in the `standalone.xml` file to be masked. The following tasks describe how to use the JBoss vault script and configure HP CSA to use the masked password.

1. Verify that the $JAVA_HOME environment variable has been defined and that $JAVA_HOME has been set to the directory in which the JRE that is used by HP CSA is installed (for example, `/usr/local/hp/csa/openjre`).

   To verify that $JAVA_HOME has been defined, from a command prompt, type:

   ```
   echo $JAVA_HOME
   ```

2. Create a keystore used by vault. This vault keystore is used to store the HP CSA keystore password.

   > **Note:** This example saves the vault keystore and encrypted vault file in the `$CSA_HOME/jboss-as/standalone/configuration/` directory (the contents of this directory are automatically backed up during an upgrade). You may choose to store the vault keystore and

> encrypted vault file in any location. However, you must remember to use those locations in subsequent steps in this task and, if those locations are not automatically backed up during upgrade, to manually back up the files before upgrade.

a. Open a command prompt.

b. Run the following command:

   ```
   <csa_jre>/bin/keytool -genkey -alias vault -validity 365 -keyalg rsa
   -keysize 2048 -keystore ./jboss-as/standalone/configuration/csa_
   vault.keystore
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

   You can use different values for `-alias`, `-validity`, `-keysize` and `-keystore`. These instructions assume that you will use the `-alias` and `-keystore` values recommended here; you will have to adjust the commands accordingly if you use different values.

c. Enter the vault keystore password (for example, csavault).

   This password is used to control access to the vault keystore. This password must be the same as the password you enter for the key in step e of this task.

d. Follow the prompts to enter your first and last name, organization, and location values.

e. Enter the key password. Click **Enter** to use the vault keystore password you supplied earlier (for example, csavault).

   Although `keytool` allows you to enter different passwords for the keystore and the key, the two passwords must be the same to work with HP CSA.

3. Run the vault script. The script will generate the masked password and the values to configure in the `standalone.xml` file in order to use the masked password.

   a. From the command prompt, make the vault script executable. Type: `chmod 775 $CSA_HOME/jboss-as/bin/vault.sh`

   b. Type: `$CSA_HOME/jboss-as/bin/vault.sh`

   c. Select **0** to start the interactive session.

   d. Enter the following information, when prompted, to configure the vault keystore:

Prompt	Description
Directory to store encrypted files	Directory in which the vault encrypted file is stored (for example, `$CSA_HOME/jboss-as/standalone/configuration`). Verify that a vault encrypted file (`ENC.dat`) does not already exist in this directory. If the file exists, select a different directory.
Keystore URL	The name and location of the vault keystore (for example, `$CSA_HOME/jboss-as/standalone/configuration/csa_vault.keystore`).
Keystore password (twice)	The password to the vault keystore (for example, csavault).
8 character salt	A random number (for example, 12345678).
Iteration count as a number	The number of times the HP CSA keystore password is hashed (for example, 25).
Keystore alias	The alias used to identify the HP CSA keystore password in the vault keystore (for example, vault).

e. Make a copy of the vault property block that is displayed. For example, copy:

```
<vault>
   <vault-option name="KEYSTORE_URL" value="$CSA_HOME/jboss-
as/standalone/configuration/csa_vault.keystore"/>
   <vault-option name="KEYSTORE_PASSWORD" value="MASK-2PtpNyQsI1E7t"/>
   <vault-option name="KEYSTORE_ALIAS" value="vault"/>
   <vault-option name="SALT" value="12345678"/>
   <vault-option name="ITERATION_COUNT" value="25"/>
   <vault-option name="ENC_FILE_DIR" value="$CSA_HOME/jboss-
as/standalone/configuration/"/>
</vault>
```

You will need to add this content to the `standalone.xml` file (the exact location is described in a later step).

f. Select **0** to store a secured attribute.

g. Enter the following information, when prompted, to generate the vault entry to use for the HP CSA keystore password in the `standalone.xml` file:

Prompt	Description
Secured attribute value (twice)	Enter the HP CSA keystore password (for example, changeit).
Vault Block	Enter a name for the vault block (for example, csa_ keystore).
Attribute Name	Enter the attribute being stored (for example, password).

Note the VAULT entry (for example, `VAULT::csa_keystore::password::1`). You will need this value when you configure the `standalone.xml` file.

h. Enter **2** to exit the script.

> **Note:** The vault script converts the format of the vault keystore (for example, $CSA_HOME/jboss-as/standalone/configuration/csa_vault.keystore) to JCEKS.

4. Open *$CSA_HOME*`/jboss-as/standalone/configuration/standalone.xml` in a text editor.

5. Locate the following entry for the HP CSA server keystore (this entry may have been modified):

```
<keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
keystore-password="changeit"/>
```

6. Update the entry by changing the value of the `keystore-password` attribute to the vault entry you generated (for example, `VAULT::csa_keystore::password::1`).

   For example:

```
<keystore path="$CSA_HOME/jboss-as/standalone/configuration/.keystore"
keystore-password="${VAULT::csa_keystore::password::1}"/>
```

7. Add the vault property block to `<server xmlns="urn:jboss:domain:1.3">` after the `system-properties` block. For example, using the example values, enter the following:

```
<server xmlns="urn:jboss:domain:1.3">
 .
 .
 .
<system-properties>
 .
 .
 .
</system-properties>
<vault>
   <vault-option name="KEYSTORE_URL" value="$CSA_HOME/jboss-
as/standalone/configuration/csa_vault.keystore"/>
   <vault-option name="KEYSTORE_PASSWORD" value="MASK-2PtpNyQsI1E7t"/>
   <vault-option name="KEYSTORE_ALIAS" value="vault"/>
   <vault-option name="SALT" value="12345678"/>
   <vault-option name="ITERATION_COUNT" value="25"/>
   <vault-option name="ENC_FILE_DIR" value="$CSA_HOME/jboss-
as/standalone/configuration/"/>
</vault>
```

Configure Secure Connections for LDAP

If the LDAP server requires a secure connection, follow these steps to import the LDAP server Certificate Authority's root certificate into the Java truststore of HP CSA. If necessary, contact your LDAP administrator to obtain the LDAP server certificate.

If the LDAP server does not require a secure connection, you can omit this task.

1. Open a command prompt and run the `keytool` utility with the following options to create a local trusted certificate entry for the LDAP server.

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -trustcacerts -alias ldap
   -keystore $CSA_JRE_HOME/lib/security/cacerts
   -file </tmp/certfile_name.crt> -storepass changeit
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed and `</tmp/certfile_name.crt>` is the path and name of the Certificate Authority's root certificate for the LDAP server. The file extension may be `.cer` rather than `.crt`. You can also use a different value for `-alias`.

2. At the prompt to import the certificate, type **Yes**.

3. Press **Enter**.

4. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Configure Secure Connections for SMTP

For each organization, if its SMTP server requires a secure connection, follow these steps to import the SMTP server Certificate Authority's root certificate into the Java truststore of HP CSA. If necessary, contact your SMTP server administrator to obtain the SMTP server certificate.

If the SMTP server does not require a secure connection, you can omit this task.

1. Open a command prompt and run the `keytool` utility with the following options to create a local trusted certificate entry for the SMTP server.

```
$CSA_JRE_HOME/bin/keytool -importcert -trustcacerts -alias smtp
-keystore $CSA_JRE_HOME/lib/security/cacerts
-file </tmp/certfile_name.crt> -storepass changeit
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed and `</tmp/certfile_name.crt>` is the path and name of the Certificate Authority's root certificate for the SMTP server. The file extension may be `.cer` rather than `.crt`. You can also use a different value for `-alias`.

2. At the prompt to import the certificate, type **Yes**.

3. Press **Enter**.

4. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Configure Secure Connections for an Oracle Database

If the Oracle database server requires a secure connection, complete the following steps (if the Oracle database does not require a secure connection, you can omit these steps):

1. Complete one of the following tasks:

   - If you do not want to configure HP CSA to check the database DN, do the following:

     i. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

     ii. Add the following to the Oracle datasource:

     ```
     <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=
     (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521)))(CONNECT_DATA =(SERVICE_
     NAME = ORCL)))</connection-url>
     ```

     where `<host>` is the name of the system on which the Oracle database server is installed.

     iii. Save and close the file.

     iv. Import the Oracle database server Certificate Authority's root certificate into the Java truststore of HP CSA.

       A. Copy the Oracle database server Certificate Authority's root certificate to the HP CSA system. If necessary, contact your database administrator to obtain the Oracle database server certificate.

B. On the HP CSA system, open a command prompt and run the keytool utility with the following options to create a local trusted certificate entry for the Oracle database server.

```
$CSA_JRE_HOME/bin/keytool -importcert -trustcacerts
-alias oracledb
-keystore $CSA_JRE_HOME/lib/security/cacerts
-file </tmp/certfile_name.crt> -storepass changeit
```

where $CSA_JRE_HOME is the directory in which the JRE that is used by HP CSA is installed and </tmp/certfile_name.crt> is the path and name of the Certificate Authority's root certificate for the Oracle database server. The file extension may be .cer rather than .crt. You can also use a different value for -alias.

C. At the prompt to import the certificate, type **Yes**.

D. Press **Enter**.

E. Restart HP CSA.

See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

- If you want to configure HP CSA to check the database DN, do the following:

i. Open $CSA_HOME/jboss-as/standalone/configuration/standalone.xml in a text editor.

ii. Add the following to the Oracle datasource:

```
<connection-url>jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST = (ADDRESS
= (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521)))(CONNECT_DATA =
(SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_
DN="CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))</connection-url>
```

where <host> is the name of the system on which the Oracle database server is installed and the values for SSL_SERVER_CERT_DN are for the DN of the Oracle database server.

iii. Add the following to the system-properties element:

```
<property name="oracle.net.ssl_server_dn_match" value="true" />
```

iv. Save and close the file.

v. Import the Oracle database server Certificate Authority's root certificate into the Java truststore of HP CSA.

A. Copy the Oracle database server Certificate Authority's root certificate to the HP CSA system. If necessary, contact your database administrator to obtain the Oracle database server certificate.

B. On the HP CSA system, open a command prompt and run the `keytool` utility with the following options to create a local trusted certificate entry for the Oracle database server.

```
$CSA_JRE_HOME/bin/keytool -importcert -trustcacerts
-alias oracledb
-keystore $CSA_JRE_HOME/lib/security/cacerts
-file </tmp/certfile_name.crt> -storepass changeit
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed and `</tmp/certfile_name.crt>` is the path and name of the Certificate Authority's root certificate for the Oracle database server. The file extension may be `.cer` rather than `.crt`. You can also use a different value for `-alias`.

C. At the prompt to import the certificate, type **Yes**.

D. Press **Enter**.

E. Restart HP CSA.

See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

2. If client authentication is enabled on the Oracle database server, do the following:

   a. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

   b. Add the following to the `system-properties` element:

```
<property name="javax.net.ssl.keyStore" value="<certificate_key_file>" />
<property name="javax.net.ssl.keyStorePassword" value="<certificate_key_
file_password>" />
<property name="javax.net.ssl.keyStoreType" value="<certificate_key_file_
type>" />
```

   where `<certificate_key_file>` is the same keystore file defined by the `certificate-key-file` attribute in the `ssl` element (for example, `$CSA_HOME/jboss-as/standalone/configuration/.keystore`), `<certificate_key_file_password>` is the password to the keystore file (for example, changeit), and `<certificate_key_file_type>` is the keystore type (for example, JKS or PKCS12).

   c. Save and close the file.

d. Use Oracle's wallet manager to import HP CSA's certificate into the Oracle database server's wallet as a trusted certificate.

Configure Secure Connections for Microsoft SQL Server

If Microsoft SQL Server requires a secure connection, complete the following steps (if Microsoft SQL Server does not require a secure connection, you can omit these steps):

1. Open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor.

2. Locate the `connection-url` entry for the Microsoft SQL Server datasource and change `ssl=request` to `ssl=authenticate`.

   For example:

   ```
   <connection-url>
      jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=~~request~~authenticate
   </connection-url>
   ```

3. Save and close the file.

4. Import the Microsoft SQL Server Certificate Authority's root certificate into the Java truststore of HP CSA.

   a. Copy the Microsoft SQL Server Certificate Authority's root certificate to the HP CSA system. If necessary, contact your database administrator to obtain the Microsoft SQL Server certificate.

   b. On the HP CSA system, open a command prompt and run the `keytool` utility with the following options to create a local trusted certificate entry for the Microsoft SQL Server.

      ```
      $CSA_JRE_HOME/bin/keytool -importcert -trustcacerts
      -alias mssqldb -keystore $CSA_JRE_HOME/lib/security/cacerts
      -file </tmp/certfile_name.crt> -storepass changeit
      ```

      where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed and `</tmp/certfile_name.crt>` is the path and name of the Certificate Authority's root certificate for the Microsoft SQL Server. The file extension may be `.cer` rather than `.crt`. You can also use a different value for `-alias`.

   c. At the prompt to import the certificate, type **Yes**.

   d. Press **Enter**.

e. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Configure Secure Connections for HP Operations Orchestration Load Balancer

If the HP Operations Orchestration Load Balancer (HP OO LB) server requires a secure connection, follow these steps to import the HP OO LB server Certificate Authority's root certificate into the Java truststore of HP Cloud Service Automation. If necessary, contact your HP OO LB administrator to obtain the HP OO LB server certificate.

For each system running HP CSA, import the root certificate of HP OO LB's Certificate Authority into HP Cloud Service Automation (you must first export HP OO LB's certificate from HP OO LB's truststore and then import it into HP CSA's truststore).

1. Open HP OO LB in a Web browser (using https).

2. Export the certificate from the Web browser.

   If you are using a Chrome Web browser, do the following:

   a. In the address bar, click the lock icon with the red X over it and select **certificate information**.

   b. In the Certificate dialog, do the following:

      i. Select the **Details** tab.

      ii. Click **Copy to File**.

      iii. In the Certificate Export Wizard, do the following:

         A. Click **Next**.

         B. Select **Base-64 encoded X.509 (.CER)** and click **Next**.

         C. Click **Browse** and select a directory in which to save the certificate.

            - If you are running HP OO LB on the same system as HP CSA, select the `$CSA_JRE_HOME/lib/security` directory (where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed), enter **paslb.cer** as the file name, and click **Save**.

            - If you are running HP OO LB on a system that is not running HP CSA, select a directory in which to store the certificate file, enter **paslb.cer** as the file name, and click **Save**.

         D. Click **Next**.

E. Click **Finish**.

F. Click **OK**.

iv. Click **OK**.

If you are using a Firefox Web browser, do the following:

a. Click **Add Exception**.

b. In the Add Security Exception dialog, click **View**.

c. In the Certificate Viewer, do the following:

i. Select the **Details** tab.

ii. Click **Export**.

iii. Select a directory in which to save the certificate.

- If you are running HP OO LB on the same system as HP CSA, select the *$CSA_JRE_HOME*`/lib/security` directory (where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed), enter **paslb.cer** as the file name, select **X.509 Certificate (PEM)** as the Type, and click **Save**.

- If you are running HP OO LB on a system that is not running HP CSA, select a directory in which to store the certificate file, enter **paslb.cer** as the file name, select **X.509 Certificate (PEM)** as the Type, and click **Save**.

iv. Click **Close**.

d. Click **Cancel**.

If you are using a Windows IE Web browser, do the following:

a. In the address bar, click **Certificate Error** and select **View certificates**.

b. In the Certificate Export Wizard, do the following:

i. Select the **Details** tab.

ii. Click **Copy to File**.

iii. In the Certificate Export Wizard, do the following:

A. Click **Next**.

B. Select **Base-64 encoded X.509 (.CER)** and click **Next**.

C. Click **Browse** and select a directory in which to save the certificate.

- If you are running HP OO LB on the same system as HP CSA, select the *$CSA_JRE_HOME*`/lib/security` directory (where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed), enter **paslb.cer** as the file name, and click **Save**.

- If you are running HP OO LB on a system that is not running HP CSA, select a directory in which to store the certificate file, enter **paslb.cer** as the file name, and click **Save**.

D. Click **Next**.

E. Click **Finish**.

F. Click **OK**.

iv. Click **OK**.

3. If you are running HP OO LB on a system that is not running HP CSA, copy the `paslb.cer` file to the `$CSA_JRE_HOME/lib/security` directory on the system running HP CSA (where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed).

4. On the system running HP CSA, open a command prompt and run the following commands:

```
cd $CSA_JRE_HOME/lib/security
```

```
../../bin/keytool  -importcert -alias paslb -file paslb.cer
-keystore cacerts -storepass changeit
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

5. When prompted to trust the certificate, enter `yes`.

Configure Secure Internal Communication

HP CSA global search services use HTTPS to communicate internally with HP CSA on TCP ports that are not normally used for communication with other systems, the Cloud Service Management Console, or the Marketplace Portal. To prevent access to these ports from an internal or external network, HP recommends configuring network firewall rules for these ports. Consult your network administrator about configuring firewall rules.

TCP Ports Used for Internal Communication

HP CSA Service	TCP Port Used	Communication between Nodes in a Clustered Environment?
HP Search Service	9000	No
Elasticsearch	9201	No
Elasticsearch	9300	Yes

Chapter 4: HP Operations Orchestration

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

> **Note:** If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

In this release, you can install HP Operations Orchestration with HP CSA using the HP CSA installer or you can install HP Operations Orchestration externally. Only one instance of HP Operations Orchestration is required for both topology and sequential designs. If you have upgraded from an earlier version of HP CSA, you may have configured multiple instances of HP Operations Orchestration for sequential designs. If you have upgraded from an earlier version of HP CSA that uses multiple instances of HP Operations Orchestration for sequential designs, you can continue to use the multiple instances of HP Operations Orchestration for sequential designs. If you have upgraded from an earlier version of HP CSA that uses only a single instance of HP Operations Orchestration or are installing HP CSA for the first time, only one configured instance of HP Operations Orchestration is supported.

This chapter describes the following tasks:

- "Configure HP Operations Orchestration for Topology Designs" below
- "Configure HP Operations Orchestration for Sequential Designs" on page 66

> **Note:** If you are configuring HP Operations Orchestration for both topology and sequential designs, complete the configuration for topology designs before the configuration for sequential designs.

Configure HP Operations Orchestration for Topology Designs

The following tasks are to configure HP Operations Orchestration for topology designs. Configure only one instance of HP Operations Orchestration for topology designs.

> **Note:** If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

Complete the following tasks to configure HP Operations Orchestration to integrate with HP CSA:

- Upgrade HP Operations Orchestration
- Configure an internal user
- Configure a secure connection between HP CSA and HP Operations Orchestration
- Configure properties in HP CSA
- Run the HP Cloud Content Capsule Installer
- Update the HP Service Manager base content pack
- Configure HP Single Sign-On
- Obscure passwords in HP Operations Orchestration flows (optional)

> **Note:** In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed and *`%ICONCLUDE_HOME%`* or *`$ICONCLUDE_HOME`* is where you installed HP Operations Orchestration.
>
> Be sure all the latest patches for HP Operations Orchestration have been installed. See the *HP Cloud Service Automation System and Software Support Matrix* for more information, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Upgrade HP Operations Orchestration

Update HP Operations Orchestration version 10.21.0001 by installing hotfix **HF_27629**.

If you are using the embedded HP Operations Orchestration (the HP Operations Orchestration that is installed with HP CSA), the upgrade was performed automatically by the HP CSA installer.

If you are using an external HP Operations Orchestration, you must manually apply this hotfix to HP Operations Orchestration. For your convenience, the hotfix is delivered with the HP CSA installation media. Locate the readme file for this hotfix and follow the instructions on how to upgrade HP Operations Orchestration.

Alternatively, you can download the hotfix from https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=HF_27629.

Configure an Internal User

Internal users can be used to configure HP Operations Orchestration for HP CSA.

This user is used for provisioning topology designs.

1. Log in to HP Operations Orchestration Central.

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

3. Select **Security** > **Internal Users**.

4. Click the **+** (Add) icon.

5. Enter the following information:

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

   The admin user is used with HP Single Sign-On (HP SSO). When HP Operations Orchestration is launched from the Cloud Service Management Console, this user allows access to HP Operations Orchestration without having to log in. If you are using topology designs, the admin user can also be used for provisioning topology designs.

6. Click **Save**.

7. If not enabled, enable authentication by selecting the **Enable Authentication** check box.

8. Select **OK** in the confirmation dialog.

Deploy Content Packs

1. From HP Operations Orchestration Central, click **Content Management**.

2. Click the **Content Packs** tab.

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

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

5. Click the **+** (Add files for deployment) icon.

6. Open a command prompt and open the `$CSA_HOME/Tools/ComponentTool/contentpacks/component-upload-sequence.txt` file.

7. Deploy the Component Tool content packs. From HP Operations Orchestration Central, navigate to the `$CSA_HOME/Tools/ComponentTool/contentpacks/` directory. Add and deploy the content

packs in the order listed in the `component-upload-sequence.txt` file (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

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

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

Configure HP Operations Orchestration Properties in the csa.properties File

If you integrated with HP Operations Orchestration using the installer (during the installation or upgrade process), you do not need to configure these properties (they are already configured). These properties are used to integrate with HP Operations Orchestration. In the subscription event overview section of the **Operations** area in the Cloud Service Management Console, selecting the Process ID opens HP Operations Orchestration to the detailed page of the selected process when these properties are configured.

Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file and configure the following properties:

Property	Description
OOS_URL	The URL used to access HP Operations Orchestration Central. This is the HP Operations Orchestration used for provisioning topology designs. For example, `https://<hostname>:8445`. This property is automatically set during installation. If you are using the embedded HP Operations Orchestration that is included with HP CSA, this property is set using the values entered for the **Fully Qualified Hostname** and **HP OO Port** fields during installation. If you are using a standalone/external HP Operations Orchestration, this property is set using the values entered for the **HP OO Hostname** and **HP OO Port** fields during installation.
OOS_USERNAME	The username used to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO User** field during installation.
OOS_PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO Password** field during installation.

Configure a Secure Connection between HP CSA and HP Operations Orchestration

If you integrated with HP Operations Orchestration using the installer (during the installation or upgrade process), you do not need to configure a secure connection (it has already been configured).

Export HP Operations Orchestration's certificate from HP Operations Orchestration's truststore. If HP Operations Orchestration and HP CSA are not installed on the same system, copy the certificate to the HP CSA system and import the certificate into HP CSA's truststore. TLS must be configured between HP CSA and HP Operations Orchestration.

Do the following:

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

2. Run the following command:

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

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

   where `C:\oo.crt` and `/tmp/oo.crt` are examples of filenames and locations used to store the exported root certificate (you can choose a different filename and location).

3. If HP Operations Orchestration is not running on the same system as HP Cloud Service Automation, copy `oo.crt` from the HP Operations Orchestration system to the system running HP Cloud Service Automation.

4. On the system running HP Cloud Service Automation, open a command prompt.

5. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias tomcat -file /tmp/oo.crt -
   trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

6. When prompted for the keystore password, enter `changeit`.

7. Enter `yes` when prompted to trust the certificate.

Run the HP Cloud Content Capsule Installer

The HP Cloud Content Capsule Installer is used to install and update content for HP CSA and HP Operations Orchestration.

1. Open a command prompt and navigate to the `$CSA_HOME/Tools/CSLContentInstaller` directory.

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/java -jar csl-content-installer.jar
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. From the installer, enter the information to deploy content to HP Operations Orchestration and import service designs into HP CSA.

   For more information about the HP Cloud Content Capsule Installer, refer to the *HP Cloud Service Automation Content Installation Guide*.

Update and Redeploy the HP Service Manager Base Content Pack

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

1. Stop the HP Operations Orchestration services:

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

      For example, `/usr/local/hp/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/hp/csa/OO/ras/bin/ras stop`

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

   ```
   <HPOOinstallation>/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
```

4. Run the following SQL command against the HP 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 HP Operations Orchestration services:

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

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

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

   a. Log in to HP 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**.

Configure HP Single Sign-On between HP CSA and HP Operations Orchestration

If HP Single Sign-On (HP SSO) was enabled during installation of HP CSA, HP SSO can be configured between HP CSA and HP Operations Orchestration. Configuring HP SSO allows you to launch HP Operations Orchestration from the Cloud Service Management Console without having to log in to HP Operations Orchestration.

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

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

Note: In order to use HP SSO between HP CSA and HP Operations Orchestration, the systems on which HP CSA and HP Operations Orchestration are installed must be in the same domain.

Configure and Enable HP Single Sign-On

To configure and enable HP SSO on HP Operations Orchestration, do the following:

1. Log in to HP Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security** > **SSO**.
4. Select the **Enable** checkbox.
5. Enter the **InitString**. The `initString` setting for HP CSA and HP Operations Orchestration must be configured to the same value. In HP CSA, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).
6. Enter the **Domain**. This is the domain name of the network of the servers on which HP CSA and HP Operations Orchestration are installed.
7. Click **Save**.

Configure LDAP Users for Single Sign-On

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

To configure LDAP for HP Operations Orchestration, do the following:

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

Obscure Passwords in HP Operations Orchestration Flows (Optional)

Some HP Operations Orchestration flows included with HP CSA may show passwords in clear text when viewed in HP Operations Orchestration Central. You can obscure these passwords by modifying the flow in HP Operations Orchestration Studio.

> **Note:** You must have HP Operations Orchestration Studio installed. HP Operations Orchestration Studio is supported on Windows platforms only and is not part of the embedded HP Operations Orchestration that is included with HP CSA. See the HP Operations Orchestration documentation, such as the *HP Operations Orchestration System Requirements*, for more information about HP Operations Orchestration Studio.

To obscure passwords in HP Operations Orchestration flows:

1. Open HP Operations Orchestration Studio.
2. Locate the flow to update.
3. Right-click on the flow and select **References > What uses this?**.

   A list of flows that use the flow is displayed (that is, the flow to update is a subflow of the flows displayed in the list).
4. Select a flow from the list of flows.
5. Locate the subflow (the flow to update).
6. Right-click on the subflow and select **Properties**.
7. Located the property to obscure (such as a password), enable it, but do not assign a value to it.
8. Save the flow.
9. Repeat this procedure for every flow from the list of flows.

Configure HP Operations Orchestration for Sequential Designs

The following tasks are to configure HP Operations Orchestration for sequential designs. If you are installing HP CSA for the first time, configure only one instance of HP Operations Orchestration. If you have upgraded from an earlier version of HP CSA that has multiple instances of HP Operations Orchestration configured for sequential designs, you can continue to use multiple instances of HP Operations Orchestration, including HP Operations Orchestration 9.07.

> **Note:** If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

Configure HP Operations Orchestration Version 10.21.0001

Complete the following tasks to configure HP Operations Orchestration to integrate with HP CSA:

- Upgrade HP Operations Orchestration
- Add a JRE to the system path
- Install the HP CSA content pack
- Configure internal users
- Deploy content packs required by HP CSA
- Set up system accounts for the HP CSA content pack
- Set up system properties
- Configure a secure connection between HP Cloud Service Automation and HP Operations Orchestration
- Run the HP Cloud Content Capsule Installer
- Update the HP Service Manager base content pack
- Configure HP Single Sign-On
- Obscure passwords in HP Operations Orchestration flows (optional)

> **Note:** In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed and *`%ICONCLUDE_HOME%`* or *`$ICONCLUDE_HOME`* is where you installed HP

Operations Orchestration.

Be sure all the latest patches for HP Operations Orchestration have been installed. See the *HP Cloud Service Automation System and Software Support Matrix* for more information, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Upgrade HP Operations Orchestration

Update HP Operations Orchestration version 10.21.0001 by installing hotfix **HF_27629**.

If you are using the embedded HP Operations Orchestration (the HP Operations Orchestration that is installed with HP CSA), the upgrade was performed automatically by the HP CSA installer.

If you are using an external HP Operations Orchestration, you must manually apply this hotfix to HP Operations Orchestration. For your convenience, the hotfix is delivered with the HP CSA installation media. Locate the readme file for this hotfix and follow the instructions on how to upgrade HP Operations Orchestration.

Alternatively, you can download the hotfix from https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=HF_27629.

Add a JRE to the System Path

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

Open a shell and enter the following command:

If HP Operations Orchestration and HP CSA are installed on the same system:

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

or

If HP Operations Orchestration and HP CSA are installed on different systems:

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

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

Install the HP CSA Content Pack

- Copy the `$CSA_HOME/CSAKit-4.5/OO Flow Content/10X/oo10-csa-cp-4.50.000-uuids.txt` file to:

  Windows
  `%ICONCLUDE_HOME%\central\cmu\exclusions`

  Linux
  `$ICONCLUDE_HOME/central/cmu/exclusions`

- If HP CSA and HP Operations Orchestration are running on different systems, copy the `$CSA_HOME/CSAKit-4.5/OO Flow Content/10X/oo10-csa-cp-4.50.0000.jar` and `oo10-csa-integrations-cp-4.50.0000.jar` files from the HP Cloud Service Automation system to the HP Operations Orchestration system (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

Configure Internal Users

Internal users can be used to configure HP Operations Orchestration for HP CSA.

1. From the system on which HP CSA is installed (the system on which the content packs are installed), log in to HP Operations Orchestration Central.
2. Click **System Configuration**.
3. Select **Security** > **Internal Users**.
4. Click the **+** (Add) button.
5. Enter the following information:

Field	Recommended Value
User Name	csaoouser
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

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

6. Click **Save**.
7. If not enabled, enable authentication by selecting the **Enable Authentication** check box.
8. Select **OK** in the confirmation dialog.

9. Click the **+** (Add) icon.

10. Enter the following information:

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

    The admin user is used with HP Single Sign-On (HP SSO). When HP Operations Orchestration is launched from the Cloud Service Management Console, this user allows access to HP Operations Orchestration without having to log in. If you are using topology designs, the admin user can also be used for provisioning topology designs.

11. Click **Save**.

12. If not enabled, enable authentication by selecting the **Enable Authentication** check box.

13. Select **OK** in the confirmation dialog.

14. Log out of HP Operations Orchestration Central and log back in as the csaoouser.

Deploy Content Packs Required by HP CSA

The following groups of content packs must be deployed in the order described below:

- Base content packs
- HP CSA sequential design content packs
- HP CSA content packs

1. From HP Operations Orchestration Central, click **Content Management**.

2. Click the **Content Packs** tab.

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

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

5. Deploy the base content packs. Navigate to the `$CSA_HOME/oo/ooContentPack` directory. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

- oo10-base-cp-1.4.4
- oo10-cloud-cp-1.4.0
- oo10-hp-solutions-cp-1.4.0
- oo10-virtualization-cp-1.4.0
- oo10-sa-cp-1.2.0.001
- oo10-sm-cp-1.0.3

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

6. After you have successfully deployed all the base content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.

7. Click the **+** (Add files for deployment) icon.

8. Deploy the HP CSA sequential design content packs. Navigate to the `$CSA_HOME/CSAKit-4.5/OOFlowContent/10X` directory. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

   - oo10-csa-integrations-cp-4.50.0000
   - oo10-csa-cp-4.50.0000

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

9. After you have successfully deployed all the HP CSA sequential design content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.

10. Open a command prompt and extract all the `.jar` files from the `$CSA_HOME/Tools/CSLContentInstaller/csa-ootb-content-04.50.000.zip` file.

11. Click the **+** (Add files for deployment) icon.

12. Deploy the HP CSA content packs. Navigate to the directory in which you extracted all the `.jar` files. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

    > **Note:** You can select more than one content pack to add and deploy at the same time. However, the `*.util.jar` content packs should be deployed first. For example, you can

> deploy two groups of content packs: select all of the `*.util.jar` content packs and deploy them first. Then, select the rest of the content packs and deploy them.

- com.hp.csl.base.util.jar
- com.hp.csl.middleware.util.jar
- com.hp.csl.openstack.util.jar
- com.hp.csl.amazon.ec2.jar
- com.hp.csl.dma.jar
- com.hp.csl.goactive.jar
- com.hp.csl.icsp.jar
- com.hp.csl.matrix.jar
- com.hp.csl.na.jar
- com.hp.csl.oneview.jar
- com.hp.csl.openstack.jar
- com.hp.csl.sa.agentinstallation.jar
- com.hp.csl.sa.softwarepolicies.jar
- com.hp.csl.sitescope.jar
- com.hp.csl.sm.jar
- com.hp.csl.ucmdb.jar
- com.hp.csl.vmware.vcenter.jar
- com.hp.csl.vpv.jar

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

13. When you have finished deploying all the content packs, click **Close** to close the dialog.

Set Up System Accounts for the HP CSA Content Pack

Set up system accounts for the content packs:

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

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

> **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Property Value** (HP Operations Orchestration version 9.07) or **Override Value** (HP Operations Orchestration version 10.21.0001) configured for the CSA_OO_USER System Property setting.

6. Click **Save**.
7. Click the **Add** icon.
8. Enter the following information if it is not already configured:

Field	Recommended Value
System Account Name	CSA_SERVICEMANAGER_CREDENTIALS
User Name	falcon
Password	*<leave_blank>*

9. Click **Save**.

Set Up System Properties for the HP CSA Content Pack

Set up the following system properties for the content packs:

1. Log in to HP Operations Orchestration Central.
2. Click **Content Management**.
3. Select **Configuration Items** > **System Properties**.

4. Click the **Add** icon.

5. Enter the following information if it is not already configured:

Field	Recommended Value
Name	CSA_REST_URI
Override Value	https://<*csa_hostname*>:8444/csa/rest

6. Click **Save**.

Configure a Secure Connection between HP Cloud Service Automation and HP Operations Orchestration

If you integrated with HP Operations Orchestration using the installer (during the installation or upgrade process), you do not need to configure a secure connection (it has already been configured).

Export HP Operations Orchestration's certificate from HP Operations Orchestration's truststore. If HP Operations Orchestration and HP CSA are not installed on the same system, copy the certificate to the HP CSA system and import the certificate into HP CSA's truststore. TLS must be configured between HP CSA and HP Operations Orchestration.

Do the following:

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

2. Run the following command:

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

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

   where `C:\oo.crt` and `/tmp/oo.crt` are examples of filenames and locations used to store the exported root certificate (you can choose a different filename and location).

3. If HP Operations Orchestration is not running on the same system as HP Cloud Service Automation, copy `oo.crt` from the HP Operations Orchestration system to the system running HP Cloud Service Automation.

4. On the system running HP Cloud Service Automation, open a command prompt.

5. Run the following command:

```
$CSA_JRE_HOME/bin/keytool -importcert -alias tomcat -file /tmp/oo.crt -
trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

6. When prompted for the keystore password, enter `changeit`.
7. Enter `yes` when prompted to trust the certificate.

Run the HP Cloud Content Capsule Installer

The HP Cloud Content Capsule Installer is used to install and update content for HP CSA and HP Operations Orchestration.

1. Open a command prompt and navigate to the `$CSA_HOME/Tools/CSLContentInstaller` directory.
2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/java -jar csl-content-installer.jar
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.
3. From the installer, enter the information to deploy content to HP Operations Orchestration and import service designs into HP CSA.

   For more information about the HP Cloud Content Capsule Installer, refer to the *HP Cloud Service Automation Content Installation Guide*.

Update and Redeploy the HP Service Manager Base Content Pack

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

1. Stop the HP Operations Orchestration services:
   a. On the server that hosts HP Operations Orchestration, run the following command: `<HPOOinstallation>/central/bin/central stop`

      For example, `/usr/local/hp/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/hp/csa/OO/ras/bin/ras stop`

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

   ```
   <HPOOinstallation>/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
   ```

4. Run the following SQL command against the HP 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 HP Operations Orchestration services:

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

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

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

   a. Log in to HP 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**.

Configure HP Single Sign-On between HP CSA and HP Operations Orchestration

If HP Single Sign-On (HP SSO) was enabled during installation of HP CSA, HP SSO can be configured between HP CSA and HP Operations Orchestration. Configuring HP SSO allows you to launch HP Operations Orchestration from the Cloud Service Management Console without having to log in to HP Operations Orchestration.

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

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

> **Note:** In order to use HP SSO between HP CSA and HP Operations Orchestration, the systems on which HP CSA and HP Operations Orchestration are installed must be in the same domain.

Configure and Enable HP Single Sign-On

To configure and enable HP SSO on HP Operations Orchestration, do the following:

1. Log in to HP Operations Orchestration Central.

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

3. Select **Security** > **SSO**.

4. Select the **Enable** checkbox.

5. Enter the **InitString**. The `initString` setting for HP CSA and HP Operations Orchestration must be configured to the same value. In HP CSA, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).

6. Enter the **Domain**. This is the domain name of the network of the servers on which HP CSA and

HP Operations Orchestration are installed.

7. Click **Save**.

Configure LDAP Users for Single Sign-On

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

To configure LDAP for HP Operations Orchestration, do the following:

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

Obscure Passwords in HP Operations Orchestration Flows (Optional)

Some HP Operations Orchestration flows included with HP CSA may show passwords in clear text when viewed in HP Operations Orchestration Central. You can obscure these passwords by modifying the flow in HP Operations Orchestration Studio.

> **Note:** You must have HP Operations Orchestration Studio installed. HP Operations Orchestration Studio is supported on Windows platforms only and is not part of the embedded HP Operations Orchestration that is included with HP CSA. See the HP Operations Orchestration documentation, such as the *HP Operations Orchestration System Requirements*, for more information about HP Operations Orchestration Studio.

To obscure passwords in HP Operations Orchestration flows:

1. Open HP Operations Orchestration Studio.
2. Locate the flow to update.
3. Right-click on the flow and select **References > What uses this?**.

A list of flows that use the flow is displayed (that is, the flow to update is a subflow of the flows displayed in the list).

4. Select a flow from the list of flows.

5. Locate the subflow (the flow to update).

6. Right-click on the subflow and select **Properties**.

7. Located the property to obscure (such as a password), enable it, but do not assign a value to it.

8. Save the flow.

9. Repeat this procedure for every flow from the list of flows.

Configure HP Operations Orchestration Version 9.07

Only if you have upgraded from an earlier version of HP CSA that uses HP Operations Orchestration 9.07 for sequential designs, you can continue to use HP Operations Orchestration 9.07. For a new installation of HP CSA, HP Operations Orchestration 9.07 is not supported.

Complete the following tasks to configure HP Operations Orchestration to integrate with HP CSA:

- Add a JRE to the system path
- Install HP CSA flows
- Set remote action services
- Configure system accounts settings
- Configure system properties settings
- Configure general system configuration settings in HP Operations Orchestration Central
- Configure a secure connection between HP CSA and HP Operations Orchestration
- Obscure passwords in HP Operations Orchestration flows (optional)
- Check RAS timeout settings (optional)
- Change HP Operations Orchestration REST API timeout (optional)
- Import HP Operations Orchestration flows

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed and *`%ICONCLUDE_HOME%`* or *`$ICONCLUDE_HOME`* is where you installed HP Operations Orchestration.

Be sure all the latest patches for HP Operations Orchestration have been installed. See the *HP Cloud Service Automation System and Software Support Matrix* for more information, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Add a JRE to the System Path

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

Open a shell and enter the following command:

If HP Operations Orchestration and HP CSA are installed on the same system:

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

or

If HP Operations Orchestration and HP CSA are installed on different systems:

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

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

Install HP CSA Flows

The flows for HP Cloud Service Automation must be installed in the HP Operations Orchestration Flow Library.

To install HP Cloud Service Automation flows:

1. If HP Cloud Service Automation and HP Operations Orchestration are running on different systems, copy the `$CSA_HOME/CSAKit-4.5/OO Flow Content/9X/CSA-4_50-ContentInstaller.jar` file from the HP Cloud Service Automation system to the HP Operations Orchestration system (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. On the system running HP Operations Orchestration, open a command prompt (Windows) or shell (Linux) and change to the directory where the `CSA-4_50-ContentInstaller.jar` is located.

3. Run the following command:

   Windows
   ```
   "%ICONCLUDE_HOME%\jre1.6\bin\java" -jar CSA-4_50-ContentInstaller.jar
   -centralPassword <OOAdminPassword>
   ```

Linux

```
$ICONCLUDE_HOME/jre1.6/bin/java -jar CSA-4_50-ContentInstaller.jar
-centralPassword <OOAdminPassword>
```

Set Remote Action Services

1. Log in to HP Operations Orchestration Studio.
2. Open the **Configuration > Remote Action Services** folder.
3. Double-click **RAS_Operator_Path**.
4. Set the **URL** to:

   ```
   https://<FQDN>:9004/RAS/services/RCAgentService
   ```

   where *<FQDN>* is the fully qualified domain name or IP address of the HP Operations Orchestration host. Do not use localhost in the URL. Using localhost does not work correctly even though it appears to work when you run HP Operations Orchestration Studio on the same machine as the RAS.

   RAS must be run on the same system as HP Operations Orchestration Studio. Running HP Operations Orchestration Studio on another machine produces errors and turns flows red with a cryptic error message about result assignments to result variables that do not exist.

Configure System Accounts Settings

1. Log in to HP Operations Orchestration Studio.
2. Open the **Configuration > System Accounts** folder.
3. Double-click **CSA_REST_CREDENTIALS**.
4. Verify the Credentials are set to the following values:
   - **User Name**: ooInboundUser
   - **Password**: cloud

   where **CSA_REST_CREDENTIALS** are the credentials for HP CSA REST authentication.

   > **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Property Value** configured for the CSA_OO_USER System Property setting.

Configure System Properties Settings

1. Log in to HP Operations Orchestration Studio.

2. Open the **Configuration > System Properties** folder.

3. Double-click **CSA_REST_URI**.

4. Set the **Property Value** to:

   ```
   https://<csa_hostname>:8444/csa/rest
   ```

5. Double-click **CSA_OO_USER**.

6. Verify the **Property Value** is set to:

   ooInboundUser

   > **Note:** The **Property Value** configured for the CSA_OO_USER System Property setting must match the **User Name** configured for the CSA_REST_CREDENTIALS System Account setting.

The other settings can be optionally configured. For information about the settings, refer to the *HP Cloud Service Automation Configuration Guide*.

Configure General System Configuration Settings in HP Operations Orchestration Central

1. Log in to HP Operations Orchestration Central.

2. Open the **Administration > System Configuration > General** tab.

3. Set the **Save history base on flags** property to `true`.

Configure a Secure Connection between HP Cloud Service Automation and HP Operations Orchestration

Export HP Operations Orchestration's certificate from HP Operations Orchestration's truststore. If HP Operations Orchestration and HP CSA are not installed on the same system, copy the certificate to the HP CSA system and import the certificate into HP CSA's truststore. TLS must be configured between HP CSA and HP Operations Orchestration.

Do the following:

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

2. Run the following command:

   Windows

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

   Linux

   ```
   ./jre1.6/bin/keytool -export -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).

3. If HP Operations Orchestration is not running on the same system as HP Cloud Service Automation, copy `oo.crt` from the HP Operations Orchestration system to the system running HP Cloud Service Automation.

4. On the system running HP Cloud Service Automation, open a command prompt.

5. Run the following command:

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

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

6. When prompted for the keystore password, enter `changeit`.

7. Enter `yes` when prompted to trust the certificate.

Obscure Passwords in HP Operations Orchestration Flows (Optional)

Some HP Operations Orchestration flows included with HP CSA may show passwords in clear text when viewed in HP Operations Orchestration Central. You can obscure these passwords by modifying the flow in HP Operations Orchestration Studio.

> **Note:** You must have HP Operations Orchestration Studio installed. HP Operations Orchestration Studio is supported on Windows platforms only and is not part of the embedded HP Operations Orchestration that is included with HP CSA. See the HP Operations Orchestration documentation, such as the *HP Operations Orchestration System Requirements*, for more information about HP Operations Orchestration Studio.

To obscure passwords in HP Operations Orchestration flows:

1. Open HP Operations Orchestration Studio.
2. Locate the flow to update.
3. Right-click on the flow and select **References > What uses this?**.

   A list of flows that use the flow is displayed (that is, the flow to update is a subflow of the flows displayed in the list).
4. Select a flow from the list of flows.
5. Locate the subflow (the flow to update).
6. Right-click on the subflow and select **Properties**.
7. Located the property to obscure (such as a password), enable it, but do not assign a value to it.
8. Save the flow.
9. Repeat this procedure for every flow from the list of flows.

Check RAS Timeout Settings (Optional)

Remote Access Server (RAS) operations are subject to a default timeout limit of 20 minutes on HP Operations Orchestration Central. You can change the time-out setting to support operations that are likely to take more than 20 minutes to complete.

If you expect to run large deployments, change the time-out setting according to **Changing the timeout limit for RAS operations** in the *HP Operations Orchestration Software Administrator's Guide*. You may also refer to *HP Operations Orchestration User's Guide* sections **Adding a RAS override** and **Best practices for runtime environment overrides**. Both documents are available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Change HP Operations Orchestration REST API Timeout (Optional)

The calls HP CSA makes to the HP Operations Orchestration REST APIs are synchronous, and HP Operations Orchestration will time-out the connection after one hour by default. To extend this time-out, do the following:

1. Open the following file in a text editor:

   Windows
   ```
   %ICONCLUDE_HOME%\Central\conf\Central.properties
   ```

   Linux
   ```
   $ICONCLUDE_HOME/Central/conf/Central.properties
   ```

2. Add the following lines:

   ```
   # the maximum flow timeout value in milliseconds, this is equivalent to 2 hrs
    dharma.headless2.continuation.timeout=7200000
   ```

3. Open the following file in a text editor:

   Windows
   `%ICONCLUDE_HOME%\Central\WEB-INF\applicationContext.xml`

   Linux
   `$ICONCLUDE_HOME/Central/WEB-INF/applicationContext.xml`

4. Add the following property to the `dharma.RCDefaults` section:

   ```
   <bean id="dharma.RCDefaults"
   class="com.iconclude.dharma.util.spring.RCDefaultsSpringFactory" lazy-
   init="false" singleton="true">

   ................

   <prop
   key="dharma.headless2.continuation.timeout">${dharma.headless2.continuation.tim
   eout}</prop>
   ```

5. Restart the HP Operations Orchestration Central service.

Import HP Operations Orchestration Flows

HP Operations Orchestration flows can be executed by HP Cloud Service Automation (HP CSA) lifecycle actions or used to submit delegated approvals. Before executing flows through HP CSA, they must be imported into HP CSA by running the process definition tool. The process definition tool creates an HP CSA process definition for every imported HP Operations Orchestration flow. The process definitions are associated with a process engine and that process engine corresponds to the HP Operations Orchestration system containing the imported flows.

To import flows, perform the following general steps, which are described in detail below:

- Install HP Cloud Service Automation flows in the HP Operations Orchestration Flow Library
- Create a database properties file
- Create an HP Operations Orchestration input file that defines the flows to be imported
- Run the process definition tool

Note: HP recommends that you generate sample database properties files and input file by doing the following:

1. Navigate to the `$CSA_HOME/Tools/ProcessDefinitionTool` directory.
2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/java -jar process-defn-tool.jar -g
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Note: In this section, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

Step 1: Install HP Cloud Service Automation flows in the HP Operations Orchestration Flow Library

Install HP Cloud Service Automation flows in the HP Operations Orchestration Flow Library (if you have not already done so when HP CSA was installed).

Step 2: Create a Database Properties File

To create a database properties file, do the following:

1. Navigate to the `$CSA_HOME/Tools/ProcessDefinitionTool` directory.
2. In the working directory, if you generated the sample database properties files as recommended in the note, make a copy of the appropriate sample database properties file, rename it to `db.properties`, and update the content (described below) as needed. Otherwise, create a file named `db.properties` with the following content:

Property Name	Description
db.type	The database used by HP Cloud Service Automation. **Examples** Oracle: `db.type=oracle` MS SQL: `db.type=mssql` PostgreSQL: `db.type=Postgres`

Property Name	Description

db.url	The JDBC URL. When specifying an IPv6 address, it must be enclosed in square brackets (see examples below).
	Examples
	Oracle (TLS not enabled):
	`db.url=jdbc:oracle:thin:@//127.0.0.1:1521/XE`
	Oracle (TLS not enabled, using an IPv6 address):
	`db.url=jdbc:oracle:thin:@//[f000:253c::9c10:b4b4]:1521/XE`
	Oracle (TLS enabled, HP CSA does not check the database DN):
	`db.url=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521)))(CONNECT_DATA =(SERVICE_NAME = ORCL)))`
	where `<host>` is the name of the system on which the Oracle database server is installed.
	Oracle (TLS enabled, HP CSA checks the database DN):
	`db.url=jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN="CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))`
	where `<host>` is the name of the system on which the Oracle database server is installed and the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server.
	MS SQL (TLS not enabled):
	`db.url=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request`
	MS SQL (TLS not enabled, using an IPv6 address):
	`db.url=jdbc:jtds:sqlserver://[::1]:1433/example;ssl=request`
	MS SQL (TLS enabled):
	`db.url=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate`
	PostgreSQL: `db.url=jdbc:postgresql://127.0.0.1:5432/csadb`

Property Name	Description
db.user	The user name of the database user you configured for HP Cloud Service Automation after installing the database.
db.password	The encrypted password for the database user (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. While you may enter a password in clear text, after you run the tool, the clear text password is automatically replaced by an encrypted password. **Example** `db.password=ENC(fc5e38d38a5703285441e7fe7010b0)`
csaTruststore	Required if certificates are imported into a truststore that is not the standard JVM truststore (`cacerts`). The truststore that stores trusted Certificate Authority certificates, in which the root certificate of the database's Certificate Authority has been imported. **Example** (if certificates are imported into a truststore that is not the standard JVM truststore) `truststore="`*`$CSA_JRE_HOME`*`/lib/security/<`*`truststore`*`>"` where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.
csaTruststorePassword	Required if certificates are imported into a truststore that is not the standard JVM truststore (`cacerts`). The encrypted password of the truststore (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. **Example** `truststorePassword=ENC(lfABFLAdgy2kAvSaDq9MSI9s=)`

Example `db.properties` content

Oracle (TLS not enabled)

```
db.type=oracle
db.url=jdbc:oracle:thin:@//127.0.0.1:1521/XE
db.user=csa
db.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

MS SQL (TLS not enabled)

```
db.type=mssql
db.url=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request
db.user=csa
db.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

MS SQL (TLS enabled)

```
db.type=mssql
db.url=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate
db.user=csa
db.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

PostgreSQL

```
db.type=Postgres
db.url=jdbc:postgresql://127.0.0.1:5432/csadb
db.user=csadbuser
db.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

Step 3: Create an HP Operations Orchestration Input File

To create an HP Operations Orchestration input file, do the following:

In the working directory (`$CSA_HOME/Tools/ProcessDefinitionTool`), if you generated the sample HP Operations Orchestration input file, make a copy of the `HPOOInputSample.xml` file, rename it to `HPOOInfoInput.xml`, and update the attributes and values, described below, as needed. The `HPOOInfoInput.xml` file is formatted as follows (attributes and values are described below):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="<CSA_process_engine>"
    uri="https://<OO_server>:8443/PAS/services/WSCentralService"
    username="<OO_user>" password="<encrypted_password>"
    truststore="<location_of_truststore>"
    truststorePassword="<truststore_encrypted_password>"
    [accessPointType="URL" | "EXTERNAL_APPROVAL" |
     "RESOURCE_POOL_SYNC"]
    [update="true" | "false"] [delete="true" | "false"] >
      <folder path="<path_name>" [flow="true" | "false"]
       [recursive="true" | "false"] [regex="<regular_expression>"]
       [update="true" | "false"] />
   </ooengine>
</ooengines>
```

where attributes define the flows that are imported and are described below:

Attributes of ooengine

Attribute	Description
name	Required. The name given to the HP CSA process engine that contains or will contain the imported flows. If the name does not exist, the process engine with the specified name is created in HP CSA. If the name exists, the contents of the existing process engine are updated based on the value of the folder's `update` attribute. **Example** `name="oo-instance-1"`

uri	Required. The URI of the HP Operations Orchestration Central server. In the URI, the <*OO_server*> can be localhost or the fully-qualified domain name if localhost or the fully-qualified domain name is configured as the `cn` in the HP Operations Orchestration server's certificate. The <*oo_server*> can also be the IP address if the `Subject Alt Name` attribute has been configured as the IP address in the HP Operations Orchestration server's certificate.
	The default port is 8443.
	Note: Use only forward slashes (/) as your path separators.
	Examples
	`uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"`
	`uri="https://localhost:8443/PAS/services/WSCentralService"`
	`uri="https://127.0.0.1:8443/PAS/services/WSCentralService"`

username	Required. The name of a user who has access to the HP Operations Orchestration flows to be imported **Example** `username="csaoouser"`
password	Required. The encrypted password of the HP Operations Orchestration user (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. While you may enter a password in clear text, after you run the tool, the clear text password is automatically replaced by an encrypted password. **Example** `password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"`

Attributes of ooengine, continued

Attribute	Description
truststore	Required. The truststore that stores trusted Certificate Authority certificates, in which the root certificate of HP Operations Orchestration's Certificate Authority has been imported. The example shows the location of HP CSA's truststore (in which the root certificate of HP Operations Orchestration's Certificate Authority should have already been imported). **Example** `truststore="`*`$CSA_JRE_HOME`*`/lib/security/cacerts"` where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed. **Note:** Use only forward slashes (/) as your path separators.
truststorePassword	Required. The encrypted password of the truststore (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. **Example** `truststorePassword="ENC(lfABFLXBEAdgy2kAvSaDq9MlPd3/aSI9s=)"`

Attributes of ooengine, continued

Attribute	Description
accessPointType	Optional. By default (if not specified), this value is URL. Defines the flows that are contained in the process engine. Valid values include URL, EXTERNAL_ APPROVAL, or RESOURCE_POOL_SYNC. The accessPointType cannot be changed after a process engine is created. **URL** When set to URL, this process engine contains flows that will be selectable in the Cloud Service Management Console when creating lifecycle actions for a resource offering or service design. Required flow inputs: none **EXTERNAL_APPROVAL** When set to EXTERNAL_APPROVAL, this process engine contains flows that will be selectable when configuring a delegating approval policy for a service catalog in the Cloud Service Management Console. Required flow inputs: • **APPROVAL_CONTEXT_ID** - The ID of the service request for which the approval is being processed. • **APPROVAL_PROCESS_ID** - The ID of the approval process being processed by the external approval system. • **CATALOG_ID** - The ID of the catalog from which the subscription was ordered. • **ORGANIZATION_ID** - The organization ID of the subscriber's organization. • **USER_CONTEXT_ID** - The ID of the subscriber who submitted the service request. **RESOURCE_POOL_SYNC** When set to RESOURCE_POOL_SYNC, this process engine contains flows that will be selectable when configuring a resource synchronization action on a resource pool in the Cloud Service Management Console. Required flow inputs: • **CSA_CONTEXT_ID** - The ID of the resource pool on which resource synchronization is being requested. • **CSA_PROCESS_ID** - The process instance ID used by the flow to notify

Attributes of ooengine, continued

Attribute	Description
	HP CSA of the completion status of the action (success or fail). **Example** `accessPointType="EXTERNAL_APPROVAL"`
update	Optional. By default (if not specified), this value is false. When set to true, the HP CSA process engine's uri, username, or password are updated. That is, this information can be updated for a process engine if, for example, the imported flows have been moved to a different HP Operations Orchestration instance or the username and password of the HP Operations Orchestration instance have been changed. **Example** `update="true"`
delete	Optional. By default (if not specified), this value is false. When set to true, the HP CSA process engine and all associated process definitions are deleted. However, if any associated process definition is used in a resource offering or service design, the process engine (and all associated process definitions) cannot be and are not deleted. Any process engine that contains a process definition that is referenced by a retired service instance cannot be deleted. Even if the resource offerings and service designs in that process definition (referenced by a retired service instance) are deleted, the process engine and its associated process definitions cannot be deleted. **Example** `delete="true"`

Attributes of folder

Attribute	Description
path	Required. The absolute path to a folder containing flows or the absolute path to a single flow on the system running HP Operations Orchestration. **Note:** Use only forward slashes (/) as your path separators. **Example** `path="/Library/ITIL/Change Management/stop_request"` **Note:** The absolute path and name of a flow among one or more HP Operations Orchestration instances must be unique in order to import it into HP Cloud Service Automation. If the flow is not unique, it is not imported. Once you import a flow, you cannot import it into a different HP Cloud Service Automation process engine (using the same absolute path and name). If you want to import flows with the same names from different HP Operations Orchestration instances, the flows on each HP Operations Orchestration instance must be stored in different folders (the absolute path names must be different). If two HP Operations Orchestration instances have the same flows stored in the same folders (same absolute path) and you customize one of the flows on one of the instances, you should rename the customized flow to a unique name in order to import it (or you could rename the unchanged flow). The flow path and name between the customized and uncustomized flow must be unique.
flow	Optional. By default (if not specified), this value is false. When set to true, the name specified in the path attribute is the absolute path and filename of a single HP Operations Orchestration flow to import. Valid values: true, false **Example** `flow="true"`
recursive	Optional. By default (if not specified), this value is false. When set to true, flows are imported from the specified path and its subdirectories. When set to false, only flows located directly in the specified path are imported. Valid values: true, false **Example** `recursive="true"`

Attributes of folder, continued

Attribute	Description
regex	Optional. Specify a regular expression, used to find HP Operations Orchestration flows to import. If the regular expression matches the filename or a string in the filename, the flow is imported. **Example** Find all flows with "lifecycle" in their names: `regex="lifecycle"`
update	Optional. By default (if not specified), this value is false. When set to false, if the specified flow has already been imported, it is not imported again. When set to true, if the specified flow has already been imported but the flow has been updated (on the HP Operations Orchestration system), the updated flow is imported to HP Cloud Service Automation (the process definition on the HP Cloud Service Automation system is updated). When set to true, if a specified flow that has already been imported no longer exists on the HP Operations Orchestration system, it is removed from HP Cloud Service Automation. However, if the flow in HP Cloud Service Automation is linked to an action, it is not removed. When set to true and the `regex` attribute is used, only specified flows are updated. If a specified flow that has already been imported no longer exists on the HP Operations Orchestration system, it is removed from HP Cloud Service Automation. However, if the flow in HP Cloud Service Automation is linked to an action, it is not removed. Valid values: true, false **Example** `update="true"`
delete	Optional. By default (if not specified), this value is false. When set to true, the flows in the specified HP Operations Orchestration folder that are not associated with an HP CSA process definition are deleted. If a flow in the HP Operations Orchestration folder is associated with an HP CSA process definition, that flow is not deleted. Valid values: true, false **Example** `delete="true"`

Examples of folder attributes and `HPOOInfoInput.xml` content are located at the end of the section.

Step 4: Run the Process Definition Tool

To run the process definition tool, log in as csauser, and in the working directory (`$CSA_HOME/Tools/ProcessDefinitionTool`), run the following command:

```
$CSA_JRE_HOME/bin/java -jar process-defn-tool.jar -d db.properties
-i HPOOInfoInput.xml
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

If a secure connection is enabled between HP CSA and the Oracle database, additional command line options must be specified based on your configuration:

```
$CSA_JRE_HOME/bin/java [-Doracle.net.ssl_server_dn_match=true]
[-Djavax.net.ssl.keyStore=<certificate_key_file>
-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>
-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>]
-jar process-defn-tool.jar -d db.properties
-i HPOOInfoInput.xml
```

The `-Doracle.net.ssl_server_dn_match=true` option is specified if a secure connection is enabled for the Oracle database server and HP CSA has been configured to check the database DN.

The `-Djavax.net.ssl.keyStore="<certificate_key_file>"`, `-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>`, and `-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>` options are specified if a secure connection and client authentication are enabled for the Oracle database server where `<certificate_key_file>` is the same keystore file defined by the `certificate-key-file` attribute in the `ssl` element of the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file (for example, `$CSA_HOME/jboss-as/standalone/configuration/.keystore`), `<certificate_key_file_password>` is the password to the keystore file (for example, changeit), and `<certificate_key_file_type>` is the keystore type (for example, JKS or PKCS12).

After the process definition tool is run, the total number of imported flows is displayed (depending on the number of flows imported, this may take some time to complete). If more than one HP Operations Orchestration system is specified in the `HPOOInfoInput.xml` file, flows are imported sequentially by system (that is, the flows from the first HP Operations Orchestration system listed are imported; once these flows have been imported/updated in HP Cloud Service Automation, the flows from the next HP Operations Orchestration system are imported).

Review the log file, `process-defn-tool.log`, for any error messages.

The following options are available in the process definition tool:

Option	Description
-d *<filename>*	Required. The name and location of the database properties file. **Example** `-d db.properties`
-i *<filename>*	Required. The name and location of the HP Operations Orchestration input file. **Example** `-i HPOOInfoInput.xml`
-g	Optional. Generate example files: `MsSqlInputSample.properties`, `OracleInputSample.properties`, `PostgreSqlInputSample.properties`, `ProcessEngineInputSample.xml`, and `HPOOInputSample.xml`. The sample `HPOOInputSample.xml` file can be used to import all the flows whose associated process definitions are referenced in the out-of-the-box resource offerings and service designs provided with HP Cloud Service Automation.
-h	Optional. List the options available in this tool.
-l	Optional. The location of the JDBC driver(s) to be used by this tool. By default, the tool looks for the JDBC driver(s) in the working directory. If you are not running the tool from `$CSA_HOME/Tools/ProcessDefinitionTool`, specify the name and location of the JDBC driver(s) to be used. For a list of supported JDBC driver versions, refer to the *HP Cloud Service Automation System and Software Support Matrix*, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport). Multiple drivers may be listed and should be delimited by a space. The absolute path name or relative path name (from the working directory) should be specified.
-v *<filename>*	Optional. Validate the HP Operations Orchestration input file. **Example** `-v HPOOInfoInput.xml`

After you have imported HP Cloud Service Automation flows into HP CSA, you can import the sample service designs provided with HP CSA (some of these imported flows are used by the sample service designs). For more information about the sample service designs provided with HP CSA, refer to the *HP Cloud Service Automation Service Design Guide*.

Examples of Folder Attributes Used to Import Flows

The following examples show how to set folder attributes to import flows from your HP Operations Orchestration instance.

Import a specific flow

Format

```
<folder path="<directory_name>" flow="true" />
```

Example

Import the flow named `stop_request` from the `Library/ITIL/Change Management` directory

```
<folder path="/Library/ITIL/Change Management/stop_request" flow="true" />
```

Import a specific flow, re-import it if it has been updated, or delete it if it no longer exists

Format

```
<folder path="<directory_name>" flow="true"  update="true" />
```

Example

Import the flow named `stop_request` from the `Library/ITIL/Change Management` directory

```
<folder path="/Library/ITIL/Change Management/stop_request" flow="true"
update="true" />
```

Import all flows in the specified directory

Format

```
<folder path="<directory_name> /">
```

Example

Import all flows in the directory `Library/ITIL/Change Management`

```
<folder path="/Library/ITIL/Change Management" />
```

Import all flows in the specified directory and all subdirectories

Format

```
<folder path="<directory_name> recursive="true" /">
```

Example

Import all flows at and below the directory `Library/ITIL/Change Management`

```
<folder path="/Library/ITIL/Change Management" recursive="true" />
```

Import all flows whose name matches a regular expression and are in the specified directory

Format

```
<folder path="<directory_name>" regex="regular_expression" />
```

Example

Import all flows with "lifecycle" in their names in the directory `Library/ITIL/Change Management`

```
<folder path="/Library/ITIL/Change Management" regex="lifecycle" />
```

Import all flows whose name matches a regular expression and are in the specified directory and all subdirectories

Format

```
<folder path="<directory_name>" regex="regular_expression"
recursive="true" />
```

Example

Import all flows with "lifecycle" in their names at and below the directory `Library/ITIL/Change Management`

```
<folder path="/Library/ITIL/Change Management" regex="lifecycle"
recursive="true" />
```

Examples of `HPOOInfoInput.xml` Content

In the following examples, an HP Operations Orchestration instance contains the following flows:

- Flows invoked by lifecycle actions: start_job, stop_job, cancel_job, start_request, stop_request, and cancel_request located in `/Library/ITIL/Change Management`
- Flows used to submit delegated approvals: job_needs_approval and request_needs_approval located in `/Library/ITIL/Change Management/Delegated Approvals`
- Flows used for resource synchronization: sync_resources located in `/Library/ITIL/Change Management/Resource Pool Sync`

Import the flow named stop_request

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="oo-instance-1"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)" >
      <folder path="/Library/ITIL/Change Management/stop_request"
       flow="true" />
   </ooengine>
</ooengines>
```

Import the flows named stop_request and start_job

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="oo-instance-1"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)">
      <folder path="/Library/ITIL/Change Management/stop_request"
       flow="true" />
      <folder path="/Library/ITIL/Change Management/start_job"
       flow="true" />
   </ooengine>
</ooengines>
```

Import the flows named stop_request and request_needs_approval

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="oo-instance-1"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)">
      <folder path="/Library/ITIL/Change Management/stop_request"
       flow="true" />
   </ooengine>
   <ooengine name="oo-instance-2"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)"
    accessPointType="EXTERNAL_APPROVAL" >
      <folder path="/Library/ITIL/Change Management/
       Delegated Approvals/request_needs_approval" flow="true" />
   </ooengine>
</ooengines>
```

Import all flows (invoked by lifecycle actions) with "st" in their name

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="oo-instance-1"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)">
      <folder path="/Library/ITIL/Change Management" regex="st" />
   </ooengine>
</ooengines>
```

In this example, the following flows are imported: **st**art_job, **st**op_job, **st**art_reque**st**, **st**op_reque**st**, and cancel_reque**st**).

Import all flows

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ooengines>
   <ooengine name="oo-instance-1"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)">
      <folder path="/Library/ITIL/Change Management" />
   </ooengine>
   <ooengine name="oo-instance-2"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)"
    accessPointType="EXTERNAL_APPROVAL" >
      <folder path="/Library/ITIL/Change Management/
       Delegated Approvals" />
   </ooengine>
   <ooengine name="oo-instance-3"
    uri="https://oo_server.xyz.com:8443/PAS/services/WSCentralService"
    username="admin" password="ENC(a3pGFPJQFwwXwtBBdpYktg==)"
    truststore="/usr/local/hp/csa/jre/lib/security/cacerts"
    truststorePassword="ENC(sh582cWFlHCfA1DB6JGgRKukv7HR3Wpd)"
    accessPointType="RESOURCE_POOL_SYNC" >
      <folder path="/Library/ITIL/Change Management/
       Resource Pool Sync" />
   </ooengine>
</ooengines>
```

Chapter 5: The Cloud Service Management Console

This chapter provides information for tasks needed to optionally customize the Cloud Service Management Console.

Tasks include:

- "Customize the Cloud Service Management Console Dashboard" below
- "Customize the Cloud Service Management Console Title" on page 118
- "Rename or Delete the Sample Consumer Organization" on page 119
- "Enable Verification of an Imported Service Design, Service Offering, or Catalog Content Archive" on page 120

Customize the Cloud Service Management Console Dashboard

The Cloud Service Management Console dashboard is made up of predefined tiles that launch predefined pages. You can customize the dashboard by using the predefined custom tile, creating new tiles, modifying existing tiles, adding secondary dashboards, or disabling existing tiles.

Topics in this section include:

- "Using the Predefined Custom Tile" on the next page
- "Enabling the Cloud Analytics Secondary Tiles" on page 103
- "Enabling the Cloud Transformation Secondary Tiles" on page 105
- "Configuring the Cloud Optimizer Tile" on page 106
- "Creating a Dashboard Tile" on page 108
- "Adding a Secondary Dashboard" on page 112
- "Modifying a Dashboard Tile" on page 115
- "Disabling a Dashboard Tile" on page 116

The Cloud Service Management Console dashboard can be customized by a user who has access to the system on which HP CSA is running and permissions to modify and save files in the HP CSA installation directory.

A disabled predefined custom tile definition, disabled sample tile definitions, and a disabled sample secondary dashboard definition are provided in HP CSA as examples of how to create a tile and secondary dashboard. Examples of how to use the sample tile definitions and secondary dashboard definition are provided in this section.

Using the Predefined Custom Tile

By default, HP CSA contains sample predefined tiles that are disabled. One predefined tile, whose `id` attribute is set to custom, is a predefined tile that can be used when you are upgrading from a previous version of HP CSA.

The predefined custom tile allows for an easy migration of customized content from a previous version of HP CSA that contained a customized tile (for information on how to upgrade a Cloud Service Management Console custom tile, refer to the *HP Cloud Service Automation Upgrade Guide*).

If you are not upgrading from an older version of HP CSA, this tile can be used to create a custom tile. Information on how to create a custom tile by modifying the predefined custom tile is included in this section.

To use the predefined custom tile to create a new custom tile, on the system running HP CSA, do the following:

1. Create a folder called `custom-content` in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war` directory (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed). Match the spelling and capitalization of the `custom-content` folder name exactly.

2. Create a Java server page named `index.jsp` in the `custom-content` directory. The `index.jsp` file contains the content that is displayed in an embedded page launched by the custom tile.

3. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` dashboard configuration file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

4. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file:

   a. Locate the tile definition whose `id` and `name` are set to `custom`.

   b. Set the `enabled` attribute to **true**.

   c. Save and exit the file.

5. Log in to the Cloud Service Management Console to view the tile. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser. Click the custom tile to launch the `index.jsp` page.

By default, the name of the tile is "Custom" and the description that appears in the tile is "Custom integration content." To modify this content, refer to "Creating a Dashboard Tile" on page 108 for more information.

Enabling the Cloud Analytics Secondary Tiles

HP IT Business Analytics automatically gathers metrics from HP CSA to build key performance indicators. It provides scorecards and dashboards so that Resource Supply Managers and Service Business Managers have insight into how to measure and optimize the cost, risk, quality and value of IT services and processes.

In HP CSA, the Resource Supply Manager, Service Business Manager, and Administrator roles have access to the Cloud Analytics tile in the dashboard. Clicking on the Cloud Analytics tile displays the next level of tiles (when these secondary tiles are enabled), which are displayed based on user roles:

- Resource Supply Managers and Administrators see the **Resource Analytics** tile which launches a report that measures the cost and usage of resource providers in HP CSA.
- Service Business Managers and Administrators see the **Service Analytics** tile which launches a report that measures the revenue, cost, and profit margin for business services in HP CSA.
- Service Business Managers and Administrators see the **Showback Report** tile which launches a showback report for an organization.
- Resource Supply Managers, Service Business Managers, and Administrators see the **Advanced Reporting** tile which launches a standalone version of HP IT Business Analytics in a separate window and allows for more advanced operations, such as running custom reports and drilling down into additional details about information provided in the report.

Prerequisites

- You must have HP IT Business Analytics installed and properly configured in your HP CSA environment.
- To ensure seamless navigation between the products, make sure that the HP Single Sign-On (HP SSO) for HP IT Business Analytics is configured to enable logging on to HP CSA.
- For HP SSO between HP CSA and HP IT Business Analytics to work successfully, both products have to be installed on machines that are in the same Domain. The value of Domain and Protected Domain parameters specified for HP SSO configuration must be the same.
- You must configure users for both HP CSA and HP IT Business Analytics for single sign-on (each user must have the same name and password). You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure HP CSA and HP IT Business Analytics to use the same LDAP source or, if HP CSA and HP IT Business Analytics use different LDAP sources, configure the same users in both sources. In either case, the HP CSA user must be assigned to the appropriate role to access the tiles that launch HP IT Business Analytics

and the HP IT Business Analytics user must be assigned a role that allows it to perform the expected functions in HP IT Business Analytics.

- If you did not enable HP SSO during the installation of HP CSA, you must configure HP SSO for the Cloud Service Management Console. Refer to "Integrate with HP Single Sign-On" on page 162 for more information about enabling HP SSO for the Cloud Service Management Console.

- When configuring HP SSO for HP IT Business Analytics, the `initString` setting for the Cloud Service Management Console and HP IT Business Analytics must be configured to the same value. If you are also configuring HP SSO between HP IT Business Analytics and the Marketplace Portal, the `initString` setting must be configured to the same value for the Cloud Service Management Console, the Marketplace Portal, and HP IT Business Analytics. For the Cloud Service Management Console, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. Use this setting to configure HP IT Business Analytics (and the Marketplace Portal).

  The `initString` value represents a secret key and should be treated as such in your environment. Change the default value of the `initString` setting for the Cloud Service Management Console.

- Review the *HP IT Business Analytics Administrator Guide* for more information.

To enable HP IT Business Analytics tiles in the Cloud Service Management Console:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file.

3. Search for a tile called `executive_scorecard`. You can search for the second occurrence of the following text: `"id": "executive_scorecard"`.

4. Under the `"tiles"` node, enable the first four tiles by changing `"enabled": false` to `"enabled": true`, and disable the fifth tile by changing `"enabled": true` to `"enabled": false`.

5. In the data section for each of the tiles, change `<<CONFIGURE_HOST_NAME>>` to match the host name of your HP IT Business Analytics installation.

6. Save and exit the file.

7. If you are logged in to the Cloud Service Management Console, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser to view the changes.

   Note: The changes do not require you to restart HP CSA.

Enabling the Cloud Transformation Secondary Tiles

HP Enterprise Maps (HP EM) manages a centralized Business Model that links to HP Cloud Service Automation. To bring the highest cost savings, improved agility, and quality using HP CSA, the right applications and services need to be selected. The HP Enterprise Maps Cloud Assessment process will identify the most suitable applications and services, and register them in HP CSA. Management can continuously evaluate the actual Cloud transformation progress to ensure that the IT infrastructure capabilities and Cloud providers are optimally used to meet the Cloud transformation goals.

Cloud Transformation Process

HP Enterprise Maps consolidates information about the existing application portfolio and sends out surveys to appropriate stakeholders using data from tools such as HP Universal CMDB, HP PPM, HP APM, or spreadsheets. Based on the collected information, HP Enterprise Maps calculates scores showing suitability of the systems from business, technical and financial points of view. The results are visualized using a set of predefined reports.

For selected services and applications, HP Enterprise Maps creates initial service designs in HP CSA using information consolidated in the first phase.

The transformation feature is available in the Cloud Service Management Console, and access is provided to the Administrator, Service Designer, and Service Business Manager roles.

Click the **Cloud Transformation** tile to see the next level of tiles (when these secondary tiles are enabled):

- **Cloud Assessment** tile – starts and manages data collection and surveys.
- **Reports** tile – displays the cloud transformation dashboard.

Prerequisites

- You must have HP Enterprise Maps installed and properly configured in your HP CSA environment.
- To ensure seamless navigation between the products, make sure that the HP Single Sign-On (HP SSO) for HP Enterprise Maps is configured to enable logging on to HP CSA.
- For HP SSO between HP CSA and HP Enterprise Maps to work successfully, both products have to be installed on machines that are in the same Domain. The value of Domain and Protected Domain parameters specified for HP SSO configuration must be the same.
- If you did not enable HP SSO during the installation of HP CSA, you must configure HP SSO for the Cloud Service Management Console. Refer to "Integrate with HP Single Sign-On" on page 162 for more information about enabling HP SSO for the Cloud Service Management Console.
- When configuring HP SSO for HP Enterprise Maps, the `initString` setting for HP CSA and HP Enterprise Maps must be configured to the same value. In HP CSA, `initString` is configured in

the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment.

- You must configure users for both HP CSA and HP Enterprise Maps for single sign-on (each user must have the same name and password). You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure HP CSA and HP Enterprise Maps to use the same LDAP source or, if HP CSA and HP Enterprise Maps use different LDAP sources, configure the same users in both sources. In either case, the HP CSA user must be assigned to the appropriate role to access the tiles that launch HP Enterprise Maps and the HP Enterprise Maps user must be assigned a role that allows it to perform the expected functions in HP Enterprise Maps.
- Review the *HP Enterprise Maps Installation and Configuration Guide* for more information.

To enable Cloud Transformation tiles in the Cloud Service Management Console:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).
2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file.
3. Search for a tile called `enterprise_maps`. You can search for the second occurrence of the following text: `"id": "enterprise_maps"`.
4. Under the `"tiles"` node, enable the first two tiles by changing `"enabled": false` to `"enabled": true`, and disable the third tile by changing `"enabled": true` to `"enabled": false`.
5. In the data section for each of the tiles, change `<<EM_HOST_NAME>>` to match the host name of your HP Enterprise Maps installation.
6. Save and exit the file.
7. If you are logged in to the Cloud Service Management Console, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser to view the changes.

   Note: The changes do not require you to restart HP CSA.

Configuring the Cloud Optimizer Tile

HP Virtualization Performance Viewer (HP vPV) is a web-based analysis and visualization tool that analyzes performance trends of elements in virtualized environments. When HP vPV is integrated with HP CSA, you can monitor the performance and analyze the capacity, usage, and forecast trends of the virtualized infrastructure.

By default, in the Cloud Service Management Console, there is a Cloud Optimizer tile that launches the product web page for HP vPV. You can configure the Cloud Optimizer tile to launch the HP vPV dashboard.

The Cloud Optimizer tile is available in the Cloud Service Management Console, and access is provided to the Administrator, Service Designer, Service Business Manager, Resource Supply Manager, and Service Operations Manager roles.

Prerequisites

- You must have HP vPV installed and properly configured in your HP CSA environment.
- To ensure seamless navigation between the products, make sure that the HP Single Sign-On (HP SSO) for HP vPV is configured to enable logging on to HP CSA.
- For HP SSO between HP CSA and HP vPV to work successfully, both products have to be installed on machines that are in the same Domain. The value of Domain and Protected Domain parameters specified for HP SSO configuration must be the same.
- If you did not enable HP SSO during the installation of HP CSA, you must configure HP SSO for the Cloud Service Management Console. Refer to "Integrate with HP Single Sign-On" on page 162 for more information about enabling HP SSO for the Cloud Service Management Console.
- When configuring HP SSO for HP vPV, the `initString` setting for HP CSA and HP vPV must be configured to the same value. In HP CSA, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment.
- You must configure users for both HP CSA and HP vPV for single sign-on (each user must have the same name and password). You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure HP CSA and HP vPV to use the same LDAP source or, if HP CSA and HP vPV use different LDAP sources, configure the same users in both sources. In either case, the HP CSA user must be assigned to the appropriate role to access the tiles that launch HP vPV and the HP vPV user must be assigned a role that allows it to perform the expected functions in HP vPV.
- Review the HP vPV online help for more information.

To configure the Cloud Optimizer tile in the Cloud Service Management Console:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).
2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file.

3. Search for a tile called `cloud_optimizer`. You can search for the occurrence of the following text: `"id": "cloud_optimizer"`.

4. In the data section, change the URL from the HP vPV product web page to the HP vPV dashboard URL. For example, change "`http://www8.hp.com/us/en/software-solutions/vpv-server-virtualization-management/`" to "`<VPV_FQDN>:8444/PV/?CTX=CSA` where *<VPV_FQDN>* is the fully-qualified domain name of the HP vPV installation.

5. Save and exit the file.

6. If you are logged in to the Cloud Service Management Console, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser to view the changes.

   Note: The changes do not require you to restart HP CSA.

Enabling Other Predefined Dashboard Tiles

HP CSA provides several predefined but disabled dashboard tiles. You can enable these tiles by doing the following:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` dashboard configuration file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file:

   a. Locate the tile definition to enable.

   b. Set the `enabled` attribute to **true**.

   c. Save and exit the file.

3. Log in to the Cloud Service Management Console to view the tile. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

   To modify the tile, refer to "Creating a Dashboard Tile" below for more information.

Creating a Dashboard Tile

The Cloud Service Management Console dashboard is made up of predefined tiles that launch predefined pages. You can customize the dashboard by creating tiles in the dashboard that launch custom pages.

Tiles are defined in a configuration file and the tile definitions determine what is displayed in the Cloud Service Management Console dashboard. The default dashboard configuration file defines a primary dashboard that consists of enabled tiles and disabled tiles, a secondary dashboard (launched from the Designs tile), and a disabled sample secondary dashboard. Information about tile attributes and values defined in the configuration file is included in the steps below. See "Adding a Secondary Dashboard" on page 112 for more information about how to add a secondary dashboard.

To create a Cloud Service Management Console dashboard tile, do the following:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` dashboard configuration file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. Edit the `config.json` dashboard configuration file.

   In the configuration file, the tiles defined for a dashboard are configured sequentially. That is, the first tile definition configured in a dashboard definition is the first tile displayed in the dashboard. The second tile definition is the second tile displayed. For example, in the default dashboard configuration file, the first tile definition configured in the primary dashboard is the Organizations tile. The Organizations tile is the first tile displayed in the Cloud Service Management Console dashboard. The second tile definition is the Resources tile and it is the second tile displayed in the Cloud Service Management Console dashboard.

   Determine where you want the tile to appear in the dashboard and find the location in the configuration file. For example, if you want a tile to appear between the Organizations and Resources tiles in the dashboard, find the location between the Organizations and Resources tile definitions. If you want the tile to appear as the last tile, find the end of the last enabled tile definition.

   a. Copy the sample tile definition, whose `id` attribute is set to blanktile, and place it in the selected location. The following is an example tile definition (multiple tile definitions are separated by a comma):

   ```
   {
      "id": "<tile_id>",
      "name": "<tile_name>",
      "description": "<tile_description>",
      "enabled": <true_or_false>,
      "style": "<tile_style>",
      "target": "<tile_target>",
      "data": "<tile_data>",
      "helptopic": "<tile_helptopic>",
      "roles": ["<role_1>", "<role_2>", ... , "<role_n>"]
   }
   ```

   b. Update the attribute values in the tile definition as described in the table.

Attribute	Description
id	A unique identifier of the tile in this dashboard among all tiles defined for this dashboard.
name	The name of the attribute in the `messages.properties` or `messages_<locale>.properties` file that defines the name of the tile that is displayed on the dashboard (where <*locale*> identifies the language to which the title has been translated, for example, `en` for English or `ja` for Japanese). The file may appear in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom` or `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/messages/dashboard` directory. If the file exists in both directories, the value defined in `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom` takes precedence.
description	The name of the attribute in the `messages.properties` or `messages_<locale>.properties` file that defines the description of the tile that is displayed on the dashboard (where <*locale*> identifies the language to which the title has been translated, for example, `en` for English or `ja` for Japanese). The file may appear in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom` or `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/messages/dashboard` directory. If the file exists in both directories, the value defined in `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom` takes precedence.
enabled	Enable or disable the tile in the dashboard. If set to **true**, the tile is displayed in the dashboard. If set to **false**, the tile is not displayed in the dashboard.
style	The name of the attribute in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/css/base.css` file that defines the color of the tile's header that is displayed on the dashboard. If you are creating an assistance tile (that is, you set `target` to **assistance**), you must set this attribute to a pre-defined style named **assistance**.

Attribute	Description
target	The type of page launched when the tile is selected. Values include: ○ **iframe** - An iframe or page is launched within the same dashboard or page. ○ **page** - A new page is launched outside of the dashboard or page. ○ **dashboard** - A sub-dashboard is launched within the same dashboard or page. ○ **assistance** - If the `data` attribute is defined, a new page is launched outside of the dashboard or page. If the `data` attribute is not defined, no page is launched and the tile simply contains content defined by the `description` attribute. The `style` attribute must be set to **assistance**.
data	What is launched, based on the type of `target`. If **iframe** or **page** is the type of `target` selected, enter a URL or relative path (relative to the location of this file, `$CSA_HOME/jboss-as/standalone/deployments/`) and filename of a Java server page to display. For example, enter **http://www.hp.com** or **/csa/administration/index.jsp**. If **dashboard** is the type of `target` selected, enter the unique dashboard `id` attribute of the dashboard to display. For example, the Designs tile of the main dashboard launches a sub- or secondary dashboard. The `id` of the secondary dashboard is **designs** therefore you would set the value of this attribute to **designs**. If **assistance** is the type of `target` selected and if you enter a value for this attribute, a `Learn More` link is displayed in the assistance tile. Clicking the `Learn More` link launches a page with the content defined by this attribute. Enter a URL or relative path (relative to the location of this file, `$CSA_HOME/jboss-as/standalone/deployments/`) and filename of a Java server page to display. For example, enter **http://www.hp.com** or **/csa/administration/index.jsp**.
helptopic	If the type of `target` selected is **iframe**, this is the name of the help topic that is displayed when the `Assistance` icon on the page is selected. If the type of `target` selected is **page**, or **dashboard**, or **assistance**, this attribute is ignored.

Attribute	Description
roles	The role required by the user in order for the tile to display in the dashboard. One or more roles may be entered. However, only one role must match the user role in order for the user to see the tile. Roles must be enclosed in quotation marks and, if more than one role is entered, separated by a comma (for example, "CSA_ADMIN", "RESOURCE_SUPPLY_MANAGER"). If no roles are specified, the tile can be seen by all users. Values include: ◦ **CONSUMER_SERVICE_ADMINISTRATOR** - The Consumer Service Administrator configures and manages consumer organizations. ◦ **CSA_ADMIN** - The Administrator has access to all functionality in the Cloud Service Management Console. ◦ **RESOURCE_SUPPLY_MANAGER** - The Resource Supply Manager creates and manages cloud resources, such as resource providers and resource pools. ◦ **SERVICE_BUSINESS_MANAGER** - The Service Business Manager creates and manages service offerings and service catalogs. ◦ **SERVICE_DESIGNER** - The Service Designer designs, implements, and maintains service designs (also referred to as blueprints), component palettes, component types, component templates, and resource offerings. ◦ **SERVICE_OPERATIONS_MANAGER** - The Service Operations Manager views and manages subscriptions and service instances. See the "Role Descriptions" help topic in the Cloud Service Management Console for more information about these roles (navigate to **Organizations > Access Control > Role Descriptions** in the online help).

c. Save and exit the file.

3. Log in to the Cloud Service Management Console to view the tile. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

Adding a Secondary Dashboard

Tiles in the Cloud Service Management Console dashboard can be configured to launch a secondary dashboard. For example, in the default configuration of the Cloud Service Management Console dashboard, the Designs tile launches another dashboard from which you can select a designer to use. The Designs tile is configured with the `target` attribute set to **dashboard** and the `data` attribute set to the id of the secondary dashboard (**designs**). A sample secondary dashboard, whose id attribute is set to providerpanel, is provided.

After a tile in the main dashboard is configured to launch a secondary dashboard, a secondary dashboard definition must be added to the dashboard configuration file. For example, in the default configuration of the Cloud Service Management Console dashboard, a secondary dashboard with an id of **designs** is defined. Information about dashboard attributes and values defined in the configuration file is included in the steps below.

To add a secondary dashboard, do the following:

1. Make a backup of the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` dashboard configuration file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. Edit the `config.json` file.

   a. Determine where you want the secondary dashboard tile (the tile that launches the secondary dashboard) to appear in the dashboard and find the location in the configuration file. For example, if you want the secondary dashboard tile to appear between the Organizations and Resources tiles in the dashboard, find the location between the Organizations and Resources tile definitions. If you want the tile to appear as the last tile, find the end of the last enabled tile definition.

      Copy the sample secondary dashboard tile definition, whose id attribute is set to providerpanel and target attribute is set to dashboard, and place it in the selected location.

      Update the content of the secondary dashboard tile (see "Creating a Dashboard Tile" on page 108 for more information about updating the content).

   b. In the configuration file, secondary dashboards are defined after the main dashboard. Locate where the main or any secondary dashboard definition ends, and add a secondary dashboard definition within the global dashboard definition. For example, in the default dashboard configuration file, you could add another secondary dashboard after the predefined **designs** secondary dashboard.

      Copy the sample secondary dashboard definition, whose id attribute is set to providerpanel and type attribute is set to secondary, and place it in the selected location. The following is an example secondary dashboard definition (multiple dashboard definitions are separated by a comma):

```
{
   "id": "<dashboard_id>",
   "name": "<dashboard_name>",
   "style": "<dashboard_style>",
   "type": "<dashboard_type>",
   "helptopic": "<dashboard_helptopic>",
   "roles": ["<role_1>", "<role_2>", ... , "<role_n>"],
   "tiles": [ { ... } ]
}
```

c. Update the attribute values in the dashboard definition as described in the table. See "Creating a Dashboard Tile" on page 108 for more information about tile attributes.

Attribute	Description
id	A unique identifier of the dashboard among all defined dashboards.
name	The name of the attribute in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/messages/dashboard/messages.properties` file that defines the name displayed in the dashboard. If this is the primary dashboard, the name is displayed above the tiles. If this is a secondary dashboard, the name is the label that is displayed next to the left-facing arrow icon or `back` button in the header.
style	The name of the attribute in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/css/base.css` file that defines the color of the secondary dashboard's `back` button. For the primary dashboard, leave this value empty.
type	The type of dashboard. Values include: ○ **primary** - The dashboard that is displayed after launching HP CSA and successfully logging into the Cloud Service Management Console. This dashboard does not contain a `back` button. Only one primary dashboard can be defined. ○ **secondary** - A sub-dashboard that is launched from a dashboard tile and contains a `back` button. Zero, one, or multiple secondary dashboards can be defined.
helptopic	The name of the help topic that is displayed when the `Assistance` icon on the page is selected.

Attribute	Description
roles	The role required by the user in order for the dashboard to display. One or more roles may be entered. However, only one role must match the user role in order for the user to see the tile. Roles must be enclosed in quotation marks and, if more than one role is entered, separated by a comma (for example, "CSA_ADMIN", "RESOURCE_SUPPLY_MANAGER"). If no roles are specified, the tile can be seen by all users. Values include: ◦ **CONSUMER_SERVICE_ADMINISTRATOR** - The Consumer Service Administrator configures and manages consumer organizations. ◦ **CSA_ADMIN** - The Administrator has access to all functionality in the Cloud Service Management Console. ◦ **RESOURCE_SUPPLY_MANAGER** - The Resource Supply Manager creates and manages cloud resources, such as resource providers and resource pools. ◦ **SERVICE_BUSINESS_MANAGER** - The Service Business Manager creates and manages service offerings and service catalogs. ◦ **SERVICE_DESIGNER** - The Service Designer designs, implements, and maintains service designs (also referred to as blueprints), component palettes, component types, component templates, and resource offerings. ◦ **SERVICE_OPERATIONS_MANAGER** - The Service Operations Manager views and manages subscriptions and service instances. See the "Role Descriptions" help topic in the Cloud Service Management Console for more information about these roles (navigate to **Organizations > Access Control > Role Descriptions** in the online help).
tiles	Tile definition. At least one tile must be configured. See "Creating a Dashboard Tile" on page 108 for more information about tile attributes.

d. Save and exit the file.

3. Log in to the Cloud Service Management Console to view the dashboard. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

Modifying a Dashboard Tile

To modify an existing dashboard tile, edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file (where `$CSA_HOME` is the directory in which

HP Cloud Service Automation is installed):

1. Locate the tile definition that you want to modify.
2. Update one or more attributes. For a description of the attributes, refer to "Creating a Dashboard Tile" on page 108.
3. Save and exit the file.

Disabling a Dashboard Tile

To disable a dashboard tile, edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/dashboard/config.json` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed):

1. Locate the tile definition that you want to disable.
2. Set the `enabled` attribute to **false**.
3. Save and exit the file.

Dashboard Configuration File Syntax

The following is an example of a dashboard configuration file configured with only one secondary dashboard that has one generic tile and an assistance tile defined.

```
{
   "dashboards": [
      {
         "id": "<primary_id>",
         "name": "<primary_name>",
         "style": "",
         "type": "primary",
         "helptopic": "<primary_helptopic>",
         "roles": ["CONSUMER_SERVICE_ADMINISTRATOR", "SERVICE_BUSINESS_MANAGER",
"SERVICE_DESIGNER", "CSA_ADMIN", "RESOURCE_SUPPLY_MANAGER", "SERVICE_OPERATIONS_
MANAGER"],
         "tiles": [
            {
               "id": "<tile_id_1>",
               "name": "<tile_name>",
               "description": "<tile_description>",
               "enabled": <true_or_false>,
               "style": "<tile_style>",
               "target": "<tile_target>",
               "data": "<tile_data>",
               "helptopic": "<tile_helptopic>",
               "roles": ["<role_1>", "<role_2>", ... , "<role_n>"]
            },
.
.
.
            {
               "id": "<tile_id_n>",
               "name": "<tile_name>",
               "description": "<tile_description>",
               "enabled": <true_or_false>,
               "style": "<tile_style>",
               "target": "<tile_target>",
               "data": "<tile_data>",
               "helptopic": "<tile_helptopic>",
               "roles": ["<role_1>", "<role_2>", ... , "<role_n>"]
            }
         ]
      }, {
         "id": "<secondary_id>",
         "name": "<secondary_name>",
         "style": "<secondary_style>",
         "type": "secondary",
         "helptopic": "<secondary_helptopic>",
         "roles": ["<role_1>", "<role_2>", ... , "<role_n>"],
         "tiles": [
            {
               "id": "<tile_id>",
               "name": "<tile_name>",
               "description": "<tile_description>",
               "enabled": <true_or_false>,
               "style": "<tile_style>",
               "target": "<tile_target>",
               "data": "<tile_data>",
               "helptopic": "<tile_helptopic>",
               "roles": ["<role_1>", "<role_2>", ... , "<role_n>"]
            }, {
               "id": "<assistance_tile_id>",
               "name": "<assistance_tile_name>",
               "description": "<assistance_tile_description>",
               "enabled": <true_or_false>,
               "style": "assistance",
               "target": "assistance",
               "data": "<optional_Learn_More_link>",
               "helptopic": "<value_is_ignored>",
               "roles": ["<role_1>", "<role_2>", ... , "<role_n>"]
            }
         ]
      }
   ]
}
```

Customize the Cloud Service Management Console Font

The font used by the Cloud Service Management Console can be customized. You can change the font if you are a user who has access to the system on which HP CSA is running. To change the font, on the system running HP CSA, do the following:

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom/custom.css` file in a text editor (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. At the end of the file, add the following:

   ```
   html, body {
   font-family: <font_name>;
   }
   ```

   where <*font_name*> is the font used by the Cloud Service Management Console.

   For example, to change the font to Arial, add the following to the file:

   ```
   html, body {
   font-family: Arial;
   }
   ```

3. Save and exit the file.

4. Log in to the Cloud Service Management Console to view the changes. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

Customize the Cloud Service Management Console Title

The Cloud Service Management Console title appears at the top of the Cloud Service Management Console next to the HP logo. By default, the title is "HP Cloud Service Automation."

You can change the title if you are a user who has access to the system on which HP CSA is running. To change the title, on the system running HP CSA, do the following:

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/custom/messages.properties` file in a text editor (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

2. Add the following attribute and value:

   csa_title=<*title*>

   where <*title*> is the title that displays at the top of the Cloud Service Management Console.

   For example, to change the title to "HP CloudSystem," add the following to the file:

   ```
   csa_title=HP CloudSystem
   ```

   > **Note:** You cannot change the HP logo.

   If you are translating the title, create a file named `messages_<locale>.properties` instead (where <*locale*> identifies the language to which the title has been translated, for example, `en` for English or `ja` for Japanese).

3. Save and exit the file.

4. Log in to the Cloud Service Management Console to view the title. If you are already logged in, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

Rename or Delete the Sample Consumer Organization

The sample consumer organization can be used by the sample `consumer` user to experiment with the Marketplace Portal. Customize the sample consumer organization by renaming it. Delete this sample consumer organization (and disable the sample `consumer` user) if you no longer are using it or if you are moving the application to production.

To rename the sample consumer organization:

1. Log in to the Cloud Service Management Console and do the following:
   a. Click the **Organizations** tab.

   b. Select the **CSA Consumer** organization.

   c. In the navigation frame, select **General Information**.

   d. Update the **Organization Display Name**.

   e. Click **Save**.

   f. Look for and remember the Organization Identifier assigned to this organization. This identifier is used to define the default organization accessed by the Marketplace Portal and is assigned the sample users who access the organization.

2. Define the default organization accessed by the Marketplace Portal (the organization that is accessed by the Marketplace Portal when the Marketplace Portal is launched from a URL that does not specify the organization). Edit the `$CSA_HOME/portal/conf/mpp.json` file and update the `defaultOrganizationName` attribute's value to the Organization Identifier (where the Organization Identifier is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console)).

3. Assign the sample users (consumer and consumerAdmin) who access the organization. Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/seededorgs.properties` file and replace the existing sample Organization Identifier (for example, CSA_CONSUMER) with the one that was assigned in step 1.

   For more information about the sample users defined in the `csa-consumer-users.properties` file, refer to "Change HP CSA Out-of-the-Box User Accounts" on page 137.

To delete the sample consumer organization and disable the sample `consumer` user:

1. Log in to the Cloud Service Management Console and delete the sample consumer organization in the **General Information** page of the **Organizations** area.

   > **Note:** In order to delete an organization, it must not have any active catalogs.

2. Edit the `$CSA_HOME/portal/conf/mpp.json` file. Update the `defaultOrganizationName` attribute's value if it is set to CSA_CONSUMER. Set the value to an existing consumer organization's Organization Identifier where the Organization Identifier is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console). The `defaultOrganizationName` attribute defines the organization that is accessed by the Marketplace Portal when the Marketplace Portal is launched from a URL that does not specify the organization.

3. Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties` file. Update the `Consumer` property to disable this user account. For example, set `Consumer` to the following encrypted value: cloud,SERVICE_CONSUMER,ROLE_REST,disabled

   See "Encrypt a Password" on page 130 for instructions on how to encrypt this value.

Enable Verification of an Imported Service Design, Service Offering, or Catalog Content Archive

Service design, service offering, and catalog content archives provide the ability to preserve these artifacts so they can be used to replicate them on another system or to restore them. HP CSA provides the ability to import archives of service designs, service offerings, catalogs, and their supported artifacts using the Cloud Service Management Console, Content Archive Tool, or REST APIs. By default, all service design, service offering, or catalog content archives are imported directly, without verification, into HP CSA.

Note: Service designs and catalogs can be imported using the Cloud Service Management Console, Content Archive Tool, or REST APIs. Service offerings can be imported using the Content Archive Tool or REST APIs.

For security reasons, you may want to verify the authenticity of a service design, service offering, or catalog content archive before importing it into HP CSA. When verification is enabled, HP CSA does the following:

- Verifies the digital signature of the content archive
- Validates the date of the certificate used to sign the content archive
- Verifies that the content in the content archive has not been modified after it was signed

If the content archive fails one of these validation or verification checks, the content archive will not be imported into HP CSA.

Caution: Verification cannot be enabled for importing a service design, service offering, or catalog content archive using the REST APIs. A service design, service offering, or catalog content archive imported using the REST APIs will always be imported directly. Verification can only be enabled for the Cloud Service Management Console or the Content Archive Tool.

Enabling the verification of imported service design, service offering, and catalog content archives requires that all imported service design, service offering, and catalog content archives be signed. Verification ensures the authenticity of the data within the service design, service offering, or catalog content archive has not been modified after it is signed. The following sections explain how to enable the verification of imported service design, service offering, and catalog content archives and how to sign these content archives so that they may be imported.

Prerequisites

Enabling verification requires that all imported service design, service offering, and catalog content archives are digitally signed using any JAR signing tool. HP CSA does not provide a JAR signing tool. A JAR signing tool is typically provided as part of a JDK, but HP CSA does not include a JDK.

Install a JDK and/or JAR signing tool on the same system that has the content archive that will be signed and the keystore used to sign the content archive. Refer to "Create a Signed Content Archive" on page 123 for more information about creating a keystore and signing the content archive.

Examples Used in this Section

The examples in the following sections use the following information. You may want to customize some of the information to something more suitable for your needs (for example, the name and location of the keystore file or the alias of the certificate in the keystore). If you customize any of the information, be sure to substitute these customizations in all of the examples.

Item	Value(s) Used in Examples
JDK installation	`/usr/bin/javac` (HP CSA does not include a JDK.)
JRE that is used by HP CSA	`<csa_jre>` (The location where the JRE used by HP CSA is installed is referred to as `<csa_jre>`.) This JRE may be the OpenJDK JRE that is installed with HP CSA or a self-installed Oracle JRE (refer to the *HP Cloud Service Automation System and Software Support Matrix* for information about supported versions of the Oracle JRE).
keytool	The keytool is available in both the JRE that is used by HP CSA and the JDK installation. Either keytool may be used. JRE: JRE: `<csa_jre>/bin/keytool` JDK: `/usr/bin/javac/bin/keytool`
Content archive	`/tmp/SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d.zip`
Keystore	`/tmp/.keystore_archive_signing`
Alias used to access the certificate in the keystore	`csa_archive`
Keystore password	`<keystore_password>`
Key password	`<key_password>`

Enable Verification

To enable HP CSA to verify a service design, service offering, or catalog content archive when imported using the Cloud Service Management Console or the Content Archive Tool, set the following property to **true** in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed):

- csa.security.enable

If a property value is updated in the `csa.properties` configuration file, HP CSA must be restarted. Refer "Restart HP CSA" on page 129 for information on how to restart HP CSA.

> **Note:** Verifying service designs and catalogs before they are imported is done using the Cloud Service Management Console or the Content Archive Tool. Verifying service offerings before they are imported is done using the Content Archive Tool.

Create a Signed Content Archive

If verification of a service design, service offering, or catalog content archive is enabled, the content archive must be signed by a JAR signing tool before it can be imported into HP CSA.

If verification of a service design, service offering, or catalog content archive is enabled, HP recommends that you sign the service design, service offering, or catalog content archive immediately after exporting it.

To create a signed content archive, do the following:

- Locate or create a keystore and certificate used to sign the content archive
- Sign the content archive

Locating or Creating a Keystore and Certificate

Before you can sign the content archive, you must have an unexpired certificate that you can use. This certificate must be stored in a keystore that you can access and you must know the alias to access the certificate. The certificate can be signed by a certificate authority or it can be self-signed.

If you do not have a keystore or certificate to use, you can create a keystore and a self-signed certificate to sign the content archive.

Creating a Keystore and Self-Signed Certificate

The example shown in this section creates a keystore named `.keystore_archive_signing`, in which a self-signed certificate can be accessed using the alias `csa_archive`. The self-signed certificate is valid for 365 days and is generated using the RSA key algorithm and a 2048 bit key size.

1. Open a command prompt and change the directory to `<csa_jre>\bin`. For example, if you are using the JRE installed with HP CSA, go to `/usr/local/hp/csa/openjre/bin`.

2. Run the following command:

   ```
   keytool -genkeypair -keystore /tmp/.keystore_archive_signing -alias csa_archive
   -validity 365 -keyalg rsa -keysize 2048
   ```

3. Enter a keystore password (`<keystore_password>`). This password is used to control access to the keystore. You will need this password when signing a content archive.

4. Follow the prompts to enter your name, organization, and location values.

5. Enter the key password (`<key_password>`). This password is used to control access to the alias. You will need this password when signing a content archive.

You have completed creating a keystore and self-signed certificate and can now sign your content archives.

Signing the Content Archive

In order to sign a content archive, the JAR signing tool, content archive to sign, and keystore must be located on the same system.

The example shown in this section signs the content archive `SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d.zip` with the certificate stored in the keystore `.keystore_archive_signing` which is accessed using the password `<keystore_password>`. The certificate is accessed using the alias `csa_archive` and the password `<key_password>`.

1. Open a command prompt and change to the JDK's `bin` directory. For example, go to `/usr/bin/javac/bin`.

2. Run the following command:

   ```
   jarsigner -keystore /tmp/.keystore_archive_signing
   -storepass <keystore_password> -keypass <key_password>
   /tmp/SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d.zip csa_archive
   ```

   Optionally, you may specify `-sigFile` with a value that will be used to name the signature files that are added to the signed content archive. If not specified, it will use the first eight letters of the alias (`csa_arch`) to name the signature files.

3. Optionally, verify the signed content archive by running the following command:

   ```
   jarsigner -verify /tmp/SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d.zip
   ```

The content archive is signed and can be imported into HP CSA.

Re-Sign a Content Archive

If the certificate you used to sign a content archive has expired, you can re-sign the content archive using a new certificate. The example in this section assumes that the JAR signing tool, content archive to re-sign, and keystore are located on the same system.

1. On the system, open a command prompt and create a directory in which to extract the files from the content archive and go to that directory. For example, run the following commands:

   ```
   mkdir /tmp/contentarchive
   cd /tmp/contentarchive
   ```

2. Extract the files from the content archive. For example, run the following command:

   ```
   /usr/bin/javac/bin/jar -xvf /tmp/SERVICE_OFFERING_
   2c9f4ab8b896014ac3520ca7016d.zip
   ```

3. Remove the expired signature files. For example, run the following command:

   ```
   rm -rf META-INF
   ```

4. Create a new content archive.

   ```
   /usr/bin/javac/bin/jar -cvf /tmp/SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d_
   NEW.zip *
   ```

5. Change to the JDK's `bin` directory. For example, go to:

   ```
   /usr/bin/javac/bin
   ```

6. If you have access to the keystore, remove the expired certificate by running the following command:

   ```
   keytool -delete -keystore /tmp/.keystore_archive_signing -alias csa_archive
   -storepass <keystore_password>
   ```

7. If you are using a certificate generated for you, get the keystore, keystore password, and alias to access the certificate. If you are using a self-signed certificate, follow the instructions in "Locating or Creating a Keystore and Certificate" on page 123 to generate a new self-signed certificate.

8. Re-sign the content archive. Follow the instructions in "Signing the Content Archive" on the previous page to re-sign the content archive (use the new content archive name, `SERVICE_OFFERING_2c9f4ab8b896014ac3520ca7016d_NEW.zip`).

Chapter 6: Common HP CSA Tasks

This chapter provides information on how to perform common HP CSA tasks.

Tasks include:

- "Launch the Cloud Service Management Console" below
- "Launch the Marketplace Portal" below
- "Start HP CSA" on page 129
- "Stop HP CSA" on page 129
- "Restart HP CSA" on page 129
- "Encrypt a Password" on page 130
- "Clear the Web Browser Cache" on page 130
- "Uninstall HP CSA" on page 131

Launch the Cloud Service Management Console

Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where `<csahostname>` is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

Launch the Marketplace Portal

Launch the default Marketplace Portal

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

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

where <*csahostname*> is the fully-qualified domain name of the system on which the Marketplace Portal instance resides and that was used when HP CSA was installed.

For example: `https://csa_system.abc.com:8444/mpp`

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

Launch an organization-specific Marketplace Portal

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

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

where:

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

Example:

`https://csa_system.xyz.com:8089/org/ORGANIZATIONA`

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

Launch the default remote instance of a Marketplace Portal

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

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

where:

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

Examples:

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

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

Launch an organization-specific remote instance of a Marketplace Portal

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

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

where:

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

Example:

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

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

Instead, start a new browser session to launch another organization's Marketplace Portal.

Start HP CSA

To start HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central start`.

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

Restart HP CSA

To restart HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type
`<embeddedHPOOinstallation>/central/bin/central stop`
`<embeddedHPOOinstallation>/central/bin/central start`.

For example, type

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

Stop HP CSA

To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

Encrypt a Password

To encrypt a password (for use with HP CSA configuration only; see "Encrypt a Marketplace Portal Password" on page 136 for information on how to encrypt a Marketplace Portal password):

1. Open a command prompt and change to the `$CSA_HOME/Tools/PasswordUtil` directory. For example:

   ```
   /usr/local/hp/csa/Tools/PasswordUtil
   ```

2. Run the following command:

   ```
   $CSA_JRE_HOME/bin/java -jar passwordUtil-standalone.jar encrypt <myPassword>
   ```

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 after upgrading HP CSA. 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**.

Uninstall HP CSA

Uninstalling HP CSA removes all the contents of `$CSA_HOME` (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

If you installed an embedded HP Operations Orchestration instance with HP CSA (you installed HP Operations Orchestration with HP CSA using the HP CSA installer), the embedded HP Operations Orchestration instance is removed. If you are using HP CSA with an external HP Operations Orchestration instance (you installed HP Operations Orchestration separately from HP CSA), the external HP Operations Orchestration instance is not removed.

Note: The HP CSA database is NOT updated or uninstalled.

To uninstall HP CSA:

1. Log in as the user who installed HP CSA (for example, `csauser`).

2. Stop all HP CSA services.

   To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type *`<embeddedHPOOinstallation>`*`/central/bin/central stop`.

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

3. Verify that the services were stopped. For example, if HP CSA was installed in `/usr/local/hp/csa`, enter the following:

   ```
   ps -ef | grep /usr/local/hp/csa
   ps -ef | grep mpp
   ps -ef | grep central
   ```

   If there are HP CSA, Marketplace Portal, or HP Operations Orchestration services running, repeat step 2 or kill the HP CSA, Marketplace Portal, and HP Operations Orchestration services.

4. Go to the `$CSA_HOME/_CSA_4_50_0_installation` directory. Enter the following:

   ```
   cd $CSA_HOME/_CSA_4_50_0_installation
   ```

5. Uninstall HP CSA. Enter the following:

   ```
   ./Change\ HP\ Cloud\ Service\ Automation\ Installation
   ```

6. Confirm that you want to uninstall HP CSA.

7. When uninstallation completes, log in as root and do the following:

   a. If all the contents in `$CSA_HOME` are not deleted, you must manually delete them and the `$CSA_HOME` directory.

   b. Delete the HP CSA and Marketplace Portal service scripts. Enter the following:

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

   c. If they exist, delete all HP CSA entries from the following file:

      ```
      /home/csauser/.com.zerog.registry.xml
      ```

   d. Optionally, remove the `csauser` user and `csagrp` group.

Chapter 7: The Marketplace Portal

This chapter provides information on how to enable global search and encrypt a password used by the Marketplace Portal.

For information about configurable attributes in the `mpp.json` file, refer to "Marketplace Portal Attributes" on page 255.

Refer to the *HP Cloud Service Management Console Help* for information about configuring the Marketplace Portal.

Enable Global Search

Global search allows you to find a certain service offering, service instance, or subscription by a meaningful keyword. For service offerings, global search finds the keyword in the name, description, option sets, options, and properties. For service instances and subscriptions, global search finds the keyword in the name, description, and instance properties (name and value).

> **Note:** The Search Results view displays the keyword found only in service offerings, service instances, and subscriptions within your organization. In the Search Results view, click on an object for more detailed information about a service offering or subscription.

By default, global search is disabled. Do the following to enable global search:

1. Configure the global search property:

   a. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor.

   b. Set the `csa.provider.es.exists` property to **yes** (for example, `csa.provider.es.exists=yes`).

   c. Save and exit the file.

2. Enable the global search icon in the top header of the Marketplace Portal:

   a. Open the `$CSA_HOME/portal/conf/dashboard.json` file in a text editor.

   b. Set the `header: search: enable` attribute to **true** (for example,

   ```
   "header": {
      .
      .
      .
     "search": {
       "enable": true
   ```

   c. Save and exit the file.

3. Copy the `$CSA_HOME/scripts/searchguard_node_key.key` file to the `$CSA_HOME/elasticsearch-1.5.2/` directory.

4. Restart HP CSA and Marketplace Portal services. See "Restart HP CSA" on page 129 for more information.

Configure the Showback Report Tile

The Showback Report tile in the Marketplace Portal is a link to HP IT Business Analytics, which automatically gathers metrics from HP CSA to build key performance indicators. HP IT Business Analytics provides scorecards and dashboards so that a Consumer Organization Administrator has insight into how to measure and optimize the cost, risk, quality, and value of IT services and processes.

In the Marketplace Portal, the Consumer Organization Administrator role has access to the Showback Report tile. By default, the Showback Report tile is enabled in the Marketplace Portal. However, you must configure the hostname of the system on which HP IT Business Analytics is installed in order to link to HP IT Business Analytics from the Marketplace Portal. Additionally, to ensure seamless navigation between the Marketplace Portal and HP IT Business Analytics, configure HP Single Sign-On (HP SSO) between the Marketplace Portal and HP IT Business Analytics.

Configure the Link to HP IT Business Analytics

1. Navigate to the `$CSA_HOME/portal/conf/` directory.

2. Make a backup copy of the `dashboard.json` file.

3. Open the `dashboard.json` file in a text editor.

4. Locate the following section:

```
"label": "common.items.SCORECARD",
"icon": {
   "className": "icon-status"
},
"link": {
   "url": "https://<CONFIGURE_HOST_NAME>/
fndwar/loadEmbeddedPage.jsp?com.hp.bsm.uim.pageUID=ef63ab7f-b86b-43c8-b8d8-
bb81869b73dc",
   "target": "_blank"
}
```

5. Replace `<CONFIGURE_HOST_NAME>` with the host name of your HP IT Business Analytics installation.

6. Save and exit the file.

7. If you are logged in to the Marketplace Portal, clear the browser cache (see "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache) and refresh the browser.

   Note: The changes to the `dashboard.json` file do not require you to restart HP CSA.

Configure HP SSO

To ensure seamless navigation between the Marketplace Portal and HP IT Business Analytics, HP SSO must be configured for HP CSA and HP IT Business Analytics. Note the following:

- Verify that HP SSO for HP IT Business Analytics is configured to enable logging on to the Marketplace Portal. Refer to the *HP IT Business Analytics Administrator Guide* for more information about configuring HP SSO for HP IT Business Analytics.

- For HP SSO between HP CSA and HP IT Business Analytics to work successfully, both products have to be installed on machines that are in the same Domain. The value of Domain and Protected Domain parameters specified for HP SSO configuration must be the same.

- You must configure users for both HP CSA and HP IT Business Analytics for single sign-on (each user must have the same name and password). You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure HP CSA and HP IT Business Analytics to use the same LDAP source or, if HP CSA and HP IT Business Analytics use different LDAP sources, configure the same users in both sources. In either case, the HP CSA user must be assigned to the appropriate role to access the tiles that launch HP IT Business Analytics and the HP IT Business Analytics user must be assigned a role that allows it to perform the expected functions in HP IT Business Analytics.

- You must enable HP SSO for the Marketplace Portal. Refer to Configure the Marketplace Portal for more information about enabling HP SSO for the Marketplace Portal.

- When configuring HP SSO, the `initString` setting for the Marketplace Portal and HP IT Business Analytics must be configured to the same value. If you are also configuring HP SSO between HP IT Business Analytics and the Cloud Service Management Console, the `initString` setting must be configured to the same value for the Cloud Service Management Console, the Marketplace Portal, and HP IT Business Analytics. For the Cloud Service Management Console, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. Use this setting to configure the Marketplace Portal and HP IT Business Analytics.

  The `initString` value represents a secret key and should be treated as such in your environment.

Encrypt a Marketplace Portal Password

To encrypt a password used by the Marketplace Portal:

1. Open a command prompt and change to the `$CSA_HOME/portal/bin` directory. For example:

   ```
   /usr/local/hp/csa/portal/bin
   ```

2. Run the following command:

   ```
   passwordUtil --keyfilePath <keyfile> --password <myPassword>
   ```

   where <keyfile> is the path to (absolute or relative to the bin directory) and name of the file that contains the Marketplace Portal's encrypted symmetric key (if the file does not exist, it will create the file) and <myPassword> is the password to be encrypted.

Chapter 8: User Administration

This chapter provides information for additional administration and configuration tasks.

Tasks include:

- "Change HP CSA Out-of-the-Box User Accounts" below (optional)

Change HP CSA Out-of-the-Box User Accounts

HP CSA ships with built-in user accounts. The user accounts are used to authenticate REST API calls and for initial setup and experimentation with the product. For security reasons, you may want to disable or change the passwords associated with these accounts (do not change the usernames).

> **Note:** Do not create users in your LDAP directory that match the out-of-the-box users provided by HP Cloud Service Automation (the out-of-the-box users are `admin`, `cdaInboundUser`, `csaCatalogAggregationTransportUser`, `csaReportingUser`, `csaTransportUser`, `idmTransportUser`, and `ooInboundUser`). Creating the same users in LDAP may allow the out-of-the-box users unintended access to the Cloud Service Management Console or give the LDAP users unintended privileges.

Cloud Service Management Console User Accounts

The following users ship out-of-the-box and are used with the Cloud Service Management Console:

admin User: Cloud Service Management Console

Username	admin
Default Password	cloud
Default Role	ROLE_REST
Usage	This account is used to initially log in to the Cloud Service Management Console to configure the provider organization.

admin User: Cloud Service Management Console, continued

To Disable	Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the `admin` property to disable this user account. For example, set `admin` to the following value (this value should be encrypted): `cloud,ROLE_REST,disabled` **Note:** This property not only determines if the account is enabled, it also contains the password and the roles that control access to HP CSA. By default, the unencrypted value of this property is: `cloud,ROLE_REST,enabled` See "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value.
To Change Password	If you change the password to this account, you must update the value of the password in the `csa-provider-users.properties` file and the `securityAdminPassword` property in the `csa.properties` file (you must use the same password). You must also update and use the same password for every REST API call that uses the password. **Updating the admin property in csa-provider-users.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password portion of the `admin` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,enabled` **Updating the securityAdminPassword property in csa.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityAdminPassword` property. Use the same encrypted password that you entered for the `admin` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

consumerAdmin User: Marketplace Portal

Username	consumerAdmin
Default Password	cloud
Default Role	CONSUMER_ORGANIZATION_ADMINISTRATOR
Usage	This account is used to initially log in to the Cloud Service Management Console to configure and manage the sample CSA Consumer organization.
To Disable	Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties` file. Update the `consumerAdmin` property to disable this user account. For example, set `consumerAdmin` to the following value (this value should be encrypted): `cloud,CONSUMER_ORGANIZATION_ADMINISTRATOR,disabled` **Note:** This property not only determines if the account is enabled, it also contains the password and the roles that control access to HP CSA. By default, the unencrypted value of this property is: `cloud,CONSUMER_ORGANIZATION_ADMINISTRATOR,enabled` See "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value.
To Change Password	Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties` file. Update the password portion of the `consumerAdmin` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `cloud,CONSUMER_ORGANIZATION_ADMINISTRATOR,enabled`

csaCatalogAggregationTransportUser User: Cloud Service Management Console

Username	csaCatalogAggregationTransportUser
Default Password	cloud
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account.
To Change Password	If you change the password to this account, you must update the value of the `securityCatalogAggregationTransportUserPassword` property in `csa.properties`. You must also update the password using the catalog aggregation registration REST APIs. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityCatalogAggregationTransportUserPassword` property. Determine a suitable new password (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

csaReportingUser User: Cloud Service Management Console

Username	csaReportingUser
Default Password	cloud
Default Roles	ROLE_REST, ROLE_DYNAMIC
Usage	This account is used when a subscription is ordered or modified and a field for the subscription includes a dynamically generated list. The dynamically generated list is a subscriber option property configured to use a dynamic query. The dynamic query uses this account to access HP Cloud Service Automation to determine the values that will appear in the list. This account has read-only access to HP Cloud Service Automation.
To Disable	Do not disable this account.

csaReportingUser User: Cloud Service Management Console, continued

To Change Password	If you change the password to this account, you must update the value of the password in the `csa-provider-users.properties` file and the `securityCsaReportingUserPassword` property in the `csa.properties` file (you must use the same password). You must also update and use the same password for every REST API call that uses the password. **Updating the csaReportingUser property in csa-provider-users.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password portion of the `csaReportingUser` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,ROLE_DYNAMIC,enabled` **Updating the securityCsaReportingUserPassword property in csa.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityCsaReportingUserPassword` property. Use the same encrypted password that you entered for the `csaReportingUser` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

csaTransportUser User: Cloud Service Management Console

Username	csaTransportUser
Default Password	csaTransportUser
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account.

csaTransportUser User: Cloud Service Management Console, continued

To Change Password	If you change the password to this account, you must update the value of the `securityTransportPassword` property in the `csa.properties` file and the `idm.csa.password` property in the `applicationContext.properties` file (you must use the same password). You must also update and use the same password for every REST API call that uses the password. **Updating the securityTransportPassword property in csa.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityTransportPassword` property. Determine a suitable new password (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Updating the idm.csa.password property in applicationContext.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file and update the value of the `idm.csa.password` property. Use the same encrypted password that you entered for the `securityTransportPassword` property in the `csa.properties` file. After modifying and saving the changes to the files, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

idmTransportUser User: Cloud Service Management Console

Username	idmTransportUser
Default Password	idmTransportUser
Default Roles	ROLE_ADMIN, PERM_IMPERSONATE
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account.

idmTransportUser User: Cloud Service Management Console, continued

To Change Password	If you change the password to this account, you must update the value of the securityIdmTransportUserPassword property in the csa.properties file, the idmTransportUser property in the integrationusers.properties file, and the password attribute in the idmProvider section of the mpp.json file (you must use the same password) and you must clear the JBoss server and web browser caches. You must also update and use the same password for every REST API call that uses the password. **Updating the securityIdmTransportUserPassword property in csa.properties** Edit the $CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties file (where $CSA_HOME is the directory in which HP Cloud Service Automation is installed) and update the value of the securityIdmTransportUserPassword property. Determine a suitable new password (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Updating the idmTransportUser property in integrationusers.properties** **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: idmTransportUser,ROLE_ADMIN,PERM_IMPERSONATE,enabled Edit the $CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/integrationusers.properties file and update the value of the idmTransportUser property. Use the same password that you used for the securityIdmTransportUserPassword property in the csa.properties file and encrypt the entire value of the idmTransportUser property, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by ENC without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value.

idmTransportUser User: Cloud Service Management Console, continued

	Updating the password attribute in mpp.json
	Edit the `$CSA_HOME/portal/conf/mpp.json` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `password` attribute in the idmProvider section and the `keyfile` attribute. Use the same password that you used for the `securityIdmTransportUserPassword` property in the `csa.properties` file and encrypt this password using the password utility that is provided by the Marketplace Portal:
	1. Open a command prompt and navigate to the `$CSA_HOME/portal/bin` directory. For example:
	`/usr/local/hp/csa/portal/bin`
	2. Run the following command:
	`../../node.js/node passwordUtil`
	When prompted, enter the name and location of the keyfile to generate (for example, `../conf/keyfile`) and the password to encrypt.
	3. An encrypted password is displayed. Copy the encrypted password to the `password` attribute value in the idmProvider section. An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. For example `ENC(3oKr7eAo25bEn3Zn2t9wIA==)`
	4. Copy the keyfile name and location to the `keyfile` attribute.
	Clearing the JBoss server and web browser caches
	After modifying and saving the changes to the files, clear the JBoss server and web browser caches.
	To clear the JBoss server cache, remove the contents from the `$CSA_HOME/jboss-as/standalone/tmp` directory.
	See "Clear the Web Browser Cache" on page 130 for information on how to clear the web browser cache.
	Restarting HP CSA
	After making these changes, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA and the Marketplace Portal.

ooInboundUser User: Cloud Service Management Console

Username	ooInboundUser
Default Password	cloud
Default Role	ROLE_REST
Usage	This account is used by HP Operations Orchestration to authenticate REST API calls with HP Cloud Service Automation.
To Disable	Do not disable this account.

ooInboundUser User: Cloud Service Management Console, continued

To Change Password	If you change the password to this account, you must update the value of the password in the `csa-provider-users.properties` file and the `securityOoInboundUserPassword` property in the `csa.properties` file (you must use the same password). You must also update and use the same password for every REST API call that uses the password. **Updating the ooInboundUser property in csa-provider-users.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password portion of the `ooInboundUser` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `cloud,ROLE_REST,enabled` You must also update and use the same password for the CSA_REST_CREDENTIALS system account in HP Operations Orchestration (located in the Configuration folder of the Public Repository). **Updating the securityOoInboundUserPassword property in csa.properties** If you change the password to this account, you must update the value of the `securityOoInboundUserPassword` property in `csa.properties`. You must also update and use the same password for the CSA_REST_CREDENTIALS system account in HP Operations Orchestration (located in the Configuration folder of the Public Repository). Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityOoInboundUserPassword` property. Use the same encrypted password that you entered for the `ooInboundUser` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

cdaInboundUser User: Cloud Service Management Console

Username	cdaInboundUser
Default Password	CDA2CSAIntegration!
Default Role	ROLE_REST
Usage	This account is used by HP Continuous Delivery Automation (HP CDA) to authenticate REST API calls with HP Cloud Service Automation.
To Disable	Do not disable this account.
To Change Password	If you change the password to this account, you must update the value of the password in the `csa-provider-users.properties` file and the `securityCdaInboundUserPassword` property in the `csa.properties` file (you must use the same password). You must also update and use the same password for every REST API call that uses the password. **Updating the cdaInboundUser property in csa-provider-users.properties** Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file. Update the password portion of the `cdaInboundUser` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `CDA2CSAIntegration!,ROLE_REST,enabled` **Updating the securityCdaInboundUserPassword property in csa.properties** If you change the password to this account, you must update the value of the `securityCdaInboundUserPassword` property in `csa.properties`. You must also update and use the same password in HP CDA. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed) and update the value of the `securityCdaInboundUserPassword` property. Use the same encrypted password that you entered for the `cdaInboundUser` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Marketplace Portal User Account

The following is a sample user that ships with HP CSA and is used to access the Marketplace Portal:

consumer User: Marketplace Portal

Username	consumer
Default Password	cloud
Default Roles	SERVICE_CONSUMER, ROLE_REST
Usage	This account is used to initially log in to and experiment with the Marketplace Portal (LDAP does not have to be configured). This user belongs to the "CSA consumer internal group" and is a member of the "CSA Consumer" organization (both the group and organization are provided as samples).
To Disable	Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties` file. Update the `consumer` property to disable this user account. For example, set `consumer` to the following value (this value should be encrypted): `cloud,SERVICE_CONSUMER,ROLE_REST,disabled` **Note:** This property not only determines if the account is enabled, it also contains the password and the roles that control access to HP CSA. By default, the unencrypted value of this property is: `cloud,SERVICE_CONSUMER,ROLE_REST,enabled` See "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value.

consumer User: Marketplace Portal, continued

To Change Password	Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-consumer-users.properties` file. Update the password portion of the `consumer` value and encrypt the entire value, including the roles and account status (see "Encrypt a Password" on page 130 for instructions on how to encrypt this value). The encrypted value is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Ensure there is no blank space at the end of the value. **Note:** This property not only contains the password, but also the roles that control access to HP CSA and if the account is enabled. By default, the unencrypted value of this property is: `cloud,SERVICE_CONSUMER,ROLE_REST,enabled`

Chapter 9: Configure IPv6

This chapter explains how to configure HP CSA to support IPv6 (both dual-stack and IPv6-only). Make sure that IPv6 has been implemented on the system on which HP CSA is running (including configuring the network and DNS) and that your Web browser, such as Firefox or Chrome, have been enabled for IPv6 support.

To configure HP CSA to support IPv6, open `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` in a text editor and make the following changes:

1. Locate the following line:

   ```
   <wsdl-host>${jboss.bind.address:127.0.0.1}</wsdl-host>
   ```

   and replace `127.0.0.1` with `[::1]`. For example,

   ```
   <wsdl-host>${jboss.bind.address:[::1]}</wsdl-host>
   ```

2. Locate the following lines:

   ```
   <interface name="management">
      <inet-address value="127.0.0.1" />
   </interface>
   ```

   and replace `127.0.0.1` with `[::1]`. For example,

   ```
   <interface name="management">
      <inet-address value="[::1]" />
   </interface>
   ```

3. Locate the following lines:

   ```
   <interface name="public">
      <inet-address value="0.0.0.0" />
   </interface>
   ```

   and replace `0.0.0.0` with `[::]`. For example,

   ```
   <interface name="public">
      <inet-address value="[::]" />
   </interface>
   ```

4. Locate the following lines:

   ```
   <interface name="unsecure">
      <inet-address value="${jboss.bind.address.unsecure:127.0.0.1}" />
   </interface>
   ```

and replace `127.0.0.1` with `[::1]`. For example,

```
<interface name="public">
   <inet-address value="${jboss.bind.address.unsecure:[::1]}" />
</interface>
```

To configure the Marketplace Portal to support IPv6, do the following:

- Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.
- In the general attribute section (for example, after the `uid` attribute), add a `bindIP` attribute and set the value to the IPv6 address to which the Marketplace Portal binds.
- Save and close the file.

To configure HP CSA tools (such as the process definition tool, purge tool, schema installation tool, provider tool, or content archive tool) to support IPv6, when configuring the `db.url`, `dbUrl`, or `jdbc.databaseUrl` attribute in the database file used by the tool (for example, `config.properties`, `jdbc.properties`, or `db.properties`), enclose the IPv6 address in square brackets (for example, `[f000:253c::9c10:b4b4]` or `[::1]`).

Launch the Cloud Service Management Console

Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://`*`<ipv6_address>`*`:8444/csa/login`

Chapter 10: Common Access Card

This chapter provides information about the integration between a Common Access Card (CAC) and HP CSA, where CAC is used as the user authentication mechanism. By configuring CAC, you are able to log into HP CSA using a Personal Identity Verification (PIV) card.

After integrating HP CSA with CAC, you can log in to the Cloud Service Management Console and the Marketplace Portal using a PIV card with a valid certificate, log in to the Cloud Service Management Console and the Marketplace Portal using an HP CSA out-of-the-box user account without a PIV card, and cannot log in to the Cloud Service Management Console and the Marketplace Portal as a valid LDAP user without a PIV card.

> **Caution:** For the Cloud Service Management Console, only the JKS keystore type is supported for CAC.

Complete the following steps to integrate HP CSA with CAC:

- Stop HP CSA
- Update JBoss configuration to set up client authentication
- Configure the Cloud Service Management Console
- Configure the Marketplace Portal
- Configure HP SSO
- Configure certificate revocation
- Start HP CSA

Stop HP CSA

To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

Update JBoss Configuration to Set Up Client Authentication

To update the JBoss configuration, do the following:

1. Download the CA certificate for the digital certificate from the PIV card.

2. Import the CA certificate into a new truststore. The truststore type must be JKS. For example, if you named the CA certificate from step 1 `CACcert.cer`, saved it in `/tmp`, and want to create a truststore named `$CSA_HOME/jboss-as/standalone/configuration/.piv_keystore`, run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -file /tmp/CACcert.cer -alias caccert
   -keystore $CSA_HOME/jboss-as/standalone/configuration/.piv_keystore -storepass
   changeit
   ```

3. Edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file:

   - Locate the `<security-realm name="CsaRealm">` element. Within this element and after `</server-identities>`, add the following:

     ```
     <authentication>
        <truststore path="<location of truststore>" keystore-password="<truststore password>"/>
     </authentication>
     ```

     For example,

     ```
     <security-realm name="CsaRealm">
        <server-identities>
           <ssl>
              <keystore keystore-password="changeit" path="/usr/local/hp/jboss-
     as/standalone/configuration/.keystore"/>
           </ssl>
        </server-identities>
        <authentication>
           <truststore path="/usr/local/hp/jboss-as/standalone/configuration/
     .keystore" keystore-password="TruststorePassword"/>
        </authentication>
     </security-realm>
     ```

     Note: This example stores the password in clear text. If you want to use an encrypted password, see "Masking Passwords in standalone.xml Using the JBoss vault Script" on page 45 for information about creating a password vault for JBoss.

   - Locate the `https-listener` element that contains the `name="https` and `security-realm="CsaRealm"` attributes. Add the `verify-client="REQUESTED"` attribute to this element. For example,

```
<https-listener enabled-cipher-suites="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_
SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, ... " name="https" security-
realm="CsaRealm" socket-binding="https" verify-client="REQUESTED"/>
```

Configure the Cloud Service Management Console

Complete the following steps to integrate the Cloud Service Management Console with CAC:

1. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file in a text editor and uncomment the following line:

   ```
   enableCAC=true
   ```

2. Update the Spring Security configuration. Open the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file in a text editor and make the following changes:

   a. Locate both occurrences of the `x509 and custom filter config for CAC` comment and uncomment both occurrences of the following line:

   ```
   <x509 subject-principal-regex="CN=(.*?)," user-service-
   ref="cacUserDetailsService" />
   ```

   Note: The `<x509 subject-principal-regex="CN=(.*?)," user-service-ref="cacUserDetailsService" />` line uses a regular expression to let Spring know that it should extract the CN (Common Name) from the certificate and use it as the username of the user to load the user details. If the username is not stored as the CN in the certificate, you can change the regex to pick it up from the relevant field.

   b. Locate and uncomment both occurrences of the following line:

   ```
   <custom-filter position="LAST" ref="cacFilter" />
   ```

   Note: The `<custom-filter position="LAST" ref="cacFilter" />` line defines the custom filter to be used and specifies that it will need to be set as the LAST filter in the chain of filters.

   c. Locate the `Below is logout filter definition` comment.

   Uncomment the following content:

   ```
   <beans:constructor-arg value="http://www.hp.com"/>
   ```

   And, comment out the following content:

```
<beans:constructor-arg value="/logout.jsp"/>
```

d. Locate the comment `Bean definitions for CAC` and uncomment the content that follows it:

```
<beans:bean id="cacUserDetailsService"
 class="com.hp.csa.authn.impl.CACUserDetailsServiceImpl">
   <beans:property name="restRole" value="ROLE_REST" />
</beans:bean>
<beans: bean id="cacFilter" class="com.hp.csa.authn.impl.CACFilter" />
```

Configure the Marketplace Portal

Complete the following steps to integrate the Marketplace Portal with CAC:

1. Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext-security.xml` file:

   a. Locate the `<!-- START Certificate Authentication Configuration -->` section.

   If you are not using HP SSO, locate and uncomment the `START without HP SSO support` section so that it appears as follows:

```
<!-- START without HP SSO support -->
 <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
     <security:http-basic />
     <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>
     <security:x509 subject-principal-regex="CN=(.*?)," user-service-
ref="cacUserDetailsService" />
     <security:custom-filter position="LAST" ref="cacFilter" />
</security:http>

<bean id="cacFilter"
     class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
     <property name="generateTokenUtil" ref="generateTokenUtil" />
     <property name="tokenFactory" ref="tokenFactory"/>
     <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
     <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
</bean>
<!-- END without HP SSO support -->
```

> **Note:** The `<security:x509 subject-principal-regex="CN=(.*?)," user-service-ref="cacUserDetailsService" />` line uses a regular expression to let Spring know that it should extract the CN (Common Name) from the certificate and use it as the username of the user to load the user details. If the username is not stored as the CN in the certificate, you can change the regex to pick it up from the relevant field. The `<security:custom-filter position="LAST" ref="cacFilter" />` line defines the custom filter to be used and specifies that it will need to be set as the LAST filter in the chain of filters.

b. Uncomment the `START Simplified Logout Configuration` section so that it appears as follows:

```
<!-- START Simplified Logout Configuration -->
<security:http pattern="/idm/v0/logout" use-expressions="true" auto-config="false">
   <security:custom-filter ref="simpleLogoutRedirect" position="FIRST"/>
   <security:http-basic />
</security:http>

<bean id="simpleLogoutRedirect" class="com.hp.ccue.identity.filter.RedirectFilter">
   <property name="url" value="/idm/v0/logout/close"/>
</bean>
<!-- END Simplified Logout Configuration -->
```

c. Uncomment the `START Certificate Authentication / SiteMinder SSO / HP SSO Configuration` section so that it appears as follows:

```
<!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
 <bean id="loginRedirectionHandler"
class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
     <property name="tokenService" ref="tokenService"/>
 </bean>

<bean name="generateTokenUtil"
         class="com.hp.ccue.identity.util.GenerateResponseTokenUtil" />
<!-- END Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
```

2. Edit the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.xml` file:

   a. Comment out `activeDirectoryAuthProvider` and `ldapAuthProvider` so that they appear as follows:

```
<bean id="multiTenantAuthProvider"
class="com.hp.ccue.identity.authn.MultiTenantAuthenticationProvider">
   <property name="providers">
     <list>
       <!-- <ref bean="activeDirectoryAuthProvider"/> -->
       <!-- <ref bean="ldapAuthProvider"/> -->
       <ref bean="seededAuthProvider"/>
    </list>
   </property>
   ......................
</bean>
```

Configure HP SSO

If you want to configure HP SSO in addition to CAC, you can configure HP SSO for the Cloud Service Management Console and/or the Marketplace Portal.

If you enabled HP SSO during the installation of HP CSA, HP SSO has been automatically configured for the Cloud Service Management Console. If you did not enable HP SSO during the installation of

HP CSA, follow the steps located in the Configure the Cloud Service Management Console section to configure HP SSO for the Cloud Service Management Console.

To configure HP SSO for the Marketplace Portal, follow the steps in the Configure the Marketplace Portal section and the Configure HP SSO for the Marketplace Portal with a CAC Integration section below.

Configure HP SSO for the Marketplace Portal with a CAC Integration

To configure HP SSO for the Marketplace Portal if CAC is also configured, complete the applicable steps in the Configure the Marketplace Portal section in addition to the following steps:

1. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring` directory.

2. Make a backup copy of the `applicationContext-security.xml` and `applicationContext-v0.xml` files.

3. Open the `applicationContext-security.xml` file in a text editor and do the following:

    a. Locate the following comment:

    ```
    <!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
    ```

    b. Verify that the following content after these comments are uncommented. If they are commented out, you should uncomment them.

    ```
    <bean id="loginRedirectionHandler"
    class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
       <property name="tokenService" ref="tokenService"/>
    </bean>

    <bean name="generateTokenUtil"
    class="com.hp.ccue.identity.utilities.GenerateResponseTokenUtil" />
    ```

    c. Locate the following comments:

    ```
    <!-- START Certificate Authentication Configuration -->
    <!-- START with HP SSO support -->
    ```

    d. Uncomment the following content after these comments:

    ```
    <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
       <security:http-basic />
       <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
       <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
       <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>
       <security:x509 subject-principal-regex="CN=(.*?)," user-service-
    ref="cacUserDetailsService" />
       <security:custom-filter position="LAST" ref="cacFilter" />
    </security:http>

    <bean id="cacFilter" class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
    ```

```
   <property name="generateTokenUtil" ref="generateTokenUtil" />
   <property name="tokenFactory" ref="tokenFactory"/>
   <property name="tokenWriter" ref="hpssoTokenWriter" />
   <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
   <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
   <property name="auditAppender" ref="auditAppender"/>
</bean>
```

> **Note:** The `<security:x509 subject-principal-regex="CN=(.*?)," user-service-ref="cacUserDetailsService" />` line uses a regular expression to let Spring know that it should extract the CN (Common Name) from the certificate and use it as the username of the user to load the user details. If the username is not stored as the CN in the certificate, you can change the regex to pick it up from the relevant field. The `<security:custom-filter position="LAST" ref="cacFilter" />` line defines the custom filter to be used and specifies that it will need to be set as the LAST filter in the chain of filters.

e. Within the `<!-- START Certificate Authentication Configuration -->` section, locate the `START without HP SSO support` section. Verify that the following content after this comment is commented out. If they are not commented out, you should comment them out.

```
 <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
     <security:http-basic />
     <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>
     <security:x509 subject-principal-regex="CN=(.*?)," user-service-
ref="cacUserDetailsService" />
     <security:custom-filter position="LAST" ref="cacFilter" />
</security:http>

<bean id="cacFilter"
     class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
     <property name="generateTokenUtil" ref="generateTokenUtil" />
     <property name="tokenFactory" ref="tokenFactory"/>
     <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
     <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
</bean>
```

f. Locate the following comment:

```
<!-- START HP SSO Configuration -->
```

g. Verify that the following content after these comments are commented out. If they are not commented out, you should comment them out.

```
<security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:custom-filter ref="noPromptFilter" before="FORM_LOGIN_FILTER" />
   <security:http-basic />
</security:http>

<security:http pattern="/idm/v0/logout" use-expressions="true" auto-config="false">
```

```
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:http-basic />
</security:http>
```

h. Locate the following comment:

```
<!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
```

i. Verify that the following content after these comments are uncommented. If they are commented out, you should uncomment them.

```
<bean id="loginRedirectionHandler"
class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
   <property name="tokenService" ref="tokenService"/>
</bean>

<bean name="generateTokenUtil"
class="com.hp.ccue.identity.utilities.GenerateResponseTokenUtil" />
```

j. Save and exit the file.

4. Open the `applicationContext-v0.xml` file in a text editor and do the following:

   a. Locate the following comment:

   ```
   <!-- START HP SSO Configuration -->
   ```

   b. Verify that the following content after these comments are commented out. If they are not commented out, you should comment them out.

   ```
   <property name="tokenWriter" ref="hpssoTokenWriter" />
   ```

   c. Save and exit the file.

Configure Certificate Revocation

You will need to revoke a certificate if it has been compromised in any way or if an employee leaves your organization.

The following are the methods to revoke a certificate:

- Configure HP CSA to use a Certificate Revocation List (CRL)
- Configure HP CSA to Use a Certificate Revocation List Distribution Point (CRL DP)
- Configure HP CSA to Use the Online Certificate Status Protocol (OCSP)

Configure HP CSA to Use a Certificate Revocation List

The following is an example of how to revoke a certificate that was generated by the certificate authority and publish a Certificate Revocation List (CRL) that contains this certificate ID in the list. The CRL must already exist. You will download and save it in a folder on the system where HP CSA is installed and point to its location using the `ca-revocation-url` parameters.

1. Copy the CRL file to the system where HP CSA is installed (for example, copy it to the `<`*`crl_file_directory`*`>` directory).

2. In the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file, add the `ca-revocation-url="<`*`crl_file`*`>"` attribute to the `<truststore path="<`*`location of truststore`*`>" keystore-password="<`*`truststore password`*`>"/>` element. For example, change the following from:

   ```
   <authentication>
      <truststore path="<location of truststore>" keystore-password="<truststore password>"/>
   </authentication>
   ```

   to

   ```
   <authentication>
      <truststore path="<location of truststore>" keystore-password="<truststore password>" ca-revocation-url="<crl_file>"/>
   </authentication>
   ```

3. Log in to the Cloud Service Management Console or the Marketplace Portal using a revoked certificate. The `Secure Connection Failed` message should display in the browser.

After restarting HP CSA (described below), you should log in to the Cloud Service Management Console or the Marketplace Portal using a revoked certificate. The `Secure Connection Failed` message should display in the browser.

Configure HP CSA to Use a Certificate Revocation List Distribution Point

To enable a Certificate Revocation List Distribution Point (CRL DP), edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file and enable revocation and CRL DP by adding the following lines under `<system-properties>`:

```
<property name="com.sun.net.ssl.checkRevocation" value="true"/>
<property name="com.sun.security.enableCRLDP" value="true"/>
```

Configure HP CSA to Use the Online Certificate Status Protocol

To enable the Online Certificate Status Protocol (OCSP), do the following:

1. Edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file and enable revocation by adding the following line under `<system-properties>`:

   ```
   <property name="com.sun.net.ssl.checkRevocation" value="true"/>
   ```

2. Edit the *`$CSA_JRE_HOME`*`/lib/security/java.security` file and uncomment the following line (where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed):

   ```
   ocsp.enable=true
   ```

Start HP CSA

See "Start HP CSA" on page 129 for detailed information on how to start HP CSA.

Chapter 11: Single Sign-On

This chapter provides information about integrating HP CSA with a single sign-on solution.

Tasks include:

- "Integrate with HP Single Sign-On" below
- "Integrate HP CSA with a Single Sign-On Solution" on page 169
- "Integrate HP CSA with CA SiteMinder" on page 173

Integrate with HP Single Sign-On

HP Single Sign-On (HP SSO) is included with HP CSA and can be used from the Cloud Service Management Console or Marketplace Portal when launching an application from the Cloud Service Management Console or Marketplace Portal. HP SSO must be installed and configured on the application before single sign-on can be integrated between it and HP CSA.

Details on how to integrate HP SSO between the Cloud Service Management Console and HP Operations Orchestration, HP IT Business Analytics, HP Enterprise Maps, or HP Virtualization Performance Viewer are included in this guide. Information regarding HP Operations Orchestration can be found in "HP Operations Orchestration" on page 57. Information regarding HP IT Business Analytics can be found in "Enabling the Cloud Analytics Secondary Tiles" on page 103. Information regarding HP Enterprise Maps can be found in "Enabling the Cloud Transformation Secondary Tiles" on page 105. Information regarding HP Virtualization Performance Viewer can be found in "Configuring the Cloud Optimizer Tile" on page 106.

Details on how to integrate HP SSO between the Marketplace Portal and HP IT Business Analytics are included in this guide. Information regarding HP IT Business Analytics can be found in "Configure the Showback Report Tile" on page 134.

You must configure a user (with the same name and password) for both HP CSA and the other application for single sign-on. You can also configure LDAP users for single sign-on. In order to enable single sign-on for LDAP users, you must either configure HP CSA and the application to use the same LDAP source or, if HP CSA and the application use different LDAP sources, configure the same users in both sources. In either case, the HP CSA user must be assigned to the appropriate role to access the tiles that launch the application and the application user must be assigned a role that allows it to perform the expected functions in the application (for example, viewing flows or viewing reports).

The following sections describe how to enable HP SSO and how to disable HP SSO.

Enable HP Single Sign-On

HP CSA installs HP SSO during installation and provides an option to enable or disable it. If HP SSO was enabled during installation, it has been enabled for the Cloud Service Management Console only. If you want to configure HP SSO for the Marketplace Portal, you must complete the tasks to configure the Marketplace Portal described in this section.

> **Note:** If you have configured or will be configuring a common access card (CAC), you must also complete the steps in Configure HP SSO for the Common Access Card.
>
> If you have configured or will be configuring CA SiteMinder, you must also complete the steps in Configure HP SSO for CA SiteMinder.

> **Caution:** If HP SSO and CA SiteMinder are both configured for HP CSA, and if only HP SSO is enabled for another application, a user logging out from the other application will not be logged out from HP CSA. For example, if HP SSO is enabled between HP CSA and HP Operations Orchestration, when a user logs out from HP Operations Orchestration Central, the user will not be logged out from the Cloud Service Management Console.

Complete the following tasks:

1. Configure the Cloud Service Management Console
2. Configure the Marketplace Portal
3. Restart HP CSA

Configure the Cloud Service Management Console

Complete the following steps to configure and enable HP SSO for the Cloud Service Management Console.

1. Configure the domain name of the network of the server on which HP CSA is installed. Applications launched from the Cloud Service Management Console and Marketplace Portal with which you want to use HP SSO must be installed on systems that belong to this domain.

   > **Note:** If you enabled HP SSO during the installation of HP CSA, you do not need to complete this step as it was automatically performed by the installer.

   a. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF` directory where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed. For example:

      ```
      /usr/local/hp/csa/jboss-as/standalone/deployments/csa.war/WEB-INF
      ```

   b. Make a backup copy of the `hpssoConfiguration.xml` file.

   c. Open the `hpssoConfiguration.xml` file in a text editor.

   d. Locate the following content:

```
<creationDomains>
   <domain>sso.domain</domain>
</creationDomains>
```

e. Change `sso.domain` to domain name of the network of the server on which HP CSA is installed. Applications launched from the Cloud Service Management Console and Marketplace Portal with which you want to use HP SSO must be installed on systems that belong to this domain.

   For example, if your system hostname is `csa_system.xyz.com`, enter `xyz.com` as the domain name.

f. Save and exit the file.

2. Set the HP SSO property.

> **Note:** If you enabled HP SSO during the installation of HP CSA, you do not need to complete this step as it was automatically performed by the installer.

a. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes` directory.

b. Make a backup copy of the `csa.properties` file.

c. Open the `csa.properties` file in a text editor.

d. Locate the following content:

```
#enableHPSSO=true
```

e. Uncomment this line.

f. Save and exit the file.

3. Optionally, change the value of the `initString` setting for the Cloud Service Management Console. If you create a new string, HP recommends using at least 44 characters that are made up of ASCII letters, numbers, and basic symbols (ones that do not need to be escaped). The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).

a. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/` directory.

b. Make a backup copy of the `hpssoConfiguration.xml` file.

c. Open the `hpssoConfiguration.xml` file in a text editor.

d. Locate the `crypto` element and replace the `initString` value.

e. Save and exit the file.

> **Note:** If you are launching the same application from both the Cloud Service Management Console and Marketplace Portal, the `initString` setting for the Cloud Service Management Console and Marketplace Portal must be configured to the same value. See Configure the Marketplace Portal for information on how to configure the setting for the Marketplace Portal

Configure the Marketplace Portal

Complete the following steps to configure HP SSO for the Marketplace Portal.

1. Configure the `initString` setting for the Marketplace Portal.

   > **Note:** If you are launching the same application from both the Cloud Service Management Console and Marketplace Portal, the `initString` setting for the Cloud Service Management Console and Marketplace Portal must be configured to the same value. See Configure the Cloud Service Management Console for information on how to configure the setting for the Cloud Service Management Console

   a. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF` directory.

   b. Make a backup copy of the `hpssoConfig.xml` file.

   c. Open the `hpssoConfig.xml` file in a text editor

   d. Locate the `crypto` element and replace the `initString` value. If you are launching the same application from both the Cloud Service Management Console and Marketplace Portal, copy the `initString` value for the Cloud Service Management Console. Otherwise, create a new string used for HP SSO. When creating a new string, HP recommends using at least 44 characters that are made up of ASCII letters, numbers, and basic symbols (ones that do not need to be escaped). The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).

   e. Save and exit the file.

2. While still in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF` directory, make a backup copy of the `web.xml` file.

3. Open the `web.xml` file in a text editor and do the following:

a. Locate the following comment (near the end of the file):

```
<!-- START HP SSO Configuration -->
```

b. Uncomment the following content after this comment:

```
<listener>
   <listener-class>com.hp.hpsso.HpSsoContextListener</listener-class>
</listener>

<context-param>
   <param-name>com.hp.sw.bto.ast.security.lwsso.conf.fileLocation</param-name>
   <param-value>/usr/local/hp/csa/jboss-as/standalone/deployments/idm-service.war/WEB-
INF/hpssoConfig.xml</param-value>
</context-param>
```

c. Save and exit the file.

4. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring` directory.

5. Make a backup copy of the `applicationContext-security.xml` file.

6. Open the `applicationContext-security.xml` file in a text editor and do the following:

   a. Locate the following comment:

```
<!-- START CAC HPSSO CONFIGURATION -->
```

   b. Uncomment the following content after this comment:

```
<bean id="hpssoFederatingProvider"
class="com.hp.ccue.identity.filter.certificate.CertificateLdapAuthenticationProvider">
   <property name="config" ref="csaAuthConfig" />
   <property name="templateFactory" ref="csaTemplateFactory" />
</bean>

<security:authentication-manager id="hpssoAuthManager">
   <security:authentication-provider ref="hpssoFederatingProvider" />
</security:authentication-manager>

<bean id="hpssoProvidedFilter" class="com.hp.hpsso.api.HpSsoFilter" />

<bean id="hpssoIntegrationFilter" class="com.hp.ccue.identity.filter.hpsso.HpSsoFilter">
   <constructor-arg ref="hpssoAuthManager" />
   <property name="generateTokenUtil" ref="generateTokenUtil" />
   <property name="tokenFactory" ref="tokenFactory"/>
   <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
</bean>

<bean id="hpssoTokenWriter" class="com.hp.ccue.identity.hpsso.HpSsoCookieTokenWriter">
   <property name="tokenStore" ref="tokenStore" />
   <property name="tokenService" ref="tokenService" />
   <property name="tokenFactory" ref="tokenFactory" />
</bean>
```

c. Locate the following comment:

```
<!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
```

d. Uncomment the content that follows the comment so that it appears as follows:

```
<bean id="loginRedirectionHandler"
class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
   <property name="tokenService" ref="tokenService"/>
</bean>

<bean name="generateTokenUtil"
class="com.hp.ccue.identity.utilities.GenerateResponseTokenUtil" />
```

e. Save and exit the file.

7. If CAC and SiteMinder are NOT configured, do the following (if you have configured or plan to configure CAC or SiteMinder, skip this step):

   a. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring` directory.

   b. Make a backup copy of the `applicationContext-security.xml` and `applicationContext-v0.xml` files.

   c. Open the `applicationContext-security.xml` file in a text editor and do the following:

      i. Locate the following comment:

```
<!-- START HP SSO Configuration -->
```

      ii. Verify that the following content after these comments are uncommented. If they are commented out, you should uncomment them.

```
<security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:custom-filter ref="noPromptFilter" before="FORM_LOGIN_FILTER" />
   <security:http-basic />
</security:http>

<security:http pattern="/idm/v0/logout" use-expressions="true" auto-config="false">

   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:http-basic />
</security:http>
```

      iii. Save and exit the file.

   d. Open the `applicationContext-v0.xml` file in a text editor and do the following:

i. Locate the following comment:

```
<!-- START HP SSO Configuration -->
```

ii. Verify that the following content after these comments are uncommented. If they are not uncommented, you should uncomment them.

```
<property name="tokenWriter" ref="hpssoTokenWriter" />
```

iii. Save and exit the file.

Configure HP SSO for the Marketplace Portal with a Common Access Card Integration

Additional steps must be completed to configure HP SSO for the Marketplace Portal with a Common Access Card (CAC) integration. See Configure HP SSO for the Marketplace Portal with a CAC Integration for more information.

> **Note:** Complete the integration with CAC before restarting HP CSA. See "Common Access Card" on page 152 for more information.

Configure HP SSO for the Marketplace Portal with a CA SiteMinder Integration

Additional steps must be completed to configure HP SSO for the Marketplace Portal with a SiteMinder integration. See Configure HP SSO for the Marketplace Portal with a SiteMinder Integration for more information.

> **Note:** Complete the integration with SiteMinder before restarting HP CSA. See "Integrate HP CSA with CA SiteMinder" on page 173 for more information.

Restart HP CSA

Restart HP CSA. To restart HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type
<embeddedHPOOinstallation>`/central/bin/central stop`
<embeddedHPOOinstallation>`/central/bin/central start`.

For example, type

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

Disable HP Single Sign-On

If you no longer want to use HP SSO, you can disable it. Do the following:

1. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes` directory.

2. Make a backup copy of the `csa.properties` file.

3. Open the `csa.properties` file in a text editor.

4. Locate the following content:

   ```
   enableHPSSO=true
   ```

5. Change **true** to **false**.

6. Save and exit the file.

7. Restart HP CSA. To restart HP CSA, on the server that hosts HP CSA, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop` `<embeddedHPOOinstallation>/central/bin/central start`.

   For example, type

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

Integrate HP CSA with a Single Sign-On Solution

While HP CSA provides an SSO solution using CA SiteMinder, there are a variety of scenarios where you may need to perform the integration with HP CSA using another SSO solution. For example, you may be using:

- an implementation where you need to authenticate with an SSO vendor other than CA SiteMinder.

- a different deployment architecture than what is provided by HP CSA.

- a different version of CA SiteMinder than what is supported by HP CSA.

- an entirely different architecture than that which is supported.

In such cases it makes sense to create a custom SSO solution so that you can extend the HP-provided implementation to your own.

For the Cloud Service Management Console and for the Marketplace Portal, SSO cannot be enabled at the same time as CAC.

Verify the HP CSA Provider Organization's LDAP Server Configuration

You should verify that an LDAP user can log into the Cloud Service Management Console and the Marketplace Portal, which should already be configured. By performing this verification, you can be confident that any login issues that occur after integration have nothing to do with this particular configuration.

If there are any login issues, then update or configure the LDAP server for both the provider organization and the consumer organization from the Cloud Service Management Console, which is the interface from which you perform all administration tasks for *both* the Cloud Service Management Console and the Marketplace Portal.

> Note: You must configure the HP CSA Provider organization to use the same LDAP server used by the custom SSO Server. If you do not configure this access point, no one will be able to access the Cloud Service Management Console.

To configure or update the provider organization's LDAP server:

1. Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

   Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

2. Log in to the Cloud Service Management Console as a CSA Administrator.

3. Click the **Organizations** tile.

4. In the left-navigation frame, select the provider organization.

5. From the provider organization's navigation frame, select **LDAP**.

6. Update the LDAP server information.

7. Click **Save**.

Verify the HP CSA Consumer Organization's LDAP Server Configuration

> **Note:** The same LDAP server must be used by the HP CSA Provider organization, HP CSA consumer organization and custom SSO Server.

To configure or update the consumer organization's LDAP server:

1. Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where *`<csahostname>`* is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

   Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

2. Log in to the Cloud Service Management Console as the CSA Administrator.
3. Click the **Organizations** tile.
4. In the left-navigation frame, select a consumer organization.
5. From the consumer organization's navigation frame, select **LDAP**.
6. Update the LDAP server information.
7. Click **Save**.
8. Repeat these steps for every consumer organization configured in HP CSA.

Only the `/csa` and `/mpp` contexts are supported (this is required by the SSO proxy setup).

Configure the Custom SSO Server to Work with HP CSA

To configure your custom SSO server to work with HP CSA, follow the instructions provided with your SSO application.

Stop HP CSA

To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

Configure the Cloud Service Management Console

To configure the Cloud Service Management Console:

1. Update the `applicationContext-security.xml` file as appropriate for your custom SSO solution (based on the Spring Security Framework documentation).

2. Update the `csa.properties` file by uncommenting the string `enableSSO=true` and setting the value of `csa.subscriber.portal.url` to `{<protocol>}://{<host>}/mpp/org/{<orgName>}`.

Configure the Marketplace Portal

To configure the Marketplace Portal:

1. Change `proxy` in the `mpp.json` file to the IP address of the proxy to be used by SSO. See the *Configure Proxy Mapping* section for details.

2. Update the `applicationContext-security.xml` file as appropriate for your custom SSO solution (based on the Spring Security Framework documentation).

3. Update the `applicationContext.xml` file as appropriate for your custom SSO solution (based on the Spring Security Framework documentation).

Configure Proxy Mapping

To configure proxy mapping:

1. Map the `/csa` proxy to the HP CSA deployment.

   > **Caution:** Use only `/csa` as the alias. Using another alias may cause HP CSA to fail.
   >
   > For example, when configuring the alias in an Apache proxy server, set the following:
   >
   > ProxyPass /csa/ https://<*csahostname*>:8444/csa/
   > ProxyPassReverse /csa/ https://<*csahostname*>:8444/csa/

2. Map the `/idm-service` proxy to the Identity Management component deployment.

3. Map the `/mpp` proxy to the Marketplace Portal deployment.

Start HP CSA

To start HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central start`.

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

Verify the SSO Integration

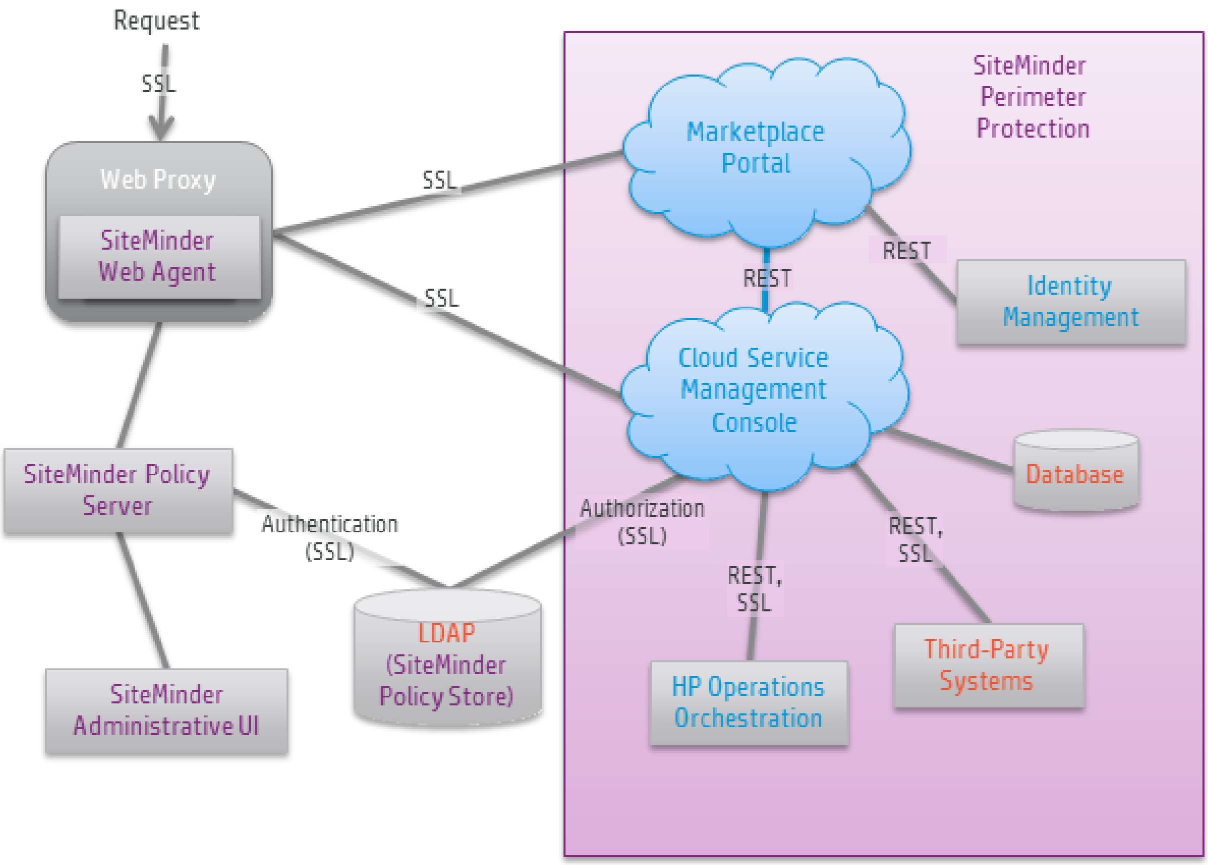
You should verify that the SSO integration works by logging into both the Cloud Service Management Console and the Marketplace Portal using the newly-integrated SSO solution.

Integrate HP CSA with CA SiteMinder

HP CSA, as well as SiteMinder (also called CA Single Sign-On) with a reverse proxy solution, must already be installed and configured before you can integrate them. The LDAP server shared by HP CSA and SiteMinder must be configured for the HP CSA provider and consumer organization (from the Cloud Service Management Console) before integration between HP CSA and SiteMinder is started.

SiteMinder is made up of several components that work with HP CSA and your LDAP server to provide secure access. The information provided in this section configures HP CSA to work with a reverse proxy solution, as shown in the following diagram.

Supported SiteMinder Deployment Architecture



For more information about how to install and configure CA SiteMinder for a reverse proxy solution, refer to the *Configure Reverse Proxy Servers* section in the *Web Agent Configuration Guide* (a Web Agent guide). Documentation for SiteMinder can be found using the following URL:

https://support.ca.com/irj/portal/anonymous/DocumentationSearch

Complete the following steps to integrate HP CSA and SiteMinder:

- Configure the HP CSA Provider and Consumer Organization's LDAP Server
- Configure the SiteMinder Policy Server for HP CSA integration
- Configure the SiteMinder Web Agent for HP CSA Integration
- Configure HP CSA for SiteMinder integration

Configure the HP CSA Provider Organization's LDAP Server

You must configure the HP CSA provider organization to use the same LDAP server used by the SiteMinder Policy Server. If you do not configure this access point before integrating HP CSA and SiteMinder, you will not be able to access HP CSA after integration.

Caution: LDAP must be configured for the HP CSA provider organization before you begin the integration between HP CSA and SiteMinder. After integrating HP CSA and SiteMinder, you can only log in to the Cloud Service Management Console via SiteMinder using a valid user from this LDAP directory. The out-of-the-box HP CSA users can no longer be used to log in to HP CSA.

When using the REST API, the out-of-the-box HP CSA users are still valid after integration.

To configure the provider organization's LDAP server, do the following:

1. Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where *<csahostname>* is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

   Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

2. Log in to the Cloud Service Management Console as a CSA Administrator.

3. Click the **Organizations** tile.

4. In the left-navigation frame, select the provider organization.

5. From the provider organization's navigation frame, select **LDAP**.

6. Update the LDAP server information.

7. Click **Save**.

Configure the HP CSA Consumer Organization's LDAP Server

You must configure each HP CSA consumer organization to use the same LDAP server used by the SiteMinder Policy Server. If you do not configure this access point, no one will be able to access the Marketplace Portal.

To configure a consumer organization's LDAP server, do the following:

1. Launch the Cloud Service Management Console by typing the following URL in a supported web browser: `https://<csahostname>:8444/csa` where *<csahostname>* is the fully-qualified domain name of the system on which the Cloud Service Management Console resides.

   Launch the Cloud Service Management Console using an IPv6 address by typing the following URL in a supported web browser: `https://<ipv6_address>:8444/csa/login`

2. Log in to the Cloud Service Management Console as the CSA Administrator.

3. Click the **Organizations** tile.

4. In the left-navigation frame, select a consumer organization.

5. From the consumer organization's navigation frame, select **LDAP**.

6. Update the LDAP server information.

7. Click **Save**.

8. Repeat these steps for every consumer organization configured in HP CSA.

Configure the SiteMinder Policy Server for HP CSA Integration

Complete the following steps to configure the SiteMinder Policy Server for HP CSA integration.

1. Navigate to **Control Panel** > **Administrative Tools** > **Services**.

2. Right-click on the HP Marketplace Portal service and select **Stop**.

3. Configure the SiteMinder Policy Server to use the LDAP server that will be shared between HP CSA and SiteMinder.

4. Configure the SiteMinder Policy Server idle timeout, the Cloud Service Management Console session timeout, and the Marketplace Portal session timeout to be the same amount of time, regardless of the units (minutes or seconds) used by the parameters in the respective configuration files. By default, the session timeout value for the Cloud Service Management Console is 60 minutes, and for the Marketplace Portal, it is 1800 seconds.

   The session timeout for the Cloud Service Management Console is configured using the `session-timeout` parameter in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/web.xml` file:

   ```
   ...
   <session-config>
   ...
     <session-timeout>60</session-timeout>
   ...
   ```

   The session timeout for the Marketplace Portal is configured using the `timeoutDuration` parameter in the `$CSA_HOME/portal/conf/mpp.json` file:

   ```
   ...
   "session": {
   ...
     "timeoutDuration": 1800,
   ...
   ```

The timeout should match that of the `timeoutDuration` parameter in the `$CSA_HOME/portal/conf/mpp.json` file:

5. Configure the SiteMinder Policy Server cleanup interval for the Marketplace Portal. By default, the cleanup interval is 3600 seconds.

   The cleanup interval for the Marketplace Portal is configured using the `cleanupInterval` parameter in the `$CSA_HOME/portal/conf/mpp.json` file:

   ```
   ...
   "session": {
   ...
     "cleanupInterval": 3600
   ...
   ```

   The `cleanupInterval` parameter is not directly related to the `timeoutDuration` parameter, but it should be twice that of the `timeoutDuration` parameter.

6. To process image file names that contain spaces, from the SiteMinder Policy Server, either comment out the `BadUrlChars` parameter or modify the SiteMinder Policy Server to allow image file names that contain spaces.

7. Navigate to **Control Panel** > **Administrative Tools** > **Services**.

8. Right-click on the HP Marketplace Portal service and select **Start**.

Configure the SiteMinder Web Agent for HP CSA Integration

Configure proxy mapping for the SiteMinder Web Agent. To configure proxy mapping:

1. Map the `/csa` proxy to the HP CSA deployment.

   > **Caution:** Use only `/csa` as the alias. Using another alias may cause HP CSA to fail.

   For example:

   ```
   ProxyPass /csa/ https://<csahostname>:8444/csa/
   ProxyPassReverse /csa/ https://<csahostname>:8444/csa/
   ```

2. Map the `/idm-service` proxy to the Identity Management component deployment. For example:

   ```
   ProxyPass /idm-service/ https://<csahostname>:8444/idm-service/
   ProxyPassReverse /idm-service/ https://<csahostname>:8444/idm-service/
   ```

3. Map the `/mpp` proxy to the Marketplace Portal deployment. For example:

   ```
   ProxyPass /mpp/ https://<csahostname>:8090/mpp/
   ProxyPassReverse /mpp/ https://<csahostname>:8090/mpp/
   ```

Note: The port number must match the value configured for the `port` attribute of the `proxy` element in the `$CSA_HOME/portal/conf/mpp.json` file. By default, this port is 8090.

If you are configuring a remote instance of the Marketplace Portal, use the hostname of the system on which the remote instance of the Marketplace Portal is installed.

Configure HP CSA for SiteMinder Integration

To configure HP CSA for SiteMinder integration, you must:

- Stop HP CSA
- Configure the Cloud Service Management Console
- Configure the Marketplace Portal
- Configure HP SSO
- Start HP CSA

Stop HP CSA

To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type *`<embeddedHPOOinstallation>`*`/central/bin/central stop`.

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

Configure the Cloud Service Management Console

Complete the following steps to configure the Cloud Service Management Console for a SiteMinder reverse proxy solution. Update the `applicationContext-security.xml` file:

1. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF` directory where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed. For example:

   ```
   /usr/local/hp/csa/jboss-as/standalone/deployments/csa.war/WEB-INF
   ```

2. Make a backup copy of the `applicationContext-security.xml` file.

3. Open the `applicationContext-security.xml` file in a text editor.

4. Locate the comment `SSO Authentication Provider` and uncomment the following content that appears after this comment:

   ```
   <security:authentication-provider ref='ssoAuthenticationProvider' />
   ```

5. Locate both occurrences of the comment `custom filter config for SSO` and uncomment both occurrences of the following content that appears after this comment:

   ```
   <custom-filter position="PRE_AUTH_FILTER" ref="ssoSiteminderFilter" />
   ```

6. Locate the comment `Below is logout filter definition` and uncomment the following content that appears after this comment:

   ```
   <beans:constructor-arg value="/ssologout.jsp"/>
   ```

7. In the same section of the file, comment out the following content (if it is not already commented out):

   ```
   <beans:constructor-arg value="/logout.jsp"/>
   ```

8. Locate the comment `Bean definitions for SSO` and uncomment the following content that appears after this comment:

   ```
   <beans:bean id="ssoSiteminderFilter"
    class="com.hp.csa.authn.impl.SSOHeaderAutheticationFilter">
      <beans:property name="principalRequestHeader" value="SM_USER" />
      <beans:property name="authenticationManager"
       ref="authenticationManager" />
      <beans:property name="exceptionIfHeaderMissing" value="true" />
      <beans:property name="ignoreURLContaining">
         <beans:list>
            <beans:value>/csa/rest/</beans:value>
            <beans:value>/csa/api/blobstore</beans:value>
         </beans:list>
      </beans:property>
   </beans:bean>

   <beans:bean id="ssoAuthenticationProvider"
    class="org.springframework.security.web.authentication.preauth.
    PreAuthenticatedAuthenticationProvider">
      <beans:property name="preAuthenticatedUserDetailsService">
         <beans:bean id="userDetailsServiceWrapper"
          class="org.springframework.security.core.userdetails.
          UserDetailsByNameServiceWrapper">
            <beans:property name="userDetailsService"
             ref="ssoPreAuthenticatedUserDetailsService" />
         </beans:bean>
      </beans:property>
   </beans:bean>
   <beans:bean id="ssoPreAuthenticatedUserDetailsService"
   ```

```
class="com.hp.csa.authn.impl.SSOUserDetailsService">
   <beans:property name="restRole" value="ROLE_REST" />
</beans:bean>
```

9. Save and exit the file.

10. Navigate to the `classes` subdirectory (`$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes`).

11. Open the `csa.properties` file in a text editor.

12. Edit the following line to configure the URL to display for the organization in the Cloud Service Management Console:

    ```
    csa.subscriber.portal.url={protocol}://{host}:8089/org/{orgName}
    ```

    You can define a hard-coded URL or a URL that is replaced by information as known by the client-side browser. The following tokens are supported: `protocol` (`http` or `https`), `host` (the host in the browser URL used to access the Cloud Service Management Console), and `orgName` (the organization name of the selected organization in the browser). For example, if the client URL is `https://csa-server.company.com:8444/csa`, for a selected organization named devteam, then after the token replacement, the client displays a URL of `https://csa-server.company.com:8089/#/login/devteam`. No port is defined, and the mpp context is added to the URL. The context should be the same as is defined for the Marketplace Portal in the `mpp.json` file.

13. Locate the comment `Needed for SSO` and uncomment the following content:

    ```
    enableSSO=true
    ```

14. Save and exit the file.

Configure the Marketplace Portal

Complete the following steps to configure the Marketplace Portal for a SiteMinder reverse proxy solution.

1. Open the `$CSA_HOME/portal/conf/mpp.json` file in a text editor.

2. In the `idmProvider` section, for `returnUrl`, change `proxy` to the IP address of the SiteMinder Web Agent proxy and add `redirectUrl` with its value set to the IP address of the SiteMinder Web Agent proxy:

    ```
    "idmProvider": {

        ...........

       "returnUrl": "https://{proxy}/mpp",
    ```

```
   "redirectUrl": "https://{proxy}",
   ............
}
```

For example:

```
"idmProvider": {

    ...........

   "returnUrl": "https://101.32.24.101/mpp",
   "redirectUrl": "https://101.32.24.101",
   ............
}
```

3. Enable the proxy element to be used by the SiteMinder Web Agent by setting `enabled` to `true` as follows:

   ```
   "proxy": {
     "enabled": true,
     "port": 8090,
     "contextPath": "/mpp"
   }
   ```

   To enable single sign-on for the Marketplace Portal, you must also set up proxy mapping on the SiteMinder Web Agent for the Marketplace Portal and for the Identity Management component service. The proxy mapping for the Marketplace Portal must use the same context name (`/mpp`) and port (`8090`) as defined here.

4. Open the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext-security.xml` file in a text editor.

5. Locate the `START SiteMinder SSO Configuration` section.

   - Uncomment the following content so that it appears as follows:

     ```
     <security:authentication-manager id="ssoAuthManager">
        <security:authentication-provider ref="ssoAuthenticationProvider"/>
     </security:authentication-manager>

     <bean id="ssoSiteminderFilter"
     class="org.springframework.security.web.authentication.preauth.RequestHeaderA
     uthenticationFilter">
        <property name="principalRequestHeader" value="SM_USER"/>
        <property name="authenticationManager" ref="ssoAuthManager" />
        <property name="exceptionIfHeaderMissing" value="true" />
     </bean>
     ```

- If you are not using HP SSO, locate both occurrences of the comment `(SiteMinder SSO only)` and uncomment the content that follows the comment so that it appears as follows:

  ```
  <!-- (SiteMinder SSO only) -->
   <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
     <security:http-basic />
     <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>
     <security:custom-filter position="PRE_AUTH_FILTER" ref="ssoSiteminderFilter" />
     <security:custom-filter position="LAST" ref="ssoFilter" />
  </security:http>

  <!-- (SiteMinder SSO only) -->
   <bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter">
     <property name="generateTokenUtil" ref="generateTokenUtil" />
     <property name="tokenFactory" ref="tokenFactory" />
     <property name="loginRedirectionHandler" ref="loginRedirectionHandler" />
  </bean>
  ```

6. Uncomment the `START Simplified Logout Configuration` section so that it appears as follows:

   ```
   <!-- START Simplified Logout Configuration -->
   <security:http pattern="/idm/v0/logout" use-expressions="true" auto-config="false">
      <security:custom-filter ref="simpleLogoutRedirect" position="FIRST"/>
      <security:http-basic />
   </security:http>

   <bean id="simpleLogoutRedirect" class="com.hp.ccue.identity.filter.RedirectFilter">
      <property name="url" value="/idm/v0/logout/close"/>
   </bean>
   <!-- END Simplified Logout Configuration -->
   ```

7. Uncomment the `START Certificate Authentication / SiteMinder SSO / HP SSO Configuration` section so that it appears as follows:

   ```
   <!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->

    <bean id="loginRedirectionHandler"
   class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
        <property name="tokenService" ref="tokenService"/>
    </bean>

   <bean name="generateTokenUtil" class="com.hp.ccue.identity.util.GenerateResponseTokenUtil" />

    <!-- END Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
   ```

8. Uncomment the `START CAC HPSSO CONFIGURATION` section so that it appears as follows:

   ```
   <!-- START CAC HPSSO CONFIGURATION -->
   <bean id="hpssoFederatingProvider"
   class="com.hp.ccue.identity.filter.certificate.CertificateLdapAuthenticationProvider">
      <property name="config" ref="csaAuthConfig" />
      <property name="templateFactory" ref="csaTemplateFactory" />
   </bean>

   <security:authentication-manager id="hpssoAuthManager">
   ```

```
   <security:authentication-provider ref="hpssoFederatingProvider" />
</security:authentication-manager>

<bean id="hpssoProvidedFilter" class="com.hp.hpsso.api.HpSsoFilter" />

<bean id="hpssoIntegrationFilter" class="com.hp.ccue.identity.filter.hpsso.HpSsoFilter">
   <constructor-arg ref="hpssoAuthManager" />
   <property name="generateTokenUtil" ref="generateTokenUtil" />
   <property name="tokenFactory" ref="tokenFactory"/>
   <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
</bean>

<bean id="hpssoTokenWriter" class="com.hp.ccue.identity.hpsso.HpSsoCookieTokenWriter">
   <property name="tokenStore" ref="tokenStore" />
   <property name="tokenService" ref="tokenService" />
   <property name="tokenFactory" ref="tokenFactory" />
</bean>
<!-- END CAC HP SSO Configuration -->
```

9. Open the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.xml` file in a text editor.

10. Uncomment the `START SiteMinder SSO Configuration` section so that it appears as follows:

```
<!-- START SiteMinder SSO Configuration -->

<bean id="ssoAuthenticationProvider"
class="org.springframework.security.web.authentication.preauth.PreAuthenticatedAuthenticatio
nProvider">
   <property name="preAuthenticatedUserDetailsService">
      <bean id="userDetailsServiceWrapper"
class="org.springframework.security.core.userdetails.UserDetailsByNameServiceWrapper">
         <property name="userDetailsService" ref="ssoPreAuthenticatedUserDetailsService" />
      </bean>
   </property>
</bean>

<bean id="ssoPreAuthenticatedUserDetailsService"
class="com.hp.ccue.identity.filter.sso.SSOUserDetailsServiceImpl">
   <property name="restRole" value="ROLE_REST" />
</bean>

<!-- END SiteMinder SSO Configuration -->
```

Configure HP SSO

If you want to configure HP SSO in addition to SiteMinder, you can configure HP SSO for the Cloud Service Management Console and/or the Marketplace Portal.

If you enabled HP SSO during the installation of HP CSA, HP SSO has been automatically configured for the Cloud Service Management Console. If you did not enable HP SSO during the installation of HP CSA, follow the steps located in the Configure the Cloud Service Management Console section to configure HP SSO for the Cloud Service Management Console.

To configure HP SSO for the Marketplace Portal, follow the steps in the Configure the Marketplace Portal section and the Configure HP SSO for the Marketplace Portal with a SiteMinder Integration section below.

Configure HP SSO for the Marketplace Portal with a SiteMinder Integration

To configure HP SSO for the Marketplace Portal if SiteMinder is also installed, complete the applicable steps in the Configure the Marketplace Portal section in addition to the following steps:

1. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring` directory.

2. Make a backup copy of the `applicationContext-security.xml` and `applicationContext-v0.xml` files.

3. Open the `applicationContext-security.xml` file in a text editor and do the following:

   a. Locate the following comment:

   ```
   <!-- START Certificate Authentication / SiteMinder SSO / HP SSO Configuration -->
   ```

   b. Verify that the following content after these comments are uncommented. If they are commented out, you should uncomment them.

   ```
   <bean id="loginRedirectionHandler"
   class="com.hp.ccue.identity.filter.LoginRedirectionHandler">
      <property name="tokenService" ref="tokenService"/>
   </bean>

   <bean name="generateTokenUtil"
   class="com.hp.ccue.identity.utilities.GenerateResponseTokenUtil" />
   ```

   c. Locate the `START SiteMinder SSO Configuration` section.

   d. Locate both occurrences of the comment (`SiteMinder SSO with HP SSO`) and uncomment the content that follows the comment so that it appears as follows:

   ```
   <!-- (SiteMinder SSO with HP SSO) -->
   <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
      <security:http-basic />
      <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
      <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
      <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
      <security:custom-filter ref="ssoSiteminderFilter" before="CAS_FILTER" />
      <security:custom-filter ref="ssoFilter" position="LAST" />
   </security:http>

   <!-- (SiteMinder SSO with HP SSO) -->
   <bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter">
      <property name="generateTokenUtil" ref="generateTokenUtil" />
      <property name="tokenFactory" ref="tokenFactory" />
      <property name="loginRedirectionHandler" ref="loginRedirectionHandler" />
      <property name="tokenWriter" ref="hpssoTokenWriter" />
   </bean>
   ```

e. Locate both occurrences of the comment `(SiteMinder SSO only)` and verify that the following content after this comment (in both locations) are commented out. If they are not commented out, you should comment them out.

```
<!-- (SiteMinder SSO only) -->
<!-- <security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
   <security:http-basic />
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>
   <security:custom-filter position="PRE_AUTH_FILTER" ref="ssoSiteminderFilter" />
   <security:custom-filter position="LAST" ref="ssoFilter" />
</security:http> -->

<!-- (SiteMinder SSO only) -->
<!-- <bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter">
   <property name="generateTokenUtil" ref="generateTokenUtil" />
   <property name="tokenFactory" ref="tokenFactory" />
   <property name="loginRedirectionHandler" ref="loginRedirectionHandler" />
</bean> -->
```

f. Locate the following comment:

```
<!-- START HP SSO Configuration -->
```

g. Verify that the following content after these comments are commented out. If they are not commented out, you should comment them out.

```
<security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:custom-filter ref="noPromptFilter" before="FORM_LOGIN_FILTER" />
   <security:http-basic />
</security:http>

<security:http pattern="/idm/v0/logout" use-expressions="true" auto-config="false">
   <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST" />
   <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER" />
   <security:custom-filter ref="hpssoIntegrationFilter" after="PRE_AUTH_FILTER" />
   <security:http-basic />
</security:http>
```

h. Save and exit the file.

4. Open the `applicationContext-v0.xml` file in a text editor and do the following:

a. Locate the following comment:

```
<!-- START HP SSO Configuration -->
```

b. Verify that the following content after these comments are commented out. If they are not commented out, you should comment them out.

```
<property name="tokenWriter" ref="hpssoTokenWriter" />
```

c. Save and exit the file.

Start HP CSA

To start HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central start`.

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

Launch the Marketplace Portal

After completing the Marketplace Portal changes and restarting HP CSA, launch the Marketplace Portal using the URL: `https://<proxy_server_ip>/mpp/`. Depending on the Web agent configuration being used, a proxy server port *may* be required.

> **Note:** If the single sign-on prompt appears multiple times when accessing the Marketplace Portal, you may need to configure the Marketplace Portal to use the fully-qualified domain name of the SiteMinder Web Agent.

Customize the Marketplace Portal Landing Page (Optional)

When accessing the Marketplace Portal during a single sign-on session, the user lands on the landing page displaying a button to be clicked to get to the Marketplace Portal dashboard. By default, the button is labeled "Log In." This might cause confusion as the authentication has already been completed using a single sign-on login prompt. In order to avoid this confusion, the label of the button can be modified:

1. Edit the `$CSA_HOME/portal/node_modules/mpp-ui/dist/locales/<locale>/rb.json` file. The location of the file depends on the locale being used. For example, for English, the file is `$CSA_HOME/portal/node_modules/mpp-ui/dist/locales/en/rb.json`:

   Modify the label of the login button. For example, to change the label to "Click to continue," make the following modification:

   ```
   "login": {
   .......
   "login": "Click to continue",
   .......
   }
   ```

2. Restart the Marketplace Portal service.

   From a command prompt, type `service mpp restart`.

Customize the Logout Page (Optional)

After clicking the `Log out` link from the Cloud Service Management Console or the Marketplace Portal, the user is directed to a logout page. This page is customizable.

The following is the name and location of the logout file. There is one file for the Cloud Service Management Console and another file for the Marketplace Portal.

- Cloud Service Management Console:

  ```
  $CSA_HOME/jboss-as/standalone/deployments/
  csa.war/ssologout.jsp
  ```

  where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed. For example:

  ```
  /usr/local/hp/csa/jboss-as/standalone/
  deployments/csa.war/ssologout.jsp
  ```

- Marketplace Portal:

  ```
  $CSA_HOME/portal/node_modules/mpp-ui/dist/locales/en/rb.json
  ```

  where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed. For example:

  ```
  /usr/local/hp/csa/portal/node_modules/mpp-ui/dist/locales/en/rb.json
  ```

  In the above example, the `rb.json` file is for the English locale (language) and is therefore in the `en` folder.

  You customize the logout message for your locale by modifying the `youAreOut` text. For example, for English locales, you can modify the text as follows:

  ```
  "logout":{
     ...
        "youAreOut": "Please close your browser window. This prevents the
  possibility of someone pressing the ''Back'' button on your browser and possibly
  viewing confidential information.",
     ...
  },
  ```

  For other locales, modify the corresponding `rb.json` files.

Note: By default, after logging out, the user must close the Web browser in order to completely clear the SiteMinder session.

The logout page can be customized to point to a SiteMinder logout page if one is available.

Configure the Marketplace Portal to Use the Fully-Qualified Domain Name of the SiteMinder Web Agent (Optional)

The single sign-on prompt might appear multiple times when trying to access the Marketplace Portal when the domain name generated in the SiteMinder cookie (SMSESSION) does not match the address that is used to access the Marketplace Portal. If this problem occurs, do the following:

1. If the system (from which the browser that accesses the Marketplace Portal is launched) is unable to recognize the fully-qualified domain name of the SiteMinder Web Agent, update the system configuration to define an alias for the fully-qualified domain name to the IP address of the SiteMinder Web Agent. For example, define an alias in the host file.

2. On the system on which the Marketplace Portal is installed, do the following:

   a. Update the following properties in the `$CSA_HOME/portal/conf/mpp.json` file:

   ```
   "idmProvider": {
   .......
   "returnUrl": "https://<FQDN_OF_SITEMINDER_WEB_AGENT>/mpp",
   "redirectUrl": "https://<FQDN_OF_SITEMINDER_WEB_AGENT>",
   .......
   }
   ```

   b. Update the system configuration to define an alias for the fully-qualified domain name to the IP address of the SiteMinder Web Agent. For example, define an alias in the host file.

   c. Restart the system. Verify that the Marketplace Portal service has restarted.

3. On the system on which HP CSA is installed, do the following:

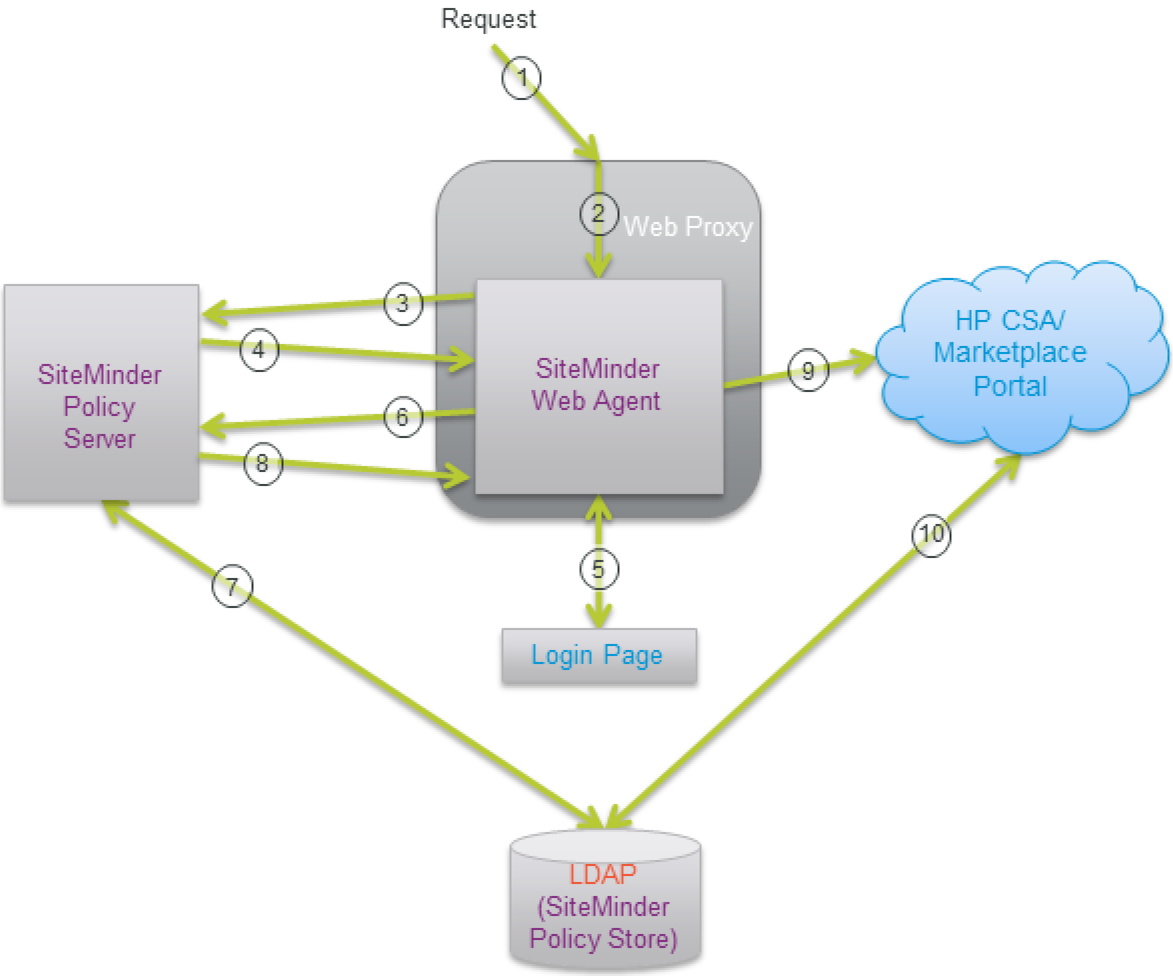
   a. Verify that the Organization URL (the URL used to access the Marketplace Portal) displayed in the Cloud Service Management Console uses the fully-qualified domain name of the SiteMinder Web Agent. To view the Organization URL, from the Cloud Service Management Console dashboard, select the Organizations tile. In the left navigation frame, select the organization. In the organization's navigation frame, select **General Information**.

   b. If the Organization URL does not use the fully-qualified domain name of the SiteMinder Web Agent, update the `csa.subscriber.portal.url` property in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file.

   c. If you updated the `csa.subscriber.portal.url` property, restart the HP Cloud Service Automation service (from a command prompt, type `service csa restart`).

Request Flow

The following diagram shows how a request is processed when HP CSA and SiteMinder are integrated.



1. A user sends a request to launch the Marketplace Portal.

2. The request is intercepted by the SiteMinder Web Agent.

3. The SiteMinder Web Agent queries the SiteMinder Policy Server to determine if it is a protected URL.

4. The SiteMinder Policy Server verifies that the URL is protected.

5. The user is redirected by the SiteMinder Web Agent to a login page where the user's credentials are collected.

6. The SiteMinder Web Agent sends the user's credentials to the SiteMinder Policy Server for authentication.

7. The SiteMinder Policy Server authenticates the user's credentials using the LDAP server (SiteMinder Policy Store).

8. The verification of the authenticated user is returned to the SiteMinder Web Agent.

9. The SiteMinder Web Agent redirects the user's request to launch the Marketplace Portal, which uses the Identity Management component to generate the necessary token.

10. HP CSA uses the token (included in the X-Auth-Token HTTP header) to perform the authorization. The name of the HTTP header may be different if you customized the `xAuthToken` configuration property in the `csa.properties` configuration file.

Additional requests from the user using the same SiteMinder session are automatically directed by the SiteMinder Web Agent to HP CSA.

Chapter 12: Database Administration

This chapter provides miscellaneous information about maintaining the database.

Tasks include:

- "Restart the Database" below
- "Configure the CSA Reporting Database User" below
- "Update the HP CSA Database User or Password" on page 195 (required if you change the database user or password)
- "Import Large Archives" on page 197
- "Purge Service Subscriptions and Audit Data" on page 199
- "Install the HP CSA Database Schema" on page 209
- "Configure HP CSA to Mitigate Frequently Dropped Database Connections" on page 216

Restart the Database

If you restart the database, you must restart the HP Cloud Service Automation service. If you do not restart the service, you may not be able to log in to the Cloud Service Management Console or Marketplace Portal.

Note: You only need to restart the HP Cloud Service Automation service. You do not need to restart the Marketplace Portal service.

To restart the service, on the server that hosts HP CSA, type the following:

```
service csa start
```

Configure the CSA Reporting Database User

This section explains how to configure the CSA reporting database user and role and run the schema installation script to define a read-only user required to use the reporting capabilities of HP CSA.

If you already configured the CSA reporting database user and role and defined the CSA reporting database user when running the installer or upgrade installer, you do not need to repeat these steps (the CSA reporting database user is already configured).

If you installed or upgraded HP CSA but did not configure the CSA reporting database user during the installation or upgrade and want to use the reporting capabilities of HP CSA, complete the tasks in this section.

To configure the CSA reporting database user, do the following:

1. Create a read-only user.

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

   For example, do one of the following, based on the database you are using with HP CSA:

   Oracle

   Run the following commands to create the CSAReportingDBRole role and CSAReportingDBUser user:

   ```
   Create user CSAReportingDBUser identified by CSAReportingDBUser;
   Create role CSAReportingDBRole;
   Grant CREATE SESSION to CSAReportingDBUser;
   Grant CSAReportingDBRole to CSAReportingDBUser;
   Alter user CSAReportingDBUser default role CSAReportingDBRole;
   ```

   You will also need to add the CREATE ANY SYNONYM privilege to the HP CSA database user. This allows the HP CSA database user to create synonyms for the HP CSA reporting (read-only) database user.

   For example, if the HP CSA database user is named CSADBUser, run the following command:

   ```
   Grant CREATE ANY SYNONYM to CSADBUser
   ```

   Microsoft SQL

   Add a reporting database user (CSAReportingDBUser) to the HP CSA database with no roles:

   ```
   CREATE LOGIN CSAReportingDBUser WITH PASSWORD = '<csareportingdbuser_
   password>';
   CREATE USER CSAReportingDBUser FOR LOGIN CSAReportingDBUser WITH DEFAULT_SCHEMA
   = csa;
   ```

   PostgreSQL

   From the psql prompt, enter the following:

   ```
   CREATE ROLE CSAReportingDBUser LOGIN PASSWORD '<csareportingdbuser_password>'
   NOSUPERUSER NOCREATEDB NOCREATEROLE INHERIT;
   GRANT CONNECT ON DATABASE csadb to CSAReportingDBUser;
   ```

2. Run the following script:

   Oracle

   ```
   $CSA_HOME/scripts/reporting/oracle/grant-reporting-user.sql
   ```

   Microsoft SQL

   ```
   $CSA_HOME/scripts/reporting/mssql/grant-reporting-user.sql
   ```

   PostgreSQL

   ```
   $CSA_HOME/scripts/reporting/postgresql/grant-reporting-user.sql
   ```

3. Restart HP CSA.

   To restart HP CSA, on the server that hosts HP CSA, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type
   `<embeddedHPOOinstallation>/central/bin/central stop`
   `<embeddedHPOOinstallation>/central/bin/central start`.

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

4. The CSA reporting database user can access the data using the following view:

   ```
   RPT_RSC_CAPACITY_V
   ```

Update the HP CSA Database System

If you changed the hostname, domain, IP address, or port of the system on which the database used by HP Cloud Service Automation is installed, you must update the HP Cloud Service Automation configuration files that store this information.

1. Stop the HP Cloud Service Automation service.

   To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type
   `<embeddedHPOOinstallation>/central/bin/central stop`.

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

2. On the system running HP Cloud Service Automation, open a command prompt and change to the `$CSA_HOME/jboss-as/standalone/configuration` directory where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

3. In a text editor, open the `standalone.xml` file.

4. In the file, locate the `<datasource>` element of the HP Cloud Service Automation database and the system information to be updated. For example:

   Microsoft SQL Server

   ```
   <datasource jndi-name="java:jboss/datasources/csaDS" pool-name="mssqlDS">
      <connection-
   url>jdbc:jtds:sqlserver://127.0.0.1:1433/csadb;ssl=request</connection-url>
      <driver>mssqlDriver</driver>
   .
   .
   .
   </datasource>
   ```

   Oracle

   ```
   <datasource jndi-name="java:jboss/datasources/csaDS" pool-name="OracleDS">
      <connection-url>jdbc:oracle:thin:@//127.0.0.1:1521/csadb</connection-url>
      <driver>oracleDriver</driver>
   .
   .
   .
   </datasource>
   ```

   PostgreSQL

   ```
   <datasource enabled="true" jndi-name="java:jboss/datasources/csaDS" jta="true"
   pool-name="csaPostgresDS" use-ccm="true" user-java-context="true">
      <connection-url>jdbc:postgresql://127.0.0.1:5432/csadb</connection-url>
      <driver>pgsqlDriver</driver>
   .
   .
   .
   </datasource>
   ```

5. The highlighted text should contain the old fully-qualified domain name, IP address, and/or port that must be updated. Replace this highlighted text with the new fully-qualified domain name, IP address, and/or port.

6. Save the `standalone.xml` file.

7. Restart HP Cloud Service Automation service.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

8. If you are using a tool (such as the content archive tool, process definition tool, provider tool, purge tool, or schema installation tool) that uses a database or configuration properties file (for example, `db.properties` or `config.properties`), update the appropriate property or properties in the file. By default, the file is located in the `$CSA_HOME/Tools/<Tool_Name>` directory.

Update the HP CSA Database User or Password

If you changed the user or password of the database used by HP Cloud Service Automation, you must update the JBoss DataSource and other files that store this information.

1. On the system running HP Cloud Service Automation, open a command prompt and change to the directory `$CSA_HOME/jboss-as` where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

2. Run the following command to generate an encoded version of the new database password:

   ```
   $CSA_JRE_HOME/bin/java -cp
   "modules/system/layers/base/org/jboss/logging/main/jboss-logging-
   3.1.4.GA.jar;modules/system/layers/base/org/picketbox/main/picketbox-
   4.0.21.Final.jar" org.picketbox.datasource.security.SecureIdentityLoginModule
   <password>
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

   Copy the encoded password value that is returned (do not include spaces).

3. Stop the HP Cloud Service Automation service.

   To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

4. In a text editor, open the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file.

5. In the file, locate the following content:

Microsoft SQL Server

```
<security-domain name="csa-encryption-sec" cache-type="default">
   <authentication>
      <login-module
code="org.picketbox.datasource.security.SecureIdentityLoginModule"
flag="required">
         <module-option name="username" value="<old_user_name>"/>
         <module-option name="password" value="<old_encoded_password>"/>
         <module-option name="managedConnectionFactoryName"
value="jboss.jca:service=LocalTxCM,name=mssqlDS"/>
      </login-module>
   </authentication>
</security-domain>
```

Oracle

```
<security-domain name="csa-encryption-sec" cache-type="default">
   <authentication>
      <login-module
code="org.picketbox.datasource.security.SecureIdentityLoginModule"
flag="required">
         <module-option name="username" value="<old_user_name>"/>
         <module-option name="password" value="<old_encoded_password>"/>
         <module-option name="managedConnectionFactoryName"
value="jboss.jca:service=LocalTxCM,name=OracleDS"/>
      </login-module>
   </authentication>
</security-domain>
```

PostgreSQL

```
<security-domain name="csa-encryption-sec" cache-type="default">
   <authentication>
      <login-module
code="org.picketbox.datasource.security.SecureIdentityLoginModule"
flag="required">
         <module-option name="username" value="<old_user_name>"/>
         <module-option name="password" value="<old_encoded_password>"/>
         <module-option name="managedConnectionFactoryName"
value="jboss.jca:service=LocalTxCM,name=PostgresDS"/>
      </login-module>
   </authentication>
</security-domain>
```

6. Replace <*old_encoded_password*> with the new encoded password you copied in step 2 and <*old_user_name*> with the new user name.

7. Save the `standalone.xml` file.

8. Restart HP Cloud Service Automation service.

See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

9. If you are using a tool (such as the content archive tool, process definition tool, provider tool, purge tool, or schema installation tool) that uses a database or configuration properties file (for example, `db.properties` or `config.properties`), update the appropriate property or properties in the file. By default, the file is located in the `$CSA_HOME/Tools/<Tool_Name>` directory.

   The password property value should be *encrypted* (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

Import Large Archives

Archives exported from HP CSA can be imported to install artifacts or update existing artifacts in HP CSA. Archives can be imported using the HP CSA Content Archive Tool, the Cloud Service Management Console, or the REST API.

The default configuration for importing archives supports an archive up to 2 MB in size. When an archive larger than 2 MB is imported (typically, a catalog), the import operation may hang or take a very long time to complete. If an archive is larger than 2 MB, HP recommends using the Content Archive Tool and increasing the JVM heap size.

Import Large Archives Using the HP CSA Content Archive Tool

If you want to import an archive larger than 2 MB, HP recommends using the Content Archive Tool because the tool uses its own JVM heap (it does not share the JVM heap used by HP CSA). When you reconfigure the JVM heap size for the tool, you do not need to restart HP CSA and HP CSA performance is not affected by the import.

To increase the JVM heap size when running the Content Archive Tool, add the `-Xms<heap_size>M -Xmx<heap_size>M` options to the command line. For example, to increase the JVM heap size to 3 GB, type:

```
$CSA_JRE_HOME/bin/java -Xms3072M -Xmx3072M -jar content-archive-tool.jar -i -z
catalog_archive.zip
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Note: By default, the JVM heap size used by the Content Archive Tool is 2 GB. If you want to use a larger JVM heap size, you must always specify the two options listed above when running the Content Archive Tool.

For more information about the Content Archive Tool, refer to the *HP Cloud Service Automation Content Archive Tool* guide.

Import Large Archives from the Cloud Service Management Console or through the REST API

If you want to import an archive larger than 2 MB, HP recommends using the Content Archive Tool. If you must use the Cloud Service Management Console or REST API to import a large archive, you must update the JVM heap size for HP CSA which requires HP CSA to be restarted. Also, importing a large archive from the Cloud Service Management Console or through the REST API may slow the performance of HP CSA.

To increase the JVM heap size before importing a large archive from the Cloud Service Management Console or through the REST API, do the following:

1. Stop HP CSA.

   To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

2. Increase the JVM heap size for HP CSA.

   a. Open the `$CSA_HOME/jboss-as/bin/standalone.conf` file in a text editor.

   b. Locate the following line:

      ```
      set "JAVA_OPTS=$JAVA_OPT -Xms2048M -Xmx2048M -XX:ReservedCodeCacheSize=256M
      "
      ```

   c. Increase the JVM heap size (by default, the JVM heap size is 1 GB). For example, to change the JVM heap size to 3 GB, change the line to:

      ```
      set "JAVA_OPTS=$JAVA_OPT -Xms3072M -Xmx3072M -XX:ReservedCodeCacheSize=256M
      "
      ```

   d. Save and close the file.

3. Start HP CSA.

   To start HP CSA, on the server that hosts HP CSA, type the following:

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

If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central start`.

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

For more information about importing archives from the Cloud Service Management Console, refer to the HP Cloud Service Management Console Help. For more information about importing archives through the REST API, refer to the *HP CSA API Reference* guide.

Purge Service Subscriptions and Audit Data

The purge tool can be used to delete service subscriptions and audit data.

About Service Subscriptions

Canceled, expired, failed, and retired service subscriptions store information in the database that, over time, is no longer needed. The purge tool can be used to delete canceled, expired, failed, and retired subscriptions along with specific associated or referenced artifacts and entities. Canceled, expired, and failed subscriptions must have a service instance status of failed, canceled, cancellation failed, or expiration failed in order to be deleted. Canceled, expired, and failed subscriptions that are not in one of these states will not be deleted. All retired subscriptions are deleted.

By default, when the purge tool is run, canceled, expired, failed, and retired subscriptions that are older than 400 days (subscriptions that have been in a canceled, expired, failed, or retired state longer than 400 days) and certain referenced artifacts and entities are deleted from the database. The age of deleted subscriptions can be increased or decreased by modifying the `age.in.days.to.purge.subscription` property in the configuration properties file used by the purge tool.

When a subscription is deleted, the following artifacts and entities are deleted from the database:

Deleted Artifact	Referenced by (Reference Fields)	Referenced Artifacts and Entities that are Deleted
ServiceSubscription		action associatedRequest basePrice catalogItem initiatingServiceRequest pricingModel property serviceInstance totalPrice

Deleted Artifact	Referenced by (Reference Fields)	Referenced Artifacts and Entities that are Deleted
ServiceRequest	ServiceSubscription (associatedRequest or initiatingServiceRequest)	action basePrice pricingModel property totalPrice
ServiceInstance	ServiceSubscription (serviceInstance)	componentRoot
ServiceComponent	ServiceInstance (componentRoot)	action property resourceBinding
ResourceBinding	ServiceComponent (resourceBinding)	action catalogItem lifecycleProperties property resourceInstance
ResourceSubscription	ResourceBinding (resourceInstance)	action catalogItem lifecycleProperties property
ProcessInstance		

About Audit Data

HP CSA creates audit event records in the database for events that occur during the lifetime of a running instance of HP CSA.

By default, when the purge tool is run, audit data that is older than 400 days is deleted from the database. The age of deleted audit data can be increased or decreased by modifying the `age.in.days.to.purge.audit` property in the configuration properties file used by the purge tool.

For more information about auditing data, refer to the *Reporting and Auditing* whitepaper.

Deleting Service Subscriptions and Audit Data

To delete canceled, expired, failed, and retired subscriptions or audit data from the database, do the following:

> **Caution:** Deleted subscriptions and audit data cannot be restored unless you have backed up the database.

1. Change to the `$CSA_HOME/Tools/db-purge-tool/` directory where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

2. Generate the sample configuration files by running the following command (a sample configuration file is generated for each type of database supported by HP CSA):

   Oracle

   ```
   $CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -g -j ojdbc6.jar
   ```

   where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool/`.

   Note: Additional command line options are required if a secure connection is enabled between the Oracle database and HP CSA. See step 4 below for more information.

   MS SQL and PostgreSQL

   ```
   $CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -g
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

3. In the current directory, copy the sample configuration file that corresponds to the type of database you are using to a file named `config.properties`. For example, if you are using an Oracle database, make a copy of the `config.properties.oracle` file and rename it to `config.properties`. Update the content of `config.properties` as needed, as described in the table:

Property Name	Description

jdbc.
driver
ClassName
	The JDBC driver class.
	Examples
	Oracle:
	`jdbc.driverClassName=oracle.jdbc.driver.OracleDriver`
	MS SQL:
	`jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver`
	PostgreSQL: `jdbc.driverClassName=org.postgresql.Driver`

Property Name	Description

jdbc.dialect	The classname that allows JDBC to generate optimized SQL for a particular database.
	Examples
	Oracle: `jdbc.dialect=org.hibernate.dialect.OracleDialect`
	MS SQL:
	`jdbc.dialect=org.hibernate.dialect.SQLServerDialect`
	PostgreSQL:
	`jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect`

Property Name	Description

jdbc.
databaseUrl
	The JDBC URL. When specifying an IPv6 address, it must be enclosed in square brackets (see examples below).
	Examples
	Oracle (TLS not enabled):
	`jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE`
	Oracle (TLS not enabled, using an IPv6 address):
	`jdbc.databaseUrl=jdbc:oracle:thin:@//[f000:253c::9c10:b4b4]:1521/XE`
	Oracle (TLS enabled, HP CSA does not check the database DN):
	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL)))` where `<host>` is the name of the system on which the Oracle database server is installed.
	Oracle (TLS enabled, HP CSA checks the database DN):
	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN="CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))` where `<host>` is the name of the system on which the Oracle database server is installed and the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server.
	MS SQL (TLS not enabled):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/ example;ssl=request`
	MS SQL (TLS not enabled, using an IPv6 address):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://[::1]:1433/ example;ssl=request`
	MS SQL (TLS enabled):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/ example;ssl=authenticate`
	PostgreSQL:
	`jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/csadb`

Property Name	Description
jdbc. username	The user name of the database user you configured for HP Cloud Service Automation after installing the database.
jdbc. password	The password for the database user. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. **Example** `jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)`
idmConfig.Url	The system on which HP CSA is installed. **Default:** https://127.0.0.1:8444
securityTransport. UserName	The user used to authenticate legacy REST API calls. **Default:** csaTransportUser

securityTransport.
password
	The password for the user used to authenticate legacy REST API calls. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.
	Example
	`securityTransport.password=`
	`ENC(rlbE8430uFSDljert85441e7fe70ljkY)`

securityIdmTransport. UserName	The user used to authenticate consumer REST API calls. **Default:** idmTransportUser

securityIdmTransport.
password
	The password for the user used to authenticate consumer REST API calls. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.
	Example
	`securityIdmTransport.password=ENC`
	`(lDdh98Kfe76op8lhjE0El897klRCB532lsb)`

Property Name	Description
age.in.days. to.purge. audit	The age of audit data, in days, that the audit data must be equal to or older than to be deleted by this tool. **Default:** 400
age.in.days. to.purge. subscription	The amount of time, in days, a subscription has been in a canceled, expired, failed, or retired state before it is deleted by this tool. **Default:** 400

Example `config.properties` content

Oracle (TLS not enabled)

```
jdbc.driverClassName=oracle.jdbc.driver.OracleDriver
jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE
jdbc.username=csa
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.OracleDialect
idmConfig.Url=https://127.0.0.1:8444
securityTransportUserName=csaTransportUser
securityTransport.password=ENC(rlbE8430uFSDljert85441e7fe70ljkY)
securityIdmTransportUserName=idmTransportUser
securityIdmTransport.password=ENC(lDdh98Kfe76op8lhjE0El897klRCB532lsb)
age.in.days.to.purge.audit=400
age.in.days.to.purge.subscription=400
```

MS SQL (TLS not enabled)

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request
jdbc.username=csa
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
idmConfig.Url=https://127.0.0.1:8444
securityTransportUserName=csaTransportUser
securityTransport.password=ENC(rlbE8430uFSDljert85441e7fe70ljkY)
securityIdmTransportUserName=idmTransportUser
securityIdmTransport.password=ENC(lDdh98Kfe76op8lhjE0El897klRCB532lsb)
age.in.days.to.purge.audit=400
age.in.days.to.purge.subscription=400
```

MS SQL (TLS enabled)

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/
 example;ssl=authenticate
jdbc.username=csa
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
```

PostgreSQL

```
jdbc.driverClassName=org.postgresql.Driver
jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/csadb
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect
idmConfig.Url=https://127.0.0.1:8444
securityTransportUserName=csaTransportUser
securityTransport.password=ENC(rlbE8430uFSDljert85441e7fe70ljkY)
securityIdmTransportUserName=idmTransportUser
securityIdmTransport.password=ENC(lDdh98Kfe76op8lhjE0El897klRCB532lsb)
age.in.days.to.purge.audit=400
age.in.days.to.purge.subscription=400
```

4. Run the following command to delete subscriptions and audit data (you can specify options to delete only subscriptions or only audit data):

> **Caution:** THE PURGE TOOL RUNS WITHOUT PROMPTING FOR A CONFIRMATION.
>
> Deleted subscriptions and audit data cannot be restored unless you have backed up the database.
>
> Verify that you have entered the correct information into the `config.properties` file before running this tool.

> **Note:** When running the tool to delete subscriptions or audit data, you will be prompted for a username and password. This user MUST be assigned to the CSA Administrator role. Users who are not assigned to this role cannot delete subscriptions nor audit data.

Oracle (TLS not enabled)

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -j ojdbc6.jar
```

where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool` and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA does not check the database DN, client authentication is enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java
-Djavax.net.ssl.keyStore="<certificate_key_file>"
-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>
-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>
-jar db-purge-tool.jar -j ojdbc6.jar
```

where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool`, `certificate_key_file` is the same keystore file defined by the certificate-key-file attribute in the ssl element of the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file (for example, `$CSA_HOME/jboss-as/standalone/configuration/.keystore`), `certificate_key_file_password` is the password to the keystore file (for example, changeit), `certificate_key_file_type` is the keystore type (for example, JKS or PKCS12), and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA does not check the database DN, client authentication is NOT enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -j ojdbc6.jar
```

where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool` and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA checks the database DN, client authentication is enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java
-Doracle.net.ssl_server_dn_match=true
-Djavax.net.ssl.keyStore="<certificate_key_file>"
-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>
-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>
-jar db-purge-tool.jar -j ojdbc6.jar
```

where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool`, `certificate_key_file` is the same keystore file defined by the certificate-key-file attribute in the ssl element of the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file (for example, `$CSA_HOME/jboss-as/standalone/configuration/.keystore`), `certificate_key_file_password` is the password to the keystore file (for example, changeit), `certificate_key_file_type` is the keystore type (for example, JKS or PKCS12), and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA checks the database DN, client authentication is NOT enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java
-Doracle.net.ssl_server_dn_match=true -jar db-purge-tool.jar -j ojdbc6.jar
```

where `ojdbc6.jar` is the name of the Oracle JDBC driver installed in `$CSA_HOME/Tools/db-purge-tool` and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

MS SQL and PostgreSQL

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar
```

where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

The following options are available in the purge tool

Option	Description
-jar db-purge-tool.jar	Required. The name of the tool to run.
-a, --audit	Optional. Purge audit data. If neither -a nor -s are specified, the tool purges both audit data and subscriptions. **Note:** When running the tool to delete subscriptions or audit data, you will be prompted for a username and password. This user MUST be assigned to the CSA Administrator role. Users who are not assigned to this role cannot delete subscriptions nor audit data.
-c <*config_properties*>, --config <*config_properties*>	Optional. The name and location of the configuration properties file. By default, the tool looks for the configuration properties file in the working directory (the directory from which the tool is run). If this option is not specified, the tool looks for the `config.properties` in the working directory. The examples in this document assume the file is located in the working directory and is named `config.properties`.
-g, --generate	Optional. Generate example configuration properties files for supported databases.
-h, --help	Optional. List the options available in this tool.
-j <*jdbc_drivers*>, --jars <*jdbc_drivers*>	Optional. The name and location of the JDBC driver(s) to be used by this tool. If more than one driver needs to be specified, separate each driver by a space. By default, the tool looks for the JDBC driver(s) in the working directory (the directory from which the tool is run). If you are not running the tool from `$CSA_HOME/Tools/db-purge-tool`, specify the name and location of the JDBC driver(s) to be used. For a list of supported JDBC driver versions, refer to the *HP Cloud Service Automation System and Software Support Matrix*, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Option	Description
-s, --subscription	Optional. Purge subscription data. If neither -s nor -a are specified, the tool purges both subscriptions and audit data. **Note:** When running the tool to delete subscriptions or audit data, you will be prompted for a username and password. This user MUST be assigned to the CSA Administrator role. Users who are not assigned to this role cannot delete subscriptions nor audit data.

Examples for Oracle (TLS is not Enabled)

Display the purge tool help:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -h -j ojdbc6.jar
```

Generate sample configuration properties files:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -g -j ojdbc6.jar
```

Purge subscriptions and associated entities:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -s  -j ojdbc6.jar
```

Purge audit data: `$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -a  -j ojdbc6.jar`

Purge subscriptions and associated entities and audit data:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar  -j ojdbc6.jar
```

Examples for MS SQL and PostgreSQL

Display the purge tool help: `$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -h`

Generate sample configuration properties files:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -g
```

Purge subscriptions and associated entities:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -s
```

Purge audit data: `$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar -a`

Purge subscriptions and associated entities and audit data:

```
$CSA_JRE_HOME/bin/java  -jar db-purge-tool.jar
```

Install the HP CSA Database Schema

The schema installation tool is used to upgrade the existing HP CSA database schema or install a fresh database schema without re-installing HP CSA. Use this tool if you did not install HP CSA database components onto the database during installation, did not upgrade the database schema during an upgrade, or if you want to drop the existing schema and install a fresh HP CSA database schema. You can also use this tool to complete an upgrade if the upgrade failed, the database schema was not updated, the failure was not due to a database problem, and the problem can be fixed without rerunning the upgrade installer. For example, if the upgrade failed but can be completed successfully by manual configuration but the database schema was not updated, you can simply make the manual changes to complete the upgrade and run the schema installation tool instead of reverting HP CSA back to the previous version and running the upgrade installer again.

Note: Do not run this tool if you installed the database components during the installation of HP CSA or if you upgraded the database schema when you upgraded HP CSA.

If you run this tool on an existing schema (where HP CSA has been upgraded but the database schema was not upgraded), the schema is upgraded and no data in the database is lost. However, if you drop the existing schema and run this tool, all data in the database associated with the dropped schema is lost. Once you run the tool, a fresh schema is installed and you cannot revert back to the dropped schema.

Caution: Once you drop an existing schema and run the database schema installation tool, you cannot revert back to the dropped schema.

Upgrading or Installing the Database Schema

To upgrade or install a fresh HP CSA database schema, do the following:

1. If HP CSA is running, stop HP CSA.

   To stop HP CSA, on the server that hosts HP Cloud Service Automation, type the following:

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

   If you installed an embedded HP Operations Orchestration instance, type `<embeddedHPOOinstallation>/central/bin/central stop`.

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

2. Change to the `$CSA_HOME/Tools/SchemaInstallationTool/` directory where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

3. During upgrade or installation of HP CSA, a file named `db.properties` was generated in `$CSA_HOME/Tools/SchemaInstallationTool/`. Verify the property values in this file. If you changed any database property values in the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file after installation, the values in `db.properties` may not be up-to-date.

If you have dropped the existing database schema and are installing a fresh database schema after upgrading to HP CSA 4.50, you must update the `driverFiles` property value. The properties defined in `db.properties` are described in the table.

Property Name	Description

dbUrl	The JDBC URL. When specifying an IPv6 address, it must be enclosed in square brackets (see examples below).
	Examples
	Oracle (TLS not enabled):
	`jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE`
	Oracle (TLS not enabled, using an IPv6 address):
	`jdbc.databaseUrl=jdbc:oracle:thin:@//[f000:253c::9c10:b4b4]:1521/XE`
	Oracle (TLS enabled, HP CSA does not check the database DN):
	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL)))` where `<host>` is the name of the system on which the Oracle database server is installed.
	Oracle (TLS enabled, HP CSA checks the database DN):
	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN= "CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))` where `<host>` is the name of the system on which the Oracle database server is installed and the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server.
	MS SQL (TLS not enabled):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request`
	MS SQL (TLS not enabled, using an IPv6 address):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://[::1]:1433/example;ssl=request`
	MS SQL (TLS enabled):
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate`
	PostgreSQL:
	`jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/csadb`

Property Name	Description
dbUserName	The user name of the database user you configured for HP Cloud Service Automation after installing the database.
dbPassword	The password for the database user. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. While you may enter a password in clear text, after you run the tool, the clear text password is automatically replaced by an encrypted password. **Example** `dbPassword=ENC(fc5e38d38a5703285441e7fe7010b0)`

Property Name	Description

driverFiles	The database driver files used by this tool. If you are running a fresh installation of HP CSA 4.50 (you did not upgrade to HP CSA 4.50), you do not need to change these values.
	If you have upgraded to HP CSA 4.50 and want to upgrade the existing schema, you do not need to change these values.
	If you have upgraded to HP CSA 4.50, have dropped the existing database schema, and are installing a fresh database schema, you must update this value to the following:
	Oracle (upgrade and dropped schema only)
	`driverFiles=$CSA_HOME/scripts/schemainstallforupg/create-oracle-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/create-oracle-topology-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/oracle/seed_data_driver.sql,`
	`%CSA_HOME%/scripts/reporting/oracle/install_views_driver.sql,`
	`%CSA_HOME%/scripts/reporting/oracle/grant-reporting-user.sql`
	PostgreSQL (upgrade and dropped schema only)
	`driverFiles=$CSA_HOME/scripts/schemainstallforupg/create-postgres-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/create-postgres-topology-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/postgres/seed_data_driver.sql,`
	`%CSA_HOME%/scripts/reporting/postgres/install_views_driver.sql,`
	`%CSA_HOME%/scripts/reporting/postgres/grant-reporting-user.sql`
	Microsoft SQL (upgrade and dropped schema only)
	`driverFiles=$CSA_HOME/scripts/schemainstallforupg/alterdb.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/create-mssql-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/create-mssql-topology-schema.sql,`
	`$CSA_HOME/scripts/schemainstallforupg/mssql/seed_data_driver.sqll,`

Property Name	Description
	%CSA_HOME%/scripts/reporting/mssql/ install_views_driver.sql, %CSA_HOME%/scripts/reporting/mssql/ grant-reporting-user.sql **Note:** Add the `grant-reporting-user.sql` file only if you have created the reporting database user for HP CSA.
jdbcDriverClassName	The JDBC driver class. Do not change this value. **Examples** Oracle: `jdbc.driverClassName=oracle.jdbc.driver.OracleDriver` MS SQL: `jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver` PostgreSQL: `jdbc.driverClassName=org.postgresql.Driver`
jdbcDriverDir	The location of the JDBC driver(s) used by this tool. Do not change this value.

4. Run the following command:

   Oracle (TLS not enabled), MS SQL, and PostgreSQL

   ```
   $CSA_JRE_HOME/bin/java -jar schema-installation-tool.jar
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

   Oracle (TLS enabled, HP CSA does not check the database DN, client authentication is enabled on the Oracle database server)

   ```
   $CSA_JRE_HOME/bin/java -Djavax.net.ssl.keyStore="<certificate_key_file>"
   -Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>
   -Djavax.net.ssl.keyStoreType=<certificate_key_file_type>
   -jar schema-installation-tool.jar
   ```

   where `certificate_key_file` is the same keystore file defined by the certificate-key-file attribute in the ssl element of the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file (for example, `$CSA_HOME/jboss-as/standalone/configuration/.keystore`), `certificate_key_file_password` is the password to the keystore file (for example, changeit), `certificate_key_file_type` is the keystore type (for example, JKS or PKCS12) and `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

   Oracle (TLS enabled, HP CSA does not check the database DN, client authentication is NOT enabled on the Oracle database server)

   ```
   $CSA_JRE_HOME/bin/java -jar schema-installation-tool.jar
   ```

where $CSA_JRE_HOME is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA checks the database DN, client authentication is enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java -Doracle.net.ssl_server_dn_match=true
-Djavax.net.ssl.keyStore="<certificate_key_file>"
-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>
-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>
-jar schema-installation-tool.jar
```

where certificate_key_file is the same keystore file defined by the certificate-key-file attribute in the ssl element of the $CSA_HOME/jboss-as/standalone/configuration/standalone.xml file (for example, $CSA_HOME/jboss-as/standalone/configuration/.keystore), certificate_key_file_password is the password to the keystore file (for example, changeit), certificate_key_file_type is the keystore type (for example, JKS or PKCS12), and $CSA_JRE_HOME is the directory in which the JRE that is used by HP CSA is installed.

Oracle (TLS enabled, HP CSA checks the database DN, client authentication is NOT enabled on the Oracle database server)

```
$CSA_JRE_HOME/bin/java -Doracle.net.ssl_server_dn_match=true
-jar schema-installation-tool.jar
```

where $CSA_JRE_HOME is the directory in which the JRE that is used by HP CSA is installed.

Configure HP CSA to Mitigate Frequently Dropped Database Connections

If you are experiencing frequently dropped database connections, configure the JBoss data source connections to mitigate the problem.

In a standalone environment, do the following:

1. Stop the HP Cloud Service Automation service.

   From a command prompt, type `service csa stop`.

2. Edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone.xml` file:

   a. Find the `dataSource` tag which is used for HP CSA database configuration.

   b. Add the following after the line that ends with `</security>`:

      Oracle

```
<validation>
<check-valid-connection-sql>select 1 from DUAL</check-valid-connection-sql>
<validate-on-match>false</validate-on-match>
</validation>
```

MS SQL or PostgreSQL

```
<validation>
<check-valid-connection-sql>select 1</check-valid-connection-sql>
<validate-on-match>false</validate-on-match>
</validation>
```

3. Start the HP Cloud Service Automation service.

   From a command prompt, type `service csa start`.

In a clustered environment, do the following:

1. Stop the HP Cloud Service Automation service.

   From a command prompt, type `service csa stop`.

2. Edit the `$CSA_HOME/jboss-as/standalone/configuration/standalone-full-ha.xml` file:

   a. Find the `dataSource` tag which is used for HP CSA database configuration.

   b. Add the following after the line that ends with `</security>`:

   Oracle

   ```
   <validation>
   <check-valid-connection-sql>select 1 from DUAL</check-valid-connection-sql>
   <validate-on-match>false</validate-on-match>
   </validation>
   ```

   MS SQL or PostgreSQL

   ```
   <validation>
   <check-valid-connection-sql>select 1</check-valid-connection-sql>
   <validate-on-match>false</validate-on-match>
   </validation>
   ```

3. Start the HP Cloud Service Automation service.

   From a command prompt, type `service csa start`.

Appendix A: Cloud Service Management Console Properties

This section lists and describes the properties that can be configured for the Cloud Service Management Console, which are located in one of the following files:

- `$CSA_HOME/jboss-as/standalone/deployments/csa.war/`
  `WEB-INF/classes/csa.properties`

- `$CSA_HOME/jboss-as/standalone/deployments/csa.war/`
  `WEB-INF/web.xml`

where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

The following areas contain properties that can be configured (for many properties, default values are provided):

- Authentication
- Security Banner
- Marketplace Portal URL
- Security
- HP Cloud Service Automation keystore
- Service request processor scheduler
- Auditing
- Process execution manager
- Lifecycle engine
- Approval engine scheduler
- LDAP cache scheduler
- Clustering
- Dynamic property
- HP CDA integration
- Marketplace Portal

- Common access card
- Single sign-on
- HP Single Sign-On
- Process executor delegate
- Miscellaneous
- HP Operations Orchestration
- HP CSA 3.x API authentication
- Topology designer
- Elasticsearch
- Microservices
- Secure connections
- LDAP access point
- Service design, service offering, and catalog content archive verification
- HP ITOC Integration
- Session timeout

For information about HP Codar properties, please refer to the HP Codar documentation.

After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Authentication

These properties are used for authentication.

These properties are configured in `csa.properties`.

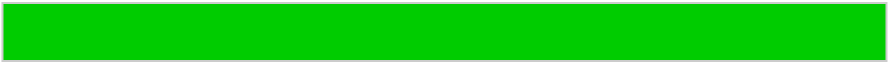
Property	Description
csa.provider.hostname	Required. The fully-qualified domain name of the system on which HP Cloud Service Automation is running. If you change this hostname, you must update the value of the `idm.csa.hostname` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file.
csa.provider.port	Required. The port used to connect to the system on which HP Cloud Service Automation is running. If you change this port, you must update the value of the `idm.csa.port` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file.
csa.provider.rest.protocol	Required. The protocol used by the REST API to connect to the system on which HP Cloud Service Automation is running. This attribute must be set to **https**. If you change this protocol, you must update the value of the `idm.csa.protocol` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file.
csa.orgName.identifier	Required. The provider organization identifier assigned to the organization who is providing this instance of the Cloud Service Management Console. This attribute must be set to **CSA-Provider**.

Security Banner Attributes

The attributes in the following table are used by the Cloud Service Management Console to enable or disable the display of a disclaimer upon logging in to the Cloud Service Management Console and a color-coded banner that appears at the top and bottom of the Cloud Service Management Console.

These properties are configured in `csa.properties`.

Attribute	Description
csa.provider.agency	By default, this attribute is commented out. When this attribute is commented out or does not contain a valid value, the login disclaimer and color-coded banners are not displayed for the Cloud Service Management Console. If you want to enable the login disclaimer and color-coded banners, uncomment this attribute and set the value to **GOVERNMENT**. If set to any other value, the login disclaimer and color-coded banners are not displayed. To edit the disclaimer page, edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/static/template/disclaimerNote.jsp` file. To edit the disclaimer content, edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/msgs/messages_en.properties` file. To locate the disclaimer content in this file, search for message property entries beginning with `csa.security.warning`.

Attribute	Description
csa.provider. contentType	By default, this attribute is commented out. This attribute defines the color and content that displays in the security banner. The security banners appear at the top and bottom of the Cloud Service Management Console. The following values are provided out-of-the-box: • UNCLASSIFIED. The banner is light green and contains no content. An example is shown below.  • UNCLASSIFIED_FOUO. For official use only. The banner is light green and displays the text "FOUO." An example is shown below. • UNCLASSIFIED_NOFORN. Not releasable to foreign nationals. The banner is light green and displays the text "NOFORN." An example is shown below. • CONFIDENTIAL. The banner is light blue and displays the text "CONFIDENTIAL." An example is shown below. • CONFIDENTIAL_FOUO. The banner is light blue and displays the text "CONFIDENTIAL-FOUO." An example is shown below. • CONFIDENTIAL_NOFORN. The banner is light blue and displays the text "CONFIDENTIAL-NOFORN." An example is shown below. • SECRET. The banner is red and displays the text "SECRET." An example is shown below. • TOPSECRET. The banner is orange and displays the text "TOPSECRET." An example is shown below. To edit the banner content, edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/msgs/messages_en.properties` file. To locate the banner content in this file, search for message property entries beginning with `csa.security.label`.

Marketplace Portal URL

This property is used to define the URL of the Marketplace Portal for an organization and is displayed in the Cloud Service Management Console.

This property is configured in `csa.properties`.

Property	Description
csa.subscriber.portal.url	The URL used to access the Marketplace Portal of an organization and is displayed in the Organization URL field in the General Information section of an organization's page in the Cloud Service Management Console. You can use specific values or one or more of the following variables: • {protocol} - The protocol used to connect to the Marketplace Portal. This is either http or https. The variable value is the same protocol used to access the Cloud Service Management Console. • {host} - The fully-qualified domain name or IP address of the system on which the Marketplace Portal is installed. The variable value is the same host on which the Cloud Service Management Console is installed. • {orgName} - The organization's name. The variable value is the Organization Identifier displayed in the General Information section of an organization's page. The Organization Identifier is based on the value entered in the Organization Display Name field. The port configured for the Marketplace Portal in this property should match the `port` attribute value configured in the `$CSA_HOME/portal/conf/mpp.json` file. If a variable's value is incorrect, you can enter a specific value in place of the variable. For example, **`https`**`://{host}:8089/org/{orgName}` or `{protocol}://`**`csa_system.xyz.com`**`:8089/#/login/`**`marketing`** Default: {protocol}://{host}:8089/org/{orgName}

Security

These properties are used to configure encrypted passwords, an encrypted signing key, files that can/cannot be uploaded to the Cloud Service Management Console, and the maximum size of files that can be uploaded to the Cloud Service Management Console.

These properties are configured in `csa.properties`.

Property	Description
securityAdminPassword	Required. The encrypted password used by the out-of-the-box `admin` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file). The admin user account is used for initial login to the Cloud Service Management Console and can also be used to authenticate REST API calls. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update the password of any REST API calls that use this password. For more information about the REST APIs, refer to the *HP Cloud Service Automation API Quick Start Guide* and *HP Cloud Service Automation API Reference Guide*.

Property	Description
securityCsaReporting UserPassword	Required. The encrypted password used by the out-of-the-box `csaReportingUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file). The csaReportingUser user account is used when a subscription is ordered or modified and a field for the subscription includes a dynamically generated list. The dynamically generated list is a subscriber option property configured to use a dynamic query. The dynamic query uses this account to access HP Cloud Service Automation to determine the values that will appear in the list. This account has read-only access to HP Cloud Service Automation. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update the password of any REST API calls that use this password. For more information about the REST APIs, refer to the *HP Cloud Service Automation API Quick Start Guide* and *HP Cloud Service Automation API Reference Guide*.
securityTransport UserName	Required. The out-of-the-box user used to authenticate REST API calls between the Marketplace Portal and Cloud Service Management Console (it should not be used to log in to the Cloud Service Management Console). If you change this username, you must update the value of the `idm.csa.username` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. For more information about the integration user account, see "Change HP CSA Out-of-the-Box User Accounts" on page 137. For more information about the REST APIs, refer to the *HP Cloud Service Automation API Quick Start Guide* and *HP Cloud Service Automation API Reference Guide*.

Property	Description
securityTransportPassword	Required. The encrypted password used by the out-of-the-box `csaTransportUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file). The csaTransportUser user account is used to authenticate REST API calls between the Marketplace Portal and Cloud Service Management Console (it should not be used to log in to the Cloud Service Management Console). The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must update the value of the `idm.csa.password` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. For more information about the integration user account, see "Change HP CSA Out-of-the-Box User Accounts" on page 137. For more information about the REST APIs, refer to the *HP Cloud Service Automation API Quick Start Guide* and *HP Cloud Service Automation API Reference Guide*.
securityOoInbound UserPassword	Required. The encrypted password used by the out-of-the-box `ooInboundUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file). The ooInboundUser user account is used by HP Operations Orchestration to authenticate REST API calls with HP Cloud Service Automation (it should not be used to log in to the Cloud Service Management Console). The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update and use the same password for the CSA_REST_CREDENTIALS system account in HP Operations Orchestration (located in the Configuration folder of the Public Repository).

Property	Description
securityCdaInbound UserPassword	Required. The encrypted password used by the out-of-the-box `cdaInboundUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/csa-provider-users.properties` file). The `cdaInboundUser` user account is used by HP CDA to authenticate REST API calls with HP Cloud Service Automation (it should not be used to log in to the Cloud Service Management Console). The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update and use the same password in HP CDA. For more information about this user account, see "Change HP CSA Out-of-the-Box User Accounts" on page 137.
securityIdmTransport UserPassword	Required. The encrypted password used by the out-of-the-box `idmTransportUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file). The `idmTransportUser` user account is used to authenticate REST API calls (it should not be used to log in to the Cloud Service Management Console). The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update the following passwords (you must use the same password): • the `idmTransportUser` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/classes/integrationusers.properties` file. • the `password` attribute in the idmProvider section of the `$CSA_HOME/portal/conf/mpp.json` file (this password uses a different password encryption utility; see "Encrypt a Marketplace Portal Password" on page 136 for more information about encrypting the `password` attribute). • the password of any REST API calls that use this password. For more information about this user account, see "Change HP CSA Out-of-the-Box User Accounts" on page 137.

Property	Description
securityCatalog AggregationTransport UserPassword	Required. The encrypted password used by the out-of-the-box `csaCatalogAggregationTransportUser` user (defined in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml` file). The csaCatalogAggregationTransportUser user account is used to authenticate catalog aggregation REST API calls with HP Cloud Service Automation (it should not be used to log in to the Cloud Service Management Console). The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. If you change this password, you must also update the password using the catalog aggregation registration REST APIs. For more information about this user account, see "Change HP CSA Out-of-the-Box User Accounts" on page 137.
securityEncrypted SigningKey	HP CSA's encrypted signing key used to encrypt and decrypt authentication data passed between HP CSA and the HP Identity Management component. If you change this key, you must also update the `idm.encryptedSigningKey` property in the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. The key should be encrypted (see "Encrypt a Password" on page 130 for instructions on how to encrypt this key). The encrypted key is preceded by `ENC` without any separating spaces and is enclosed in parentheses.
com.hp.ccue.consumption disallowedExtensions	A comma-delimited list of the file extensions that designate the types of documents or files that cannot be uploaded to the Cloud Service Management Console. Default: exe,bat,com,cmd

Property	Description
csa.additionalSupportedExtensionsForImport	A comma-delimited list of the file extensions that designate the types of documents or files that can be uploaded to the Cloud Service Management Console. The file extensions listed can be the sole extension of the file or the start of the file extension followed by one or more characters. For example, listing `txt` as a file extension will match both `mydocument.txt` and `mydocument.txt_3491767613`. Files can be uploaded using the Cloud Service Management Console, the content archive tool, or the import API. Refer to the HP Cloud Service Management Console Help, *HP Cloud Service Automation API Reference Guide*, or *HP Cloud Service Automation Content Archive Tool* for more information about using these features. The following extensions are automatically supported (and do not need to be defined by this property): jpg, jpeg, jpe, jfif, svg, tif, tiff, ras, cmx, ico, pnm, pbm, pgm, ppm, rgb, xbm, xpm, xwd, png, gif, bmp, cod, ief, json, xml, jsp, jspf. Default: (no default defined) Example: txt,log
csa.maxFileUploadSize	The maximum size of a file, in megabytes (MB), that can be uploaded to the HP CSA system using the Cloud Service Management Console. If this property is not listed or is not set in the `csa.properties` file, the default maximum size of 50 MB is used. Default: 50 (MB)

HP Cloud Service Automation Keystore

These properties are used to configure information about HP Cloud Service Automation's keystore.

These properties are configured in `csa.properties`.

Property	Description
csaTruststore	Required. The HP Cloud Service Automation keystore that stores trusted Certificate Authority certificates. Default: No default specified **Example** `/usr/local/hp/csa/openjre/lib/security/cacerts` **Note:** Use only forward slashes (/) as your path separators.
csaTruststorePassword	Required. The encrypted password of the HP Cloud Service Automation keystore (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Default: ENC(<*encrypted_value*>) where the default value of <*encrypted_value*> is the encrypted value of "changeit".

Service Request Processor Scheduler

These properties are used to configure the service request processor scheduler. The service request processor scheduler validates a consumer's requests, initiates the approval process, if configured, and maintains a request's status.

These properties are configured in `csa.properties`.

Property	Description
serviceRequestProcessorScheduler.maxInstancesToProcess	Optional. The maximum number of service requests the service request processor can process when it checks the start and end dates of submitted subscriptions. Default: 100
serviceRequestProcessorScheduler.period	Optional. How often, in milliseconds, the service request processor checks the start and end dates of submitted subscriptions. Default: 5000 (5 seconds)

Auditing

These properties are used to configure auditing.

These properties are configured in `csa.properties`.

Property	Description
csaAuditEnabled	Optional. Enable or disable auditing, which tracks user activities and system-generated events. Messages are logged to the `CSA_AUDIT_EVENT` table in the database. Default: true (enabled)
jboss.shutdown.log.location	Required. This property is set during installation and *must not be changed*. The location of the JBoss log file that records when the HP CSA service was stopped. Used for auditing purposes. Default: `$CSA_HOME/jboss-as/bin/shutdown.log` **Note:** Use only forward slashes (/) as your path separators.

Property	Description
csa.origin.ip.header	Optional. Defines a custom HTTP header used to capture the originating IP address of a REST API call. If this property is disabled (commented out) or not set to a value, the standard HTTP header X-Forwarded-For is used to capture the originating IP address. If the originating IP address is not captured by either this custom or the standard header, HP CSA fetches the originating IP address from the incoming request. The originating IP address is used for auditing. HP CSA sets the following precedence when capturing the originating IP address of a REST API call: 1. Uses the custom HTTP header (if defined) 2. Uses the X-Forwarded-For header 3. Fetches from the incoming request If this property is set to a custom HTTP header, HP CSA checks if this custom HTTP header is defined (set to the originating IP address) in the REST API call. If this property is not set or if the custom header is not defined, HP CSA checks if the X-Forwarded-For header is defined in the REST API call. If the X-Forwarded-For header is not defined, HP CSA fetches the originating IP address from the incoming request. HP CSA does not validate the captured value (if the value is an IP address and if it is a valid IP address). The following is a list of HP CSA REST API types and which ones do and do not capture the originating IP address: • Legacy HP CSA 3.x APIs: originating IP address IS CAPTURED • Consumer (Consumption) APIs that include onBehalf parameter in the Response Content Type (i.e. Consumer APIs that use the POST, PUT, or DELETE methods): originating IP address IS CAPTURED • Consumer (Consumption) APIs that do not include onBehalf parameter in the Response Content Type (i.e. Consumer APIs that use the GET method): originating IP address IS NOT CAPTURED • Management (Consumption) APIs: originating IP address IS NOT CAPTURED The originating IP address is stored in the ORIGIN_IP field of the RPT_AUDIT_EVENT_V view and the ORIGIN_IP column of the CSA_AUDIT_EVENT table. If the originating IP address is not captured, the field or column is empty. Default: (disabled)

Process Execution Manager

These properties are used to configure the process execution manager. The process execution manager starts internal actions and HP Operations Orchestration flow actions, checks the status of process instances, and performs callback once the actions are completed.

These properties are configured in `csa.properties`.

Property	Description
com.hp.csa.ProcessExecutor.THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the process execution manager starts new process instances (which start HP Operations Orchestration flows) and checks the status of process instances. Default: 5000 (5 seconds)
com.hp.csa.ProcessExecutor.THREAD_POOL_CORE_SIZE	Optional. The maximum number of threads used to run process instances. Default: 2
com.hp.csa.PEM.PARAM_PROCESS_INSTANCE_ID	Optional. The token that stores the process instance ID and is used when HP Cloud Service Automation starts an HP Operations Orchestration flow. Default: CSA_PROCESS_ID
com.hp.csa.PEM.PARAM_CONTEXT_ID	Optional. The token that stores the artifact ID of the artifact that owns the action that executes the HP Operations Orchestration flow. Default: CSA_CONTEXT_ID

Lifecycle Engine

These properties are used to configure the lifecycle engine. The lifecycle engine processes service instances and executes lifecycle actions.

These properties are configured in `csa.properties`.

Property	Description
com.hp.csa.LifecycleExecutor.THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the lifecycle engine checks for service components that it needs to transition. Default: 5000 (5 seconds)
com.hp.csa.LifecycleExecutor.THREAD_POOL_SIZE	Optional. The maximum number of threads used to transition service components. Default: 2

Approval Engine Scheduler

These properties are used to configure the approval engine scheduler. The approval engine scheduler checks each approver's response to a pending approval process to see if the process can be marked as completed and updates the decision and status of an approval process, as needed.

This property is configured in `csa.properties`.

Property	Description
com.hp.csa.ApprovalDecisionMaker.THREAD_POOL_SIZE	Optional. The maximum number of threads used to process approvals. Default: 4
com.hp.csa.ApprovalDecisionMaker.THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the approval engine scheduler checks for completion of an approval process to determine if an approval process should be approved or denied. Default: 5000 (5 seconds)

LDAP Cache Scheduler

These properties are used to configure the LDAP cache scheduler. The LDAP cache scheduler checks the age of the user group cache and deletes it if it has expired.

For users who can log in to the Cloud Service Management Console or Marketplace Portal, certain actions require authorization (verification if the user belongs to a group). When authorization is requested for a user, HP CSA checks for group membership by using the cache. If the cache does not exist, LDAP is queried for the user's user groups which are temporarily cached to the database. After a configured expiration time, the cache is deleted. During a single session, the cache may be deleted and refreshed as needed.

These properties are configured in `csa.properties`.

Property	Description
com.hp.csa.UserGroupExecutor.THREAD_WAKEUP_TIME	Optional. How often, in minutes, the LDAP cache scheduler checks for user group caches that have expired. This number should be less than the value configured for `com.hp.csa.UserGroupExecutor.CACHE_EXPIRATION_TIME`. Default: 20
com.hp.csa.UserGroupExecutor.CACHE_EXPIRATION_TIME	Optional. How long, in minutes, LDAP user groups for a user are temporarily cached in the database before they are deleted. This time should be greater than the value configured for `com.hp.csa.UserGroupExecutor.THREAD_WAKEUP_TIME`. Default: 30
com.hp.csa.UserGroupExecutor.UserGroupDeletionBatchSize	Optional. The maximum number of user IDs that are deleted in a single batch from the cache. This number cannot be larger than 1,000. Default: 250

Clustering

This property is used to configure clustering.

This property is configured in `csa.properties`.

Property	Description
deploymentMode	Required. The mode in which HP CSA is running (single or clustered). When set to `single`, HP CSA runs in standalone mode (on a single instance) and all HP CSA services are run on this instance. When set to `clustered`, HP CSA runs in a clustered environment and all HP CSA services run on only one node (which is selected by the cluster as the singleton-service provider). Default: single

Dynamic Property

These configuration properties are used to limit the amount of time to retrieve data and the amount of data retrieved when using a dynamic property. A dynamic property is a Dynamic Query value entry method for a subscriber option property that defines what information is retrieved. A dynamic property allows the Service Designer to list a dynamic set of values that change based on the user context (for example, the organization to which the user belongs).

These properties are configured in `csa.properties`.

Property	Description
DynamicPropertyFetch.READ_TIMEOUT	Optional. How long, in milliseconds, HP Cloud Service Automation attempts to fetch or retrieve data for dynamic properties. Default: 30000 (30 seconds)
DynamicPropertyFetch.RESPONSE_SIZE	Optional. The maximum amount of data, in bytes, that can be retrieved for dynamic properties. Default: 50000

Group Approval

This configuration property is used when configuring a group approval template.

This property is configured in `csa.properties`.

Property	Description
csa.group.numberOfApprovers	Optional. The maximum number of members in an LDAP group used for approvals. For reasonable performance, do not specify more than ten (10) members. Default: 10

HP CDA Integration

This configuration property is used when integrating with HP Continuous Delivery Automation (HP CDA).

This property is configured in `csa.properties`.

Property	Description
defaultDaysToExtendExpirationDate	Optional. How long, in days, HP Cloud Service Automation automatically extends an expired subscription if the subscription is based on HP CDA designs and other services depend on this subscription. If a subscription is based on HP CDA designs and other services depend on the HP Cloud Service Automation service subscription, this subscription cannot be canceled. Default: 1

Marketplace Portal

These properties are the default values displayed in the Cloud Service Management Console that are used to configure the Marketplace Portal for an organization. The values configured in the Cloud Service Management Console take precedence over the values set in this properties file.

These properties are configured in `csa.properties`.

Property	Description
csa.consumer. featuredCategory	Optional. The default value of the Featured Category field displayed in the Cloud Service Management Console of a selected organization. This value may be overwritten in the Cloud Service Management Console. The value configured in the Cloud Service Management Console takes precedence over this value. This is the category that is used when displaying service offerings in the Marketplace Portal. The value entered for this attribute is the name of a category configured in the Cloud Service Management Console but is in all capitalized letters and replaces any spaces with an underscore (_). For example, if you configure a category named **e-mail Servers** and want to feature this category, you would set this attribute to **E-MAIL_SERVERS**. • ACCESSORY • APPLICATION_SERVERS - Default. • APPLICATION_SERVICES • BACKUP_SERVICES • CRM • DATABASE_SERVERS • FILE_SERVERS • HARDWARE • MAIL_SERVICES • NETWORK_SERVICES • PLATFORM_SERVICES • SIMPLE_SYSTEM • SOFTWARE • WEB_HOSTING_SERVICES For more information about the featured services, refer to the *Marketplace Portal Help*. Default: APPLICATION_SERVERS

Property	Description
csa.consumer. endDatePeriod	Optional. The default value of the Subscription End Date field displayed in the Cloud Service Management Console of a selected organization. This value may be overwritten in the Cloud Service Management Console by a lower value. The value configured in the Cloud Service Management Console takes precedence over this value. This is the maximum length of a subscription, in months, if a requested end date is specified. When a subscriber selects a requested start date and requests an end date, the length of the subscription cannot be longer than the value of this property. The maximum allowed value is 12 months. For example, if the subscriber selects a requested start date of June 15, 2015, based on the default value of this property, the requested end date cannot be later than June 14, 2016. If **no end date** is selected, this value is ignored. Default: 12 (months)
csa.consumer. legalNoticeUrl	Optional. The default value of the Privacy Statement Link field displayed in the Cloud Service Management Console of a selected organization. This value may be overwritten in the Cloud Service Management Console. The value configured in the Cloud Service Management Console takes precedence over this value. This is a link to an organization's privacy statement and, when enabled in the Cloud Service Management Console, appears on the login page below the copyright statement. Default: HP's online privacy statement
csa.consumer. termsOfUseUrl	Optional. The default value of the Terms and Conditions Link field displayed in the Cloud Service Management Console of a selected organization. This value may be overwritten in the Cloud Service Management Console. The value configured in the Cloud Service Management Console takes precedence over this value. This is a link to an organization's terms and conditions statement and, when enabled in the Cloud Service Management Console, appears when a subscriber is ordering a service. Default: HP's terms of use statement

Common Access Card

This property is used to enable integration between Common Access Card (CAC) and HP CSA.

This property is configured in `csa.properties`.

Property	Description
enableCAC	Optional. Enable integration between CAC and HP CSA, where the CAC is used as an approval mechanism. To enable, this property must be uncommented and set to true. To disable, either comment out the property or set it to false. Default: (disabled)

Single Sign-On

This property is used to enable integration between CA SiteMinder and HP CSA.

This property is configured in `csa.properties`.

Property	Description
enableSSO	Optional. Enable integration between CA SiteMinder and HP CSA, where the SiteMinder is used for single sign-on. To enable, this property must be uncommented and set to true. To disable, either comment out the property or set it to false. Default: (disabled)

HP Single Sign-On

This property is used to enable integration between HP Single Sign-On (HP SSO) and the Cloud Service Management Console. HP SSO can be used when launching an application, such as HP IT Business Analytics, from the Cloud Service Management Console.

This property is configured in `csa.properties`.

Property	Description
enableHPSSO	Optional. Enable integration between HP SSO and the Cloud Service Management Console. To enable, this property must be uncommented and set to true. To disable, either comment out the property or set it to false. This property is automatically set during installation.

Process Executor Delegate

These properties are used to configure the process executor delegate. The process executor delegate handles processing of the process instances. It discovers the ready instances, submits them to different thread pools for processing based on process definition and model type (sequenced or topology).

These properties are configured in `csa.properties`.

Property	Description
com.hp.csa.service.process. ProcessExecutorDelegate. INTERNAL_POOL_SIZE	Optional. The maximum number of threads used for processing internal executors (for example, clone patterns). Default: 2
com.hp.csa.service.process. ProcessExecutorDelegate. EXTERNAL_POOL_SIZE	Optional. The maximum number of threads used for processing external executors (for example, HP Operations Orchestration). Default: 2
com.hp.csa.service.process. ProcessExecutorDelegate. CALLBACK_POOL_SIZE	Optional. The maximum number of threads used by the callback pool. Default: 2
com.hp.csa.service.process. ProcessExecutorDelegate. MONITOR_POOL_SIZE	Optional. The maximum number of threads used by the monitor pool. Default: 2

Miscellaneous

The following are miscellaneous properties that do not fall under any specific category.

These properties are configured in `csa.properties`.

Property	Description
com.hp.csa.aosMonitor. THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the background thread monitors plug-in processes. Default: 20000
com.hp.csa.TimeoutChecker. THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the background thread monitors for processes that have timed out. Default: 300000

HP Operations Orchestration

These properties are used to integrate with HP Operations Orchestration.

These properties are configured in `csa.properties`.

The following properties configure the interaction between the Cloud Service Management Console and HP Operations Orchestration. In the subscription event overview section of the **Operations** area in the Cloud Service Management Console, selecting the Process ID opens HP Operations Orchestration to the detailed page of the selected process when these properties are configured.

Property	Description
OOS_URL	The URL used to access HP Operations Orchestration Central. This is the HP Operations Orchestration used for provisioning topology designs. For example, `https://`*`<hostname>`*`:8445`. This property is automatically set during installation. If you are using the embedded HP Operations Orchestration that is included with HP CSA, this property is set using the values entered for the **Fully Qualified Hostname** and **HP OO Port** fields during installation. If you are using a standalone/external HP Operations Orchestration, this property is set using the values entered for the **HP OO Hostname** and **HP OO Port** fields during installation.
OOS_USERNAME	The username used to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO User** field during installation.
OOS_PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO Password** field during installation.

The following properties configure background services to monitor HP Operations Orchestration.

Property	Description
com.hp.csa.oo.OOClient.SOCKET_TIMEOUT	Optional. How long, in milliseconds, HP CSA keeps a socket open for SOAP-based communication with HP Operations Orchestration. Default: 60000

Property	Description
com.hp.csa.OosMonitor.THREAD_WAKEUP_TIME	Optional. How often, in milliseconds, the background thread monitors HP Operations Orchestration processes. Default: 60000
com.hp.csa.service.process.OosMonitorDelegate.MONITOR_POOL_SIZE	Optional. The maximum number of threads used by the monitor pool. Default: 2
OOS_MASTER_OOFLOW_CONTENT_LOCATION	The location in HP Operations Orchestration where HP CSA generates topology design-based master HP Operations Orchestration flows and related subflows. The folder structure must use forward slashes. Default: Library/CSA/Topology_Generated_Flows

HP CSA 3.x API Authentication

These properties are used to configure authentication for the HP CSA 3.x API.

These properties are configured in `csa.properties`.

Property	Description
xAuthToken	Optional. An optional token in the Authorization header used for HTTP basic authentication by the HP CSA 3.x API. If the token is sent, it is used to authenticate the userIdentifier parameter in the REST API. For more information about the HP CSA API, refer to the *HP Cloud Service Automation API Quick Start Guide*. Default: X-Auth-Token

Property	Description
integrationAccountUserList	Required. A comma-delimited list of users who are authorized to exercise the HP CSA 3.x API. The username in the Authorization header used for HTTP basic authentication must match one of the users in this list. By default, the following HP CSA out-of-the-box users are configured: admin, csaCatalogAggregationTransportUser, csaReportingUser, csaTransportUser, ooInboundUser, and cdaInboundUser. You can also add LDAP users (identified by the User ID) to this list. For example, if you use email addresses for the User ID, you could add `user1@xyz.com` to the list. For more information about the HP CSA API, refer to the *HP Cloud Service Automation API Quick Start Guide*. Default: admin,csaReportingUser,ooInboundUser, cdaInboundUser,csaTransportUser, csaCatalogAggregationTransportUser

Topology Designer

These properties are used to configure the features of topology designs.

These properties are configured in `csa.properties`.

Property	Description
TopologyDesignProvisioning. TIMEOUT	Optional. The amount of time, in seconds, HP CSA attempts to provision or de-provision a topology design (topology design provisioning and de-provisioning is orchestrated by interacting with resource providers corresponding to the components used in the design). If the time is exceeded, in the Operations area of the Cloud Service Management Console, the subscription (to a service offering that is created from a topology design) will show a Subscription Status of `Failed` and a Service Instance Status of `Failed`. If you select the Events tab of the subscription, the event will show a Status of `Timeout`. If you select the Topology tab of the subscription, the topology view will show the status of the components in the service instance as their respective status just before the timeout occurred. HP recommends that this value is set to the same value as the HP Operations Orchestration flow timeout value. Default: 7200 (2 hours)
OrchestratedTopologyDesignProvisioning. ProviderSelection.Enabled	Optional. Enable or disable resource environment and provider selection by the subscriber in the Marketplace Portal for service offerings based on topology designs. For more information, refer to the *HP Cloud Service Management Console Help*. Default: true (enabled)

Elasticsearch

These properties are used to integrate global search with HP CSA.

These properties are configured in `csa.properties`.

Property	Description
csa.provider.es.exists	Required. Enable or disable the global search feature on this HP CSA node. If enabled, additional microservice properties may be configured. To enable the global search feature, set this property to **yes**. Default: no (disabled)
csa.provider.es.authUser	Required if `csa.provider.es.exists` is enabled (set to yes). The user used by the Elasticsearch service to authenticate requests coming from HP CSA. HP recommends creating a user specifically for this purpose. If the out-of-the-box consumer user is disabled or another user is used, either another out-of-the-box user or LDAP user must be configured. If using an out-of-the-box user, this user must have the SERVICE_CONSUMER role configured. If using an LDAP user, this user must be assigned to the Service Consumer role. Default: consumer
csa.provider.es.authPassword	Required if `csa.provider.es.exists` is enabled (set to yes). The encrypted password of the `csa.provider.es.authUser` user. The password should be encrypted (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Default: *<encrypted password of the consumer user>*

Property	Description
csa.provider.es.authOrganization	Required if `csa.provider.es.exists` is enabled (set to yes). The name of the organization to which the `csa.provider.es.authUser` user belongs. The organization is used only for authentication purposes. The Elasticsearch service will index the service offerings, service instances, or subscriptions for all organizations. However, global search results for a Marketplace Portal user will be limited to the service offerings, service instances, or subscriptions of the organization to which the user belongs and to which the user has access. If the out-of-the-box CSA_CONSUMER organization is disabled or removed, the `csa.provider.es.authUser`, `csa.provider.es.authPassword`, and `csa.provider.es.authOrganization` properties must be updated to use a valid user and organization. Default: CSA_CONSUMER
csa.provider.es.idmURL	Required if `csa.provider.es.exists` is enabled (set to yes). The URL used to generate Identity Management component tokens for Elasticsearch service authentication. If an HP CSA cluster is configured for high availability using a load balancer, `localhost` must be changed to the hostname or IP address of the system on which the load balancer is running. Default: https://localhost:8444/idm-service

Microservices

These properties are used to configure the HP Search Service, which creates the indices for Elasticsearch. The Elasticsearch property, `csa.provider.es.exists`, must be enabled for these properties to take effect.

These properties are configured in `csa.properties`.

Property	Description
csa.provider.msvc.hostname	Required if `csa.provider.es.exists` is enabled (set to yes). The fully-qualified domain name of the system on which the HP Search Service is running or localhost. Default: localhost

Property	Description
csa.provider.msvc.port	Required if `csa.provider.es.exists` is enabled (set to yes). The port used to connect to the system on which the HP Search Service is running. Default: 9000
csa.provider.msvc.rest.protocol	Required if `csa.provider.es.exists` is enabled (set to yes). The protocol used by the REST API to connect to the system on which the HP Search Service is running. Default: https

Secure Connections

This property is used to configure if certificate validation, hostname verification, and certificate authentication are performed when secure connections are established with HP CSA.

This property is configured in `csa.properties`.

Property	Description
com.hp.csa.service.ssl.certificate.validation	Required. Determines if certificate validation, hostname verification, and certificate authentication are performed by HP CSA when making a secure connection (only using HTTPS) with an application or a component of HP CSA. Examples of an application include HP Operations Orchestration or a resource provider. Examples of a component of HP CSA include the Marketplace Portal and the Identity Management component. Other non-HTTP connections that have been configured to be secure are not affected by this property. For example, secure connections to the database, LDAP server, or SMTP server are not affected. **Note:** If HP CSA is running in a FIPS-compliant environment, this property is not used. In a FIPS-compliant environment, certificate validation, hostname verification, and certificate authentication will always be performed when making a secure connection with HP CSA. By default, this property is set to false. That is, when HP CSA establishes a secure connection with another application or component, the connection will only be encrypted. No validation, verification, or authentication is performed. This mode should only be used during post-installation configuration or when troubleshooting problems with certificates. This mode should NOT be used in a production environment. When set to true, when HP CSA establishes a secure connection with another application or component, the following occurs: • The connection will be encrypted • Certificate validation - Checks that the certificate used by the application/component has not expired • Hostname verification - Checks that the certificate hostname matches the URL hostname of the application/component to which HP CSA is connecting • Certificate authentication - Checks that the certificate or the root certificate used to sign the certificate has been imported into HP CSA's JRE truststore (for example, `$CSA_JRE_HOME/lib/security/cacerts`) Default: false

LDAP Access Point

This property is used to enable or disable access to the LDAP access point configuration in the Cloud Service Management Console.

This property is configured in `csa.properties`.

Property	Description
csa.ldapReadOnly	Required. Enable or disable access to the LDAP access point configuration in the Cloud Service Management Console. By default, the property is set to false and the CSA administrator can configure the LDAP access point of any organization from the Cloud Service Management Console (the LDAP access point is typically configured when an organization is created in the Cloud Service Management Console). LDAP configuration includes fields for the LDAP Server Information, LDAP Attributes, and User Login Information in the Cloud Service Management Console. The LDAP access point is used by HP CSA for authentication and authorization. For security reasons, you may not want to allow the CSA administrator to configure the LDAP access point from the Cloud Service Management Console. You can disable access to the LDAP access point fields for all organizations from the Cloud Service Management Console by setting this property to true (disabling access makes the LDAP configuration fields read-only in the Cloud Service Management Console). By disabling this access, only the system administrator or other privileged users on the HP CSA system can update the LDAP access point using the LDAP Configuration Tool. Refer to the *LDAP Configuration Tool* guide for more information about the LDAP Configuration Tool. To enable access to the LDAP access point configuration in the Cloud Service Management Console, set this property to false. To disable access to the LDAP access point configuration in the Cloud Service Management Console, set this property to true. Default: false

Service Design, Service Offering, and Catalog Content Archive Verification

This property is used to enable or disable service design, service offering, and catalog content archive verification.

This property is configured in `csa.properties`.

Property	Description
csa.security.enable	Required. Enable or disable service design, service offering, and catalog content archive verification. By default, the property is set to false (verification is disabled), allowing the Cloud Service Management Console or Content Archive Tool to import a service design, service offering, or catalog content archive directly without verification. When the property is set to true (verification is enabled), HP CSA verifies the digital signature of the content archive, validates the date of the certificate used to sign the content archive, and verifies that the content in the content archive has not been modified after it was signed. If the content archive fails one of these validation or verification checks, the content archive will not be imported into HP CSA. When enabled, all imported service design, service offering, or catalog content archives must be signed. Refer to "Signing the Content Archive" on page 124 for the steps required to sign a content archive. **Note:** Verifying service designs and catalogs before they are imported is done using the Cloud Service Management Console or the Content Archive Tool. Verifying service offerings before they are imported is done using the Content Archive Tool. **Caution:** Verification cannot be enabled for importing a service design, service offering, or catalog content archive using the REST APIs. A service design, service offering, or catalog content archive imported using the REST APIs will always be imported directly. Verification can only be enabled for the Cloud Service Management Console or the Content Archive Tool. Default: false

HP ITOC Integration

These properties are used to enable integration between HP CSA and HP IT Operations Compliance (ITOC).

This property is configured in `csa.properties`.

Property	Description
csa.ITOC.Integration.enabled	Optional. Enable or disable integration between HP CSA and HP ITOC. To enable, this property must be uncommented and set to true. To disable, either comment out the property or set it to false. Default: (disabled)
csa.ITOC.Notification.BaseUri	Required if integration between HP CSA and HP ITOC is enabled. To enable, this property must be uncommented and set to the endpoint of the HP ITOC instance. The endpoint is the URL for connecting to the HP ITOC instance where <*protocol*> is the protocol used to communicate with the HP ITOC instance (for example, http or https), <*itoc_host*> is the hostname of the HP ITOC instance, and <*port*> is the port used to connect to the system on which HP ITOC is running. Default: (disabled)
csa.ITOC.Notification.username	Required if integration between HP CSA and HP ITOC is enabled. To enable, this property must be uncommented and set to the username used to log in to the HP ITOC instance. Default: (disabled)
csa.ITOC.Notification.password	Required if integration between HP CSA and HP ITOC is enabled. To enable, this property must be uncommented and set to the encrypted password used by the user defined in `csa.ITOC.Notification.username` to log in to the HP ITOC instance (see "Encrypt a Password" on page 130 for instructions on encrypting passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Default: (disabled)
csa.ITOC.Notification.tenant	Required if integration between HP CSA and HP ITOC is enabled. To enable, this property must be uncommented and set to the tenant group to which the user defined in `csa.ITOC.Notification.username` belongs. Default: (disabled)

Session Timeout

This property is used to configure the Cloud Service Management Console session.

This property is configured in `web.xml`.

Property	Description
session-timeout	Optional. The amount of inactivity, in minutes, that causes the Cloud Service Management Console session to time out. Default: 60

Restart the HP Cloud Service Automation Service

After modifying the `csa.properties` file, restart HP CSA. See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Appendix B: Marketplace Portal Attributes

This section lists and describes the attributes that can be configured for the Marketplace Portal. Recommended modifications to the values can be found in the related feature's section in this guide or other documentation (for example, refer to the Identity Management component section in this guide for more information about the Identity Management component-related attributes).

The attributes are located in the following file:

```
$CSA_HOME/portal/conf/mpp.json
```

where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

The following areas contain attributes that can be configured (for many attributes, default values are provided):

- General Marketplace Portal attributes
- Shopping cart attributes
- Provider attributes
- Identity Management component attributes
- Secure connection attributes
- High availability attributes
- Logging attributes
- Proxy server attributes

General Marketplace Portal Attributes

These attributes are general purpose attributes that can be configured for the Marketplace Portal.

Attribute	Description
uid	A unique identifier of the Marketplace Portal process used only on Linux systems. Default: ccue_mpp

Attribute	Description
port	The port used to connect to the system on which the Marketplace Portal is running. The port configured for the Marketplace Portal in this attribute should match the port value configured for the `csa.subscriber.portal.url` property in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file. Default: 8089
defaultOrganizationName	The organization identifier of the organization that is accessed by the Marketplace Portal when the Marketplace Portal is launched from a URL that does not specify the organization. The organization identifier is the unique name that HP Cloud Service Automation assigns to the organization, based on the organization display name (the organization identifier can be found in the General Information section of the **Organizations** tile of the Cloud Service Management Console). Default: CSA_CONSUMER
defaultHelpLocale	The language in which the online help is presented. Available languages can be found in the `$CSA_HOME/portal/node_modules/mpp-ui/dist/ccue-marketplaceportal-help/help/<defaultHelpLocale>` directory. Default: en_US (English)
defaultHelpPage	The name of the help file that is launched if there is no context-sensitive help available for a topic. The page is relative to `$CSA_HOME/portal/node_modules/mpp-ui/dist/ccue-marketplaceportal-help/help/<defaultHelpLocale>` and uses the defaultHelpLocale to determine which language to use. Default: MarketplacePortal_Help_CSA.htm
keyfile	The file that contains the Marketplace Portal's encrypted symmetric key and is used by the Marketplace Portal to encrypt and decrypt data in the Marketplace Portal. The path to the file can be absolute or relative to the `$CSA_HOME/portal/bin` directory. If this file does not exist, it can be generated using the `$CSA_HOME/portal/bin/passwordUtil` utility (see "Encrypt a Marketplace Portal Password" on page 136 for more information). Default: ../conf/keyfile

Attribute	Description
rejectUnauthorized	Allows the Marketplace Portal to accept or reject requests based on the type of certificate passed. If enabled (set to true), the Marketplace Portal will only accept requests that use a Certificate Authority-signed or subordinate Certificate Authority-signed certificate and it will reject requests that use a self-signed certificate. If disabled (set to false), the Marketplace Portal will accept requests that use a Certificate Authority-signed, subordinate Certificate Authority-signed certificate, or a self-signed certificate. Default: false
session: cookieSecret	The authentication cookie used to verify if a user is logged in and to encrypt the user's identification. The cookie/password should be encrypted (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.
session: timeoutDuration	The amount of inactivity, in seconds, that causes the Marketplace Portal session to time out. Default: 1800 (30 minutes)
session: cleanupInterval	How often, in seconds, a background process is run to clean up expired sessions. Default: 3600 (1 hour)

Shopping Cart Attributes

These attributes are used to configure the shopping cart for the Marketplace Portal.

Attribute	Description
thresholdQuantity	The minimum number of items in a shopping cart that, upon submission, may delay response time of the submission. Default: 20
maximumQuantity	The maximum number of items in a shopping cart that can be submitted. Default: 100

Provider Attributes

These attributes are used to configure how the Marketplace Portal interacts with HP CSA.

Attribute	Description
url	The URL to access HP CSA. Default: https://localhost:8444
contextPath	The context path to access HP CSA. Default: /csa/api/mpp
strictSSL	When enabled, when the Marketplace Portal establishes a secure connection to HP CSA, the following occurs: • The connection will be encrypted • Certificate validation - Checks that the certificate used by HP CSA has not expired • Hostname verification - Checks that the certificate hostname matches the URL hostname of the HP CSA system to which the Marketplace Portal is connecting • Certificate authentication - Checks that the certificate or the root certificate used to sign the certificate is listed in the file defined by the `ca` attribute When enabled, if the hostname configured for the certificate is not valid, access is denied to the Marketplace Portal. To check if this is causing access problems to the Marketplace Portal, look for the following error message in the `$CSA_HOME/portal/logs/mpp.log` file: `ERROR GetPost : java.security.cert.CertificateException: No name matching <csa.provider.hostname> found` When disabled, when the Marketplace Portal establishes a secure connection to HP CSA, the connection will be encrypted. Certificate validation, hostname verification, and certificate authentication do not occur. Default: true (enabled)
secureProtocol	Used for FIPS 140-2 compliance. Determines the connection method used and understood by the server. Default: TLSv1_method

Attribute	Description
ca	Used only when `strictSSL` is enabled. The path to and name of the file that is an actual certificate or contains a comma-delimited list of certificates for HP CSA, which may include Certificate Authority-signed and self-signed certificates. If you are using a self-signed certificate, it must be listed in this file. The path to the file can be absolute or relative to the `$CSA_HOME/portal/bin` directory. The certificates must be in a PEM or DER format. To use the self-signed certificate generated during the installation of HP CSA, set this attribute's value to `$CSA_HOME/jboss-as/standalone/configuration/jboss.crt` where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

Identity Management Component Attributes

These attributes are used to configure how the Marketplace Portal interacts with the Identity Management component.

Attribute	Description
url	The URL to access the Identity Management component. Default: https://localhost:8444
returnUrl	If proxy configuration is enabled, this is the URL to which the Identity Management component is redirected after authentication has succeeded. Default: https://localhost:8089
contextPath	The context path to access the Identity Management component. Default: /idm-service
username	The name of the account used by HP CSA to authenticate REST API calls. Default: idmTransportUser
password	The encrypted password for the `username` (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. See "Change HP CSA Out-of-the-Box User Accounts" on page 137 for more information about this account.

Attribute	Description
strictSSL	When enabled, when the Marketplace Portal establishes a secure connection to the Identity Management component, the following occurs: • The connection will be encrypted • Certificate validation - Checks that the certificate used by the Identity Management component has not expired • Hostname verification - Checks that the certificate hostname matches the URL hostname of the Identity Management component system to which the Marketplace Portal is connecting • Certificate authentication - Checks that the certificate or the root certificate used to sign the certificate is listed in the file defined by the `ca` attribute When enabled, if the hostname configured for the certificate is not valid, access is denied to the Marketplace Portal. To check if this is causing access problems to the Marketplace Portal, look for the following error message in the `$CSA_HOME/portal/logs/mpp.log` file: `ERROR GetPost : java.security.cert.CertificateException: No name matching <csa.provider.hostname> found` When disabled, when the Marketplace Portal establishes a secure connection to the Identity Management component, the connection will be encrypted. Certificate validation, hostname verification, and certificate authentication do not occur. Default: true (enabled)
secureProtocol	Used for FIPS 140-2 compliance. Determines the connection method used and understood by the server. Default: TLSv1_method
ca	Used only when `strictSSL` is enabled. The path to and name of the file that is an actual certificate or contains a comma-delimited list of certificates for the Identity Management component, which may include Certificate Authority-signed and self-signed certificates. If you are using a self-signed certificate, it must be listed in this file. The path to the file can be absolute or relative to the `$CSA_HOME/portal/bin` directory. The certificates must be in a PEM or DER format. To use the self-signed certificate generated during the installation of HP CSA, set this attribute's value to `$CSA_HOME/jboss-as/standalone/configuration/jboss.crt` where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed.

Secure Connection Attributes

These attributes are used to configure a secure connection for the Marketplace Portal.

Attribute	Description
enabled	Determines the protocol used by the Marketplace Portal. If enabled (set to true), the Marketplace Portal uses the HTTPS protocol. If disabled (set to false), the Marketplace Portal uses the HTTP protocol. The options listed below are used only when this attribute is enabled. Additional options may be specified and are defined at http://nodejs.org/api/tls.html#tls_tls_createserver_options_secureconnectionlistener. Default: true
options: pfx	The file that contains the Marketplace Portal's private key, self-signed certificate, and Certificate Authority-signed certificates (also known as a PKCS #12 archive). The path to the file can be absolute or relative to the `$CSA_HOME/portal/bin` directory. Default: ../conf/.mpp_keystore
options: passphrase	The encrypted password used to access the `pfx` (see "Encrypt a Marketplace Portal Password" on page 136 for instructions on encrypting Marketplace Portal passwords). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.
options: secureProtocol	Used for FIPS 140-2 compliance. Determines the connection method used and understood by the server. Default: TLSv1_method

High Availability Attributes

These attributes are used to configure the Marketplace Portal in a clustered environment. For more information on how to configure HP CSA in a clustered environment, (which disables these attributes), refer to the *Configuring an HP CSA Cluster for High Availability Using an Apache Web Server* or *Configuring an HP CSACluster for High Availability Using a Load Balancer* guides.

Attribute	Description
enabled	Determines the environment in which the Marketplace Portal is running. If enabled (set to true), the Marketplace Portal is running in a clustered environment. If disabled (set to false), the Marketplace Portal is running in a standalone environment. Default: false

Attribute	Description
numWorkers	The number of workers on which to deploy the Marketplace Portal. Each worker is deployed on each CPU and is therefore bound by the number of CPUs on the host. Default: 2
redis: options: host	The hostname of the system on which the Redis data structure server is running. Default: localhost
redis: options: port	The port to connect to the Redis data structure server. Default: 6379

Logging Attributes

These attributes are used to configure logging.

Attribute	Description
console: enabled	Determines if messages are written to the console. If enabled (set to true), messages are displayed in the console. If disabled (set to false), messages are not displayed in the console. Default: false
console: level	The level of logging. For example, error, warn, info, debug, or trace. Default: info
file: enabled	Determines if messages are written to a log file. If enabled (set to true), messages are logged to a file (`$CSA_HOME/portal/logs/mpp.log`). If disabled (set to false), messages are not logged to a file. Default: true
file: level	The level of logging. For example, error, warn, info, debug, or trace. Default: info
file: maxSizeMB	The maximum size to which the log file can grow, in megabytes, before it is archived. Default: 10
file: maxFile	The maximum number of archived log files. Default: 10

Attribute	Description
cef: enabled	If the Marketplace Portal logging has been integrated with ArcSight Logger, determines if log events are sent and stored in ArcSight Logger. If enabled (set to true), log events are sent and stored in ArcSight Logger. If disabled (set to false), log events are not sent and stored in ArcSight Logger. For information on HP CSA and ArcSight Logger integration, see the *Integration with ArcSight Logger* technical white paper. Default: false
cef: host	The hostname of the system on which the ArcSight Logger is installed. Default: localhost
cef: port	The port used to connect to the system on which the ArcSight Logger is installed. Default: 9876
cef: level	The level of logging. For example, error, warn, info, or debug. Default: warn

Proxy Attributes

These attributes are used to configure proxy settings for the Marketplace Portal.

Attribute	Description
enabled	Determines if a proxy (an alternate URL using a different port and context path) is used to access the Marketplace Portal (for example, you may need to use a proxy, such as `http://localhost:8090/mpp` instead of `http://localhost:8089`, when the Marketplace Portal is integrated with a single sign-on solution). If enabled (set to true), the Marketplace Portal uses a proxy. If enabled, you must update the `returnUrl` attribute to use the proxy for the Identity Management component (this attribute is also located in the `mpp.json` file). If disabled (set to false), the Marketplace Portal does not use a proxy. Default: false
port	The port used for proxying. Default: 8090
contextPath	The mount path to which the Marketplace Portal is forwarded. Default: /mpp

Appendix C: HP Operations Orchestration Settings

This section is provided as a reference only.

The following areas contain settings that can be configured from HP Operations Orchestration Studio:

- Remote Action Services
- System Accounts
- System Properties

Remote Action Services

Setting	Description
RAS_ Operator_ Path	Required. The name and URL that accesses the RAS used by HP Operations Orchestration Central. HP recommends the following value: `https://<FQDN>:9004/RAS/services/RCAgentService` where *<FQDN>* is the fully qualified domain name or IP address of the HP Operations Orchestration host. Do not use localhost in the URL. Using localhost does not work correctly even though it appears to work when you run HP Operations Orchestration Studio on the same machine as the RAS. RAS must be run on the same system as HP Operations Orchestration Studio. Running HP Operations Orchestration Studio on another machine produces errors and turns flows red with a cryptic error message about result assignments to result variables that do not exist.

System Accounts

Setting	Description
CSA_REST_ CREDENTIALS	Required. Credentials for HP CSA REST authentication. HP recommends the Credentials are set to the following values: • **User Name**: ooInboundUser • **Password**: cloud **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Property Value** (HP Operations Orchestration version 9.07) or **Override Value** (HP Operations Orchestration version 10.21.0001) configured for the CSA_OO_USER System Property setting.

System Properties

Setting	Description
CSA_DMA_WorkflowTimeout	Required. The amount of time, in seconds, to wait for a DMA workflow to complete. Default Property Value: 3600
CSA_NA_CreateVlanScript	Required. The name of the HP Network Automation command script to create a VLAN that was imported when you integrated HP Network Automation with HP CSA. Default Property Value: HPN Create Vlan
CSA_NA_DeleteVlanScript	Required. The name of the HP Network Automation command script to delete a VLAN that was imported when you integrated HP Network Automation with HP CSA. Default Property Value: HPN Delete Vlan

System Properties, continued

Setting	Description
CSA_OO_USER	Required. The user that communicates with HP CSA using the REST API. Default Property Value: ooInboundUser **Note:** The **Property Value** (HP Operations Orchestration version 9.07) or **Override Value** (HP Operations Orchestration version 10.21.0001) configured for the CSA_OO_USER System Property setting must match the **User Name** configured for the CSA_REST_CREDENTIALS System Account setting.
CSA_REST_URI	Required. The URI used to communicate with HP Cloud Service Automation using the REST API. HP recommends the following Property Value: `https://<csa_hostname>:8444/csa/rest`
CSA_SiteScope_MonitoringLockId	Required. HP SiteScope monitoring lock ID. Default Property Value: SiteScope Lock for Deploying Monitors
CSA_SiteScope_RootMonitorGroup	Required. The default name of the HP SiteScope root monitor group path. Default Property Value: CSA Monitors
CSA_SiteScope_MonitoringSleepTime	Required. The amount of time, in seconds, to wait before acquiring the HP SiteScope monitoring lock. This time may be increased if there are a large number of subscription requests. Default Property Value: 30
CSA_vCenterPropertyCollectionTimeout	Required. How often, in seconds, properties are collected about a deployed virtual machine. Default Property Value: 1800

Appendix D: Identity Management Configuration

If you are using the Identity Management component, the identity service and its components require configuration. Because it is a Spring Framework application, most of its configuration is defined in the `applicationContext.xml` file, although key attributes are externalized to the `applicationContext.properties` file. Both files are in `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/`.

You should make most common configuration changes to the `applicationContext.properties` file. To avoid service disruptions, only advanced users who understand the Spring Framework should change the `applicationContext.xml` file.

You must also configure the Java Relying Party Library.

Note: You should always make a copy of a configuration file before editing it.

External Configuration

Selected settings are pulled from the `applicationContext.properties` file, which you can override by an external properties file set as a JVM argument: `-Didm.properties="<`*`external_properties_filename`*`>"`. You can add this JVM argument to the `JAVA_OPTS` environment variable or by editing the `standalone.conf` file in `$CSA_HOME/jboss-as/bin/` to add it to `JAVA_OPTS` for the HP CSA JBoss container.

The table below describes the properties that are set in the properties file. These properties are required (although if you set the `idm.keystone.enabled` property to `false`, all other `idm.keystone*` properties in this table are ignored).

If you are integrating with Keystone, the `idm.keystone*` properties must match the Keystone network location, transport user credentials, and so on. All `idm.csa*` properties and all `ConvergedLdapAuthConfig` properties (which are listed in the *ConvergedLdapAuthConfig* section below) must match the HP CSA network location and transport user credentials.

Property Name	Description
`idm.ssl.requireValidCertificate`	Flag indicating whether valid certificates are required: `true` or `false`
`idm.csa.protocol`	The protocol used to access the HP CSA instance: `http` or `https`
`idm.csa.hostname`	The hostname or IP address of the HP CSA server
`idm.csa.port`	The port number used by the HP CSA server
`idm.csa.username`	The username for the HP CSA integration account

Property Name	Description
idm.csa.password	The password for the HP CSA integration account. For improved security, this value should be encrypted.
idm.encryptedSigningKey	The shared signing key for all token factory objects. For improved security, this value should be encrypted.
idm.keystone.enabled	Flag indicating whether secondary authentication through Keystone is enabled: true or false
idm.keystone.required	Flag indicating whether successful secondary authentication through Keystone is required for authentication to succeed: true or false
idm.keystone.protocol	The protocol used to access the Keystone instance: http or https
idm.keystone.hostname	The hostname or IP address of the Keystone server
idm.keystone.port	The port number used by the Keystone server. Typically 5000.
idm.keystone.servicePath	The service path where the Keystone service listens. The typical value is v3.
idm.keystone.domainName	The OpenStack domain name to use for all authentication on the Keystone server. The typical value is Default.
idm.keystone.transportUsername	The username for the integration account used to communicate with Keystone and perform OpenStack operations.
idm.keystone.transportPassword	The password for the integration account used to communicate with Keystone and perform OpenStack operations. For improved security, this value should be encrypted.
idm.keystone.transportProject	The Keystone project name for the integration account. All Keystone users must belong to a project whose name exactly matches the HP CSA organization ID used to log in — including case (for example, a Keystone project name of project_name will not match an HP CSA organization ID of PROJECT_NAME.

Configure Seeded Authentication

The top-level configuration file for seeded authentication is specified by the configFile property of the SeededAuthenticationProvider bean defined in the applicationContext.xml configuration file. In the default configuration, this file is seededorgs.properties, but it can be changed. Each line in this file contains a key-value pair. The key is an HP CSA organization ID, and the value is the name of another properties file that contains the users for that organization. By default, the following organizations are configured to use the specified files.

Organization	User File
CSA_CONSUMER	csa-consumer-users.properties

You can define additional organizations or change the user file associated with any organization. Each line in each user file contains a key-value pair. The key is the username, and the value is a comma-separated list of the password, granted authorities, and an optional flag indicating whether the account is enabled. For improved security, the *entire* value should be encrypted. Following is an example of a line from a user file that defines a user named consumer with the password cloud and granted the SERVICE_CONSUMER and ROLE_REST authorities.

```
consumer=cloud,SERVICE_CONSUMER,ROLE_REST,enabled
```

Configure the Java Relying Party Library

The Java Relying Party Library is a set of classes provided by the identity service that abstract and simplify invoking the service from Java applications, such as HP CSA. You modify the properties listed in this section in the $CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml file. The tokenFactory property value should be the same for all AuthenticationProvider beans (listed in the *Internal Configuration* section below) in the identity service and in the Java Relying Party library.

IdentityServiceConfig

Configures the connection to the identity service.

Class: com.hp.ccue.identity.rp.IdentityServiceConfig

Property Name	Description
protocol	The protocol (http or https) to use to connect to the identity service
hostname	The hostname or IP address of the server running the identity service
port	The port number where the identity service is running, typically 8444
servicePath	The path on the server to the identity service, typically idm-service

IdentityAuthenticationProvider

Abstracts the invocation of the identity service to perform authentication.

Class: com.hp.ccue.identity.rp.IdentityAuthenticationProvider

Property Name	Description
`templateFactory`	Creates the `RestTemplate` object that facilitates performing REST calls
`configuration`	Network configuration of the identity service to connect to perform authentication: an `IdentityServiceConfig` object
`tokenFactory`	The token factory to validate returned tokens
`tenantHeaderName`	The name of the HTTP header where the tenant name is passed. The default is `HP-Tenant-Name`

HeaderAuthenticationProvider

Performs authentication based on a token passed in an HTTP header.

Class: `com.hp.ccue.identity.rp.HeaderAuthenticationProvider`

Property Name	Description
`headerName`	The name of the HTTP header where the token is transferred
`tokenValidator`	The `TokenValidator` object to use to validate tokens

Internal Configuration

The `applicationContext.xml` file defines the configuration of the classes in the identity service. The `tokenFactory` property value should be the same for all `AuthenticationProvider` beans (listed in the sections below) in the identity service and in the Java Relying Party library.

> **Note:** Modify this file only if you cannot express the necessary configuration change in the `applicationContext.properties` file. The `applicationContext.xml` file must follow the syntax rules specified by the Spring Framework. In the following tables, the default values are used if no values are provided in the configuration file. You can configure items marked as externalized in the `applicationContext.properties` file.

JwtTokenFactory

Defines how tokens are created.

Class: `com.hp.ccue.identity.domain.JwtTokenFactory`

Property Name	Description
lifetimeMinutes	Required. The lifetime of the token, in minutes. The lifetime as installed is 30 minutes. Reducing this value will render tokens invalid faster and thus requires a more-frequent token refresh, which might reduce performance. Increasing this value allows tokens to last longer, which might allow someone who has intercepted a valid token to access the system for a period of time. Default value: (None) Externalized: No
defaultTypeName	Optional. Default type of JWT token to create: `PLAINTEXT`, `SIGNED`, or `ENCRYPTED` Default value: `PLAINTEXT` Externalized: No
signingKey	Required if `defaultTypeName` is set to `SIGNED`. This is a Base64-encoded byte array representing the key used to sign signed tokens. If `defaultTypeName` is set to `SIGNED`, this value must be the same for all components that validate tokens. For improved security, this item should be encrypted. Default value: (None) Externalized: `idm.encryptedSigningKey`
refreshEnabled	Optional. Boolean value indicating whether token refresh is enabled: `true` or `false`. The recommended value is `true`. Default value: `true` Externalized: No

ConvergedLdapAuthConfig

Defines the configuration for connecting to an HP CSA server to get LDAP configuration information. The `idm.csa*` external properties (which are listed in the *External Configuration* section above) and all `ConvergedLdapAuthConfig` properties must match the HP CSA network location and transport user credentials.

Class: `com.hp.ccue.identity.ldap.ConvergedLdapAuthConfig`

Property Name	Description
providerProtocol	Required if using ActiveDirectory or LDAP. `http` or `https`, depending on the protocol used by the HP CSA instance Default value: (None) Externalized: `idm.csa.protocol`

Property Name	Description
`providerHostname`	Required if using ActiveDirectory or LDAP. Hostname or IP address of the HP CSA server Default value: (None) Externalized: `idm.csa.hostname`
`providerPort`	Required if using ActiveDirectory or LDAP. Port number used by the HP CSA server Default value: (None) Externalized: `idm.csa.port`
`securityTransportUsername`	Required if using ActiveDirectory or LDAP. Username for the HP CSA integration account Default value: (None) Externalized: `idm.csa.username`
`securityTransportPassword`	Required if using ActiveDirectory or LDAP. Password for the HP CSA integration account Default value: (None) Externalized: `idm.csa.password`

ConvergedActiveDirectoryAuthenticationProvider and ConvergedLdapAuthenticationProvider

Performs authentication with Active Directory and LDAP authentication mechanisms.

Class: `com.hp.ccue.identity.ldap.ConvergedActiveDirectoryAuthenticationProvider`, `com.hp.ccue.identity.ldap.ConvergedLdapAuthenticationProvider`

Property Name	Description
`config`	Required if using ActiveDirectory or LDAP. The `ConvergedLdapAuthConfig` that represents the HP CSA server to use to get the LDAP configuration for each organization Default value: (None) Externalized: No

Property Name	Description
`tokenFactory`	Required if using ActiveDirectory or LDAP. The token factory for creating identity tokens in response to successful authentications Default value: (None) Externalized: No

SeededAuthenticationProvider

Performs seeded authentication.

Class: `com.hp.ccue.identity.seeded.SeededAuthenticationProvider`

Property Name	Description
`configFile`	Required if using seeded authentication. Typically `seededorgs.properties`, which is the file that defines the seeded organizations Default value: (None) Externalized: No
`tokenFactory`	Required if using seeded authentication. The token factory for creating identity tokens in response to successful authentications Default value: (None) Externalized: No

IdentityAuthenticationProvider

Performs integration account authentication.

Class: `com.hp.ccue.identity.seeded.IntegrationAuthenticationProvider`

Property Name	Description
`configFile`	Required. Typically `integrationusers.properties`, which is the file that defines the seeded organizations Default value: (None) Externalized: No

Property Name	Description
`tokenFactory`	Required. The token factory for creating identity tokens in response to successful authentications Default value: (None) Externalized: No

MultiTenantAuthenticationProvider

Connects to mechanism-specific authentication providers.

Class: `com.hp.ccue.identity.authn.MultiTenantAuthenticationProvider`

Property Name	Description
`providers`	Required. List of `AuthenticationProvider` objects that provide mechanism-specific authentication Default value: (None) Externalized: No
`secondaryEnabled`	Required if using Keystone. Flag that indicates whether the secondary authentication path (Keystone) is enabled Default value: `false` Externalized: `idm.keystone.enabled`
`secondaryProvider`	Required if using Keystone. Reference to Authentication provider bean to use for secondary authentication path. The Keystone authentication provider is the only one that supports this type of usage. Default value: (None) Externalized: No
`secondaryRequired`	Required if using Keystone. Flag that indicates whether secondary (Keystone) authentication must succeed in order for authentication to be considered a success. Default value: `false` Externalized: `idm.keystone.required`

IdentityServiceImpl

The identity service implementation object.

Class: `com.hp.ccue.identity.service.IdentityServiceImpl`

Property Name	Description
provider	Required. Reference to the AuthenticationProvider bean to use to perform authentication. This is the MultiTenantAuthenticationProvider Default value: (None) Externalized: No
tokenFactory	Required. The token factory for creating identity tokens in response to successful authentications Default value: (None) Externalized: No
queryService	Required. The persistence service that provides all persistence operations. Default value: (None) Externalized: No
trustFactory	Required. The TrustFactory for validating all Trust objects. Default value: (None) Externalized: No

IdentityController

The controller object that provides the REST API for the identity service.

Class: `com.hp.ccue.identity.service.IdentityController`

Property Name	Description
identityService	Required. The IdentityService object that implements the identity service. You must set the value of this to the IdentityServiceImpl instance. Default value: (None) Externalized: No

KeystoneAuthenticationProvider

Uses Keystone (if used) to perform authentication.

Class: `com.hp.ccue.identity.keystone.KeystoneAuthenticationProvider`

Property Name	Description
`templateFactory`	Required. Creates the `RestTemplate` object that facilitates performing REST calls Default value: (None) Externalized: No
`configuration`	Required. Network configuration of the Keystone service to connect to in order to perform authentication: a `KeystoneConfig` object Default value: (None) Externalized: No
`tokenFactory`	Required. The token factory to validate returned tokens Default value: (None) Externalized: No

KeystoneConfig

Identifies the Keystone endpoint for authentication.

Property Name	Description
`protocol`	Optional if the default value is not acceptable. The protocol to access Keystone Default value: `http` Externalized: `idm.keystone.protocol`
`hostname`	Required. Optional if the default value is not acceptable. The hostname or IP address of the Keystone server Default value: (None) Externalized: `idm.keystone.hostname`
`port`	Optional if the default value is not acceptable. The port number for Keystone on `hostname` Default value: `5000` Externalized: `idm.keystone.port`

Property Name	Description
`servicePath`	Optional if the default value is not acceptable. The service path to the Keystone API on the Keystone server Default value: `v3` Externalized: `idm.keystone.servicePath`
`domainName`	Optional if the default value is not acceptable. The Keystone domain name under which all operations are performed Default value: `Default` Externalized: `idm.keystone.domainName`
`transportUsername`	Required. The username for the Keystone transport user Default value: (None) Externalized: `idm.keystone.transportUsername`
`transportPassword`	Required. The password for the Keystone transport user Default value: (None) Externalized: `idm.keystone.transportPassword`
`transportProject`	Required. The project for the Keystone transport user Default value: (None) Externalized: `idm.keystone.transportProject`

KeystoneSecondaryAuthenticationProvider

Uses Keystone (if used) to perform authentication.

Class: `com.hp.ccue.identity.keystone.KeystoneSecondaryAuthenticationProvider`

Property Name	Description
`keystoneConfigurations`	Required. Associative array mapping configuration identifiers to `KeystoneConfig` objects defining network configurations to connect to one or more Keystone services. Default value: (None) Externalized: No

Property Name	Description
`configurationFile`	Required. Filename for properties file that contains Keystone configurations. Default value: (None) Externalized: No
`tokenFactory`	Required. The token factory to validate returned tokens. Default value: (None) Externalized: No
`templateFactory`	Required. Creates the `RestTemplate` object that facilitates performing REST calls. Default value: (None) Externalized: No

RestTemplateFactoryImpl

Configures how REST services are invoked.

Class: `com.hp.ccue.identity.rest.RestTemplateFactoryImpl`

Property Name	Description
`fipsEnabled`	A flag that indicates whether the template factory should ignore settings that interfere with FIPS 140-2 compliance Default value: `false` Externalized: No
`wrapEnabled`	A flag that indicates whether the template factory should wrap JSON output in its specified root value or assume that incoming JSON is wrapped in the root value. This setting depends on the REST service being invoked. For template factories used to invoke HP CSA REST APIs, it should be set to `false`; for template factories used to invoke Keystone REST APIs, it should be set to `true`. Default value: `true` Externalized: No

Property Name	Description
`requireValidCertificate`	A flag that indicates whether the template factory should perform certificate validation and hostname verification (`true`) or ignore them (`false`). If this value is set to `true`, then the corresponding server host names for all beans that use that template factory must be given in a way that matches the certificate for that server (a fully-qualified domain name is generally required). Default value: `true` Externalized: `idm.ssl.requireValidCertificate`

TrustFactory

Configures how the Identity Management component trusts are created and validated.

Class: `com.hp.ccue.identity.domain.impersonation.TrustFactory`

Property Name	Description
`lifetime`	Required. The lifetime of a trust. Default value: 90 (days) Externalized: No
`lifetimeMinutes`	Required. Alternate setter for trust lifetime, expressed in minutes (write only). Default value: (None) Externalized: No
`lifetimeHours`	Required. Alternate setter for trust lifetime, expressed in hours (write only). Default value: (None) Externalized: No
`lifetimeDays`	Required. Alternate setter for trust lifetime, expressed in days (write only). Default value: (None) Externalized: No

Appendix E: HP Operations Orchestration Manual Configuration for Designs

The HP CSA solution includes a number of HP Operations Orchestration flows that perform HP CSA operations. This appendix describes how to configure HP Operations Orchestration for topology and sequential designs without using the HP Cloud Content Capsule Installer.

Note: If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

In this release, you can install HP Operations Orchestration with HP CSA using the HP CSA installer or you can install HP Operations Orchestration externally. Only one instance of HP Operations Orchestration is required for both topology and sequential designs. If you have upgraded from an earlier version of HP CSA, you may have configured multiple instances of HP Operations Orchestration for sequential designs. If you have upgraded from an earlier version of HP CSA that uses multiple instances of HP Operations Orchestration for sequential designs, you can continue to use the multiple instances of HP Operations Orchestration for sequential designs. If you have upgraded from an earlier version of HP CSA that uses only a single instance of HP Operations Orchestration or are installing HP CSA for the first time, only one configured instance of HP Operations Orchestration is supported.

This appendix describes the following tasks:

- "Configure HP Operations Orchestration for Topology Designs" on page 57
- "Configure HP Operations Orchestration for Sequential Designs" on page 66

Note: If you are configuring HP Operations Orchestration for both topology and sequential designs, complete the configuration for topology designs before the configuration for sequential designs.

Manually Configure HP Operations Orchestration for Topology Designs

The following tasks are to configure HP Operations Orchestration for topology designs. Configure only one instance of HP Operations Orchestration for topology designs without using the HP Cloud Content Capsule Installer.

Note: If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

Complete the following tasks to configure HP Operations Orchestration to integrate with HP CSA:

- Upgrade HP Operations Orchestration
- Configure a secure connection between HP CSA and HP Operations Orchestration
- Configure an internal user
- Deploy content packs
- Update the HP Service Manager base content pack
- Configure properties in HP CSA
- Configure HP Single Sign-On
- Obscure passwords in HP Operations Orchestration flows (optional)

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed and *`%ICONCLUDE_HOME%`* or *`$ICONCLUDE_HOME`* is where you installed HP Operations Orchestration.

Be sure all the latest patches for HP Operations Orchestration have been installed. See the *HP Cloud Service Automation System and Software Support Matrix* for more information, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Upgrade HP Operations Orchestration

Update HP Operations Orchestration version 10.21.0001 by installing hotfix **HF_27629**.

If you are using the embedded HP Operations Orchestration (the HP Operations Orchestration that is installed with HP CSA), the upgrade was performed automatically by the HP CSA installer.

If you are using an external HP Operations Orchestration, you must manually apply this hotfix to HP Operations Orchestration. For your convenience, the hotfix is delivered with the HP CSA installation media. Locate the readme file for this hotfix and follow the instructions on how to upgrade HP Operations Orchestration.

Alternatively, you can download the hotfix from https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=HF_27629.

Configure a Secure Connection between HP CSA and HP Operations Orchestration

Export HP Operations Orchestration's certificate from HP Operations Orchestration's truststore. If HP Operations Orchestration and HP CSA are not installed on the same system, copy the certificate to the HP CSA system and import the certificate into HP CSA's truststore. TLS must be configured between HP CSA and HP Operations Orchestration.

Do the following:

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

2. Run the following command:

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

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

   where `C:\oo.crt` and `/tmp/oo.crt` are examples of filenames and locations used to store the exported root certificate (you can choose a different filename and location).

3. If HP Operations Orchestration is not running on the same system as HP Cloud Service Automation, copy `oo.crt` from the HP Operations Orchestration system to the system running HP Cloud Service Automation.

4. On the system running HP Cloud Service Automation, open a command prompt.

5. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias tomcat -file /tmp/oo.crt -
   trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

6. When prompted for the keystore password, enter `changeit`.

7. Enter `yes` when prompted to trust the certificate.

Configure an Internal User

Internal users can be used to configure HP Operations Orchestration for HP CSA.

This user is used for provisioning topology designs.

1. From the system on which HP CSA is installed (the system on which the content packs are installed), log in to HP Operations Orchestration Central.

2. Click **System Configuration**.

3. Select **Security** > **Internal Users**.

4. Click the **+** (Add) icon.

5. Enter the following information:

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

   The admin user is used with HP Single Sign-On (HP SSO). When HP Operations Orchestration is launched from the Cloud Service Management Console, this user allows access to HP Operations Orchestration without having to log in. If you are using topology designs, the admin user can also be used for provisioning topology designs.

6. Click **Save**.

7. If not enabled, enable authentication by selecting the **Enable Authentication** check box.

8. Select **OK** in the confirmation dialog.

Deploy Content Packs

The following groups of content packs must be deployed in the order described below:

- Base content packs
- Component Tool content packs
- HP CSA content packs
- HP Codar content packs (optional)

Note: Do not deploy the Component Tool and HP CSA content packs until after you have deployed the base content packs. These content packs must be deployed separately from the base content packs and after you have deployed the base content packs.

1. From HP Operations Orchestration Central, click **Content Management**.

2. Click the **Content Packs** tab.

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

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

5. Deploy the base content packs. Navigate to the `$CSA_HOME/oo/ooContentPack` directory. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

   - oo10-base-cp-1.4.4

   - oo10-cloud-cp-1.4.0

   - oo10-hp-solutions-cp-1.4.0

   - oo10-virtualization-cp-1.4.0

   - oo10-sa-cp-1.2.0.001

   - oo10-sm-cp-1.0.3

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

6. After you have successfully deployed all the base content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.

7. Click the **+** (Add files for deployment) icon.

8. Open a command prompt and open the `$CSA_HOME/Tools/ComponentTool/contentpacks/component-upload-sequence.txt` file.

9. Deploy the Component Tool content packs. From HP Operations Orchestration Central, navigate to the `$CSA_HOME/Tools/ComponentTool/contentpacks/` directory. Add and deploy the content packs in the order listed in the `component-upload-sequence.txt` file (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

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

10. After you have successfully deployed all the Component Tool content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.

11. Open a command prompt and extract all the `.jar` files from the `$CSA_HOME/Tools/CSLContentInstaller/csa-ootb-content-04.50.000.zip` file.

12. From HP Operations Orchestration Central, click the **+** (Add files for deployment) icon.

13. Deploy the HP CSA content packs. Navigate to the directory in which you extracted all the `.jar` files. Add and deploy the following content packs shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

    > **Note:** You can select more than one content pack to add and deploy at the same time. You may add and deploy all of these HP CSA content packs at the same time.

    - com.hp.csl.amazon.ec2.topology.jar
    - com.hp.csl.openstack.topology.jar
    - com.hp.csl.sitescope.topology.jar
    - com.hp.csl.vcenter.topology.jar

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

14. If you want to install the HP Codar content packs (these steps are optional), open a command prompt and extract all the `.jar` files from the `$CSA_HOME/Tools/CSLContentInstaller/codar-ootb-content-01.50.000.zip` file.

15. From HP Operations Orchestration Central, click the **+** (Add files for deployment) icon.

16. Deploy the HP Codar content packs. Navigate to the directory in which you extracted all the HP Codar `.jar` files. Add and deploy the following content packs shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

    > **Note:** You can select more than one content pack to add and deploy at the same time. You may add and deploy all of these HP Codar content packs at the same time.

    - CODAR-cp-1.00.0000.jar
    - CSA-HPOO-cp-4.50.0000.jar
    - EXISTING-INFRASTRUCTURE-WINDOWS-cp-1.50.0000.jar

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

17. When you have finished deploying all the content packs, click **Close** to close the dialog.

Update and Redeploy the HP Service Manager Base Content Pack

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

1. Stop the HP Operations Orchestration services:

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

      For example, `/usr/local/hp/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/hp/csa/OO/ras/bin/ras stop`

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

   `<HPOOinstallation>/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`

4. Run the following SQL command against the HP 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 HP Operations Orchestration services:

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

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

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

a. Log in to HP 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**.

Configure HP Operations Orchestration Properties in the csa.properties File

If you integrated with HP Operations Orchestration using the installer (during the installation or upgrade process), you do not need to configure these properties (they are already configured). These properties are used to integrate with HP Operations Orchestration. In the subscription event overview section of the **Operations** area in the Cloud Service Management Console, selecting the Process ID opens HP Operations Orchestration to the detailed page of the selected process when these properties are configured.

To configure the HP Operations Orchestration properties:

1. Edit the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/classes/csa.properties` file and configure the following properties:

Property	Description
OOS_URL	The URL used to access HP Operations Orchestration Central. This is the HP Operations Orchestration used for provisioning topology designs. For example, `https://<hostname>:8445`. This property is automatically set during installation. If you are using the embedded HP Operations Orchestration that is included with HP CSA, this property is set using the values entered for the **Fully Qualified Hostname** and **HP OO Port** fields during installation. If you are using a standalone/external HP Operations Orchestration, this property is set using the values entered for the **HP OO Hostname** and **HP OO Port** fields during installation.

Property	Description
OOS_USERNAME	The username used to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO User** field during installation.
OOS_PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log in to HP Operations Orchestration Central. This property is automatically set during installation using the value entered for the **HP OO Password** field during installation.

2. Restart HP CSA.

   See "Restart HP CSA" on page 129 for detailed information on how to restart HP CSA.

Configure HP Single Sign-On between HP CSA and HP Operations Orchestration

If HP Single Sign-On (HP SSO) was enabled during installation of HP CSA, HP SSO can be configured between HP CSA and HP Operations Orchestration. Configuring HP SSO allows you to launch HP Operations Orchestration from the Cloud Service Management Console without having to log in to HP Operations Orchestration.

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

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

Note: In order to use HP SSO between HP CSA and HP Operations Orchestration, the systems on which HP CSA and HP Operations Orchestration are installed must be in the same domain.

Configure and Enable HP Single Sign-On

To configure and enable HP SSO on HP Operations Orchestration, do the following:

1. Log in to HP Operations Orchestration Central.

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

3. Select **Security** > **SSO**.

4. Select the **Enable** checkbox.

5. Enter the **InitString**. The `initString` setting for HP CSA and HP Operations Orchestration must be configured to the same value. In HP CSA, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).

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

7. Click **Save**.

Configure LDAP Users for Single Sign-On

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

To configure LDAP for HP Operations Orchestration, do the following:

1. Log in to HP Operations Orchestration Central.

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

3. Select **Security** > **LDAP**.

4. Enter the information to configure LDAP.

5. Click **Save**.

Obscure Passwords in HP Operations Orchestration Flows (Optional)

Some HP Operations Orchestration flows included with HP CSA may show passwords in clear text when viewed in HP Operations Orchestration Central. You can obscure these passwords by modifying the flow in HP Operations Orchestration Studio.

Note: You must have HP Operations Orchestration Studio installed. HP Operations Orchestration Studio is supported on Windows platforms only and is not part of the embedded HP Operations Orchestration that is included with HP CSA. See the HP Operations Orchestration documentation, such as the *HP Operations Orchestration System Requirements*, for more information about HP Operations Orchestration Studio.

To obscure passwords in HP Operations Orchestration flows:

1. Open HP Operations Orchestration Studio.
2. Locate the flow to update.
3. Right-click on the flow and select **References > What uses this?**.

   A list of flows that use the flow is displayed (that is, the flow to update is a subflow of the flows displayed in the list).
4. Select a flow from the list of flows.
5. Locate the subflow (the flow to update).
6. Right-click on the subflow and select **Properties**.
7. Located the property to obscure (such as a password), enable it, but do not assign a value to it.
8. Save the flow.
9. Repeat this procedure for every flow from the list of flows.

Manually Configure HP Operations Orchestration for Sequential Designs

The following tasks are to configure HP Operations Orchestration for sequential designs. If you are installing HP CSA for the first time, configure only one instance of HP Operations Orchestration. If you have upgraded from an earlier version of HP CSA that has multiple instances of HP Operations Orchestration configured for sequential designs, you can continue to use multiple instances of HP Operations Orchestration, including HP Operations Orchestration 9.07.

Note: If you followed the instructions in the *HP Cloud Service Automation Installation Guide* or *HP Cloud Service Automation Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section.

Complete the following tasks to configure HP Operations Orchestration to integrate with HP CSA:

Note: If you have manually configured HP Operations Orchestration for topology designs, you have already completed some of these tasks. Skip the tasks that you have already completed.

- Upgrade HP Operations Orchestration
- Add a JRE to the system path
- Install the HP CSA content pack
- Configure internal users
- Deploy content packs
- Update the HP Service Manager base content pack
- Set up system accounts for the HP CSA content pack
- Set up system properties
- Import HP Operations Orchestration flows
- Configure a secure connection between HP Cloud Service Automation and HP Operations Orchestration
- Configure HP Single Sign-On
- Obscure passwords in HP Operations Orchestration flows (optional)

Note: In the following instructions, `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed and *`%ICONCLUDE_HOME%`* or *`$ICONCLUDE_HOME`* is where you installed HP Operations Orchestration.

Be sure all the latest patches for HP Operations Orchestration have been installed. See the *HP Cloud Service Automation System and Software Support Matrix* for more information, available on the HP Software Support Web site at http://h20230.www2.hp.com/selfsolve/manuals/ (this site requires that you register with HP Passport).

Upgrade HP Operations Orchestration

Update HP Operations Orchestration version 10.21.0001 by installing hotfix **HF_27629**.

If you are using the embedded HP Operations Orchestration (the HP Operations Orchestration that is installed with HP CSA), the upgrade was performed automatically by the HP CSA installer.

If you are using an external HP Operations Orchestration, you must manually apply this hotfix to HP Operations Orchestration. For your convenience, the hotfix is delivered with the HP CSA installation media. Locate the readme file for this hotfix and follow the instructions on how to upgrade HP Operations Orchestration.

Alternatively, you can download the hotfix from https://patch-central.corp.hp.com/crypt-web/protected/viewContent.do?patchId=HF_27629.

Add a JRE to the System Path

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

Open a shell and enter the following command:

If HP Operations Orchestration and HP CSA are installed on the same system:

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

or

If HP Operations Orchestration and HP CSA are installed on different systems:

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

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

Install the HP CSA Content Pack

- Copy the `$CSA_HOME/CSAKit-4.5/OO Flow Content/10X/oo10-csa-cp-4.50.000-uuids.txt` file to:

  Windows
  `%ICONCLUDE_HOME%\central\cmu\exclusions`

  Linux
  `$ICONCLUDE_HOME/central/cmu/exclusions`

- If HP CSA and HP Operations Orchestration are running on different systems, copy the `$CSA_HOME/CSAKit-4.5/OO Flow Content/10X/oo10-csa-cp-4.50.0000.jar` and `oo10-csa-integrations-cp-4.50.0000.jar` files from the HP Cloud Service Automation system to the HP Operations Orchestration system (where `$CSA_HOME` is the directory in which HP Cloud Service Automation is installed).

Configure Internal Users

Internal users can be used to configure HP Operations Orchestration for HP CSA.

1. From the system on which HP CSA is installed (the system on which the content packs are installed), log in to HP Operations Orchestration Central.

2. Click **System Configuration**.

3. Select **Security** > **Internal Users**.

4. Click the **+** (Add) button.

5. Enter the following information:

Field	Recommended Value
User Name	csaoouser
Password	cloud
Roles	ADMINISTRATOR, SYSTEM_ADMIN

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

6. Click **Save**.

7. If not enabled, enable authentication by selecting the **Enable Authentication** check box.

8. Select **OK** in the confirmation dialog.

9. Click the **+** (Add) icon.

10. Enter the following information:

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

The admin user is used with HP Single Sign-On (HP SSO). When HP Operations Orchestration is launched from the Cloud Service Management Console, this user allows access to HP Operations Orchestration without having to log in. If you are using topology designs, the admin user can also be used for provisioning topology designs.

11. Click **Save**.

12. If not enabled, enable authentication by selecting the **Enable Authentication** check box.

13. Select **OK** in the confirmation dialog.

14. Log out of HP Operations Orchestration Central and log back in as the csaoouser.

Deploy Content Packs

The following groups of content packs must be deployed in the order described below:

- Base content packs
- HP CSA sequential design content packs
- HP CSA content packs

1. From HP Operations Orchestration Central, click **Content Management**.
2. Click the **Content Packs** tab.
3. Click the **Deploy New Content** icon.
4. In the Deploy New Content dialog, in the upper left corner, click the **+** (Add files for deployment) icon.
5. Deploy the base content packs. Navigate to the `$CSA_HOME/oo/ooContentPack` directory. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

   - oo10-base-cp-1.4.4
   - oo10-cloud-cp-1.4.0
   - oo10-hp-solutions-cp-1.4.0
   - oo10-virtualization-cp-1.4.0
   - oo10-sa-cp-1.2.0.001
   - oo10-sm-cp-1.0.3

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

6. After you have successfully deployed all the base content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.
7. Click the **+** (Add files for deployment) icon.
8. Deploy the HP CSA sequential design content packs. Navigate to the `$CSA_HOME/CSAKit-4.5/OOFlowContent/10X` directory. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+**

(Add files for deployment) icon):

- oo10-csa-integrations-cp-4.50.0000
- oo10-csa-cp-4.50.0000

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

9. After you have successfully deployed all the HP CSA sequential design content packs, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon.

10. Open a command prompt and extract all the `.jar` files from the `$CSA_HOME/Tools/CSLContentInstaller/csa-ootb-content-04.50.000.zip` file.

11. Click the **+** (Add files for deployment) icon.

12. Deploy the HP CSA content packs. Navigate to the directory in which you extracted all the `.jar` files. Add and deploy the following content packs in the order shown below (after each successful deployment, to add and deploy the next content pack without closing the dialog, click the **Reset** icon in the upper left corner to clear the dialog and enable the **+** (Add files for deployment) icon):

    > **Note:** You can select more than one content pack to add and deploy at the same time. However, the `*.util.jar` content packs should be deployed first. For example, you can deploy two groups of content packs: select all of the `*.util.jar` content packs and deploy them first. Then, select the rest of the content packs and deploy them.

    - com.hp.csl.base.util.jar
    - com.hp.csl.middleware.util.jar
    - com.hp.csl.openstack.util.jar
    - com.hp.csl.amazon.ec2.jar
    - com.hp.csl.dma.jar
    - com.hp.csl.goactive.jar
    - com.hp.csl.icsp.jar
    - com.hp.csl.matrix.jar
    - com.hp.csl.na.jar
    - com.hp.csl.oneview.jar
    - com.hp.csl.openstack.jar

- com.hp.csl.sa.agentinstallation.jar
- com.hp.csl.sa.softwarepolicies.jar
- com.hp.csl.sitescope.jar
- com.hp.csl.sm.jar
- com.hp.csl.ucmdb.jar
- com.hp.csl.vmware.vcenter.jar
- com.hp.csl.vpv.jar

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

13. When you have finished deploying all the content packs, click **Close** to close the dialog.

Update and Redeploy the HP Service Manager Base Content Pack

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

1. Stop the HP Operations Orchestration services:

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

      For example, `/usr/local/hp/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/hp/csa/OO/ras/bin/ras stop`

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

   `<HPOOinstallation>/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`

4. Run the following SQL command against the HP 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 HP Operations Orchestration services:

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

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

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

   a. Log in to HP 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**.

Set Up System Accounts for the Content Packs

Set up system accounts for the content packs:

1. Log in to HP Operations Orchestration Central.

2. Click **Content Management**.

3. Select **Configuration Items** > **System Accounts**.

4. Click the **Add** icon.

5. Enter the following information if it is not already configured:

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

> **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Property Value** (HP Operations Orchestration version 9.07) or **Override Value** (HP Operations Orchestration version 10.21.0001) configured for the CSA_ OO_USER System Property setting.

6. Click **Save**.

7. Click the **Add** icon.

8. Enter the following information if it is not already configured:

Field	Recommended Value
System Account Name	CSA_SERVICEMANAGER_CREDENTIALS
User Name	falcon
Password	*<leave_blank>*

9. Click **Save**.

Set Up System Properties for the Content Packs

Set up the following system properties for the content packs:

1. Log in to HP Operations Orchestration Central.

2. Click **Content Management**.

3. Select **Configuration Items** > **System Properties**.

4. Click the **Add** icon.

5. Enter the following information if it is not already configured:

Field	Recommended Value
Name	CSA_REST_URI
Override Value	https://<*csa_hostname*>:8444/csa/rest

6. Click **Save**.

Import HP Operations Orchestration Flows

See "Import HP Operations Orchestration Flows" on page 84 for more information.

Note: Use the `$CSA_HOME/Tools/CSLContentInstaller/CslHPOOInput.xml` file as the HP Operations Orchestration input file that defines the flows to be imported.

Configure a Secure Connection between HP Cloud Service Automation and HP Operations Orchestration

Export HP Operations Orchestration's certificate from HP Operations Orchestration's truststore. If HP Operations Orchestration and HP CSA are not installed on the same system, copy the certificate to the HP CSA system and import the certificate into HP CSA's truststore. TLS must be configured between HP CSA and HP Operations Orchestration.

Do the following:

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

2. Run the following command:

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

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

   where `C:\oo.crt` and `/tmp/oo.crt` are examples of filenames and locations used to store the exported root certificate (you can choose a different filename and location).

3. If HP Operations Orchestration is not running on the same system as HP Cloud Service Automation, copy `oo.crt` from the HP Operations Orchestration system to the system running HP Cloud Service Automation.

4. On the system running HP Cloud Service Automation, open a command prompt.

5. Run the following command:

   ```
   $CSA_JRE_HOME/bin/keytool -importcert -alias tomcat -file /tmp/oo.crt -
   trustcacerts -keystore $CSA_JRE_HOME/lib/security/cacerts
   ```

   where `$CSA_JRE_HOME` is the directory in which the JRE that is used by HP CSA is installed.

6. When prompted for the keystore password, enter `changeit`.

7. Enter `yes` when prompted to trust the certificate.

Configure HP Single Sign-On between HP CSA and HP Operations Orchestration

If HP Single Sign-On (HP SSO) was enabled during installation of HP CSA, HP SSO can be configured between HP CSA and HP Operations Orchestration. Configuring HP SSO allows you to launch HP Operations Orchestration from the Cloud Service Management Console without having to log in to HP Operations Orchestration.

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

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

Note: In order to use HP SSO between HP CSA and HP Operations Orchestration, the systems on which HP CSA and HP Operations Orchestration are installed must be in the same domain.

Configure and Enable HP Single Sign-On

To configure and enable HP SSO on HP Operations Orchestration, do the following:

1. Log in to HP Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security** > **SSO**.
4. Select the **Enable** checkbox.
5. Enter the **InitString**. The `initString` setting for HP CSA and HP Operations Orchestration must be configured to the same value. In HP CSA, `initString` is configured in the `crypto` element in the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/hpssoConfiguration.xml` file. The `initString` value represents a secret key and should be treated as such in your environment (this string is used to encrypt and decrypt the LWSSO_COOKIE_KEY cookie that is used to authenticate the user for single sign-on).
6. Enter the **Domain**. This is the domain name of the network of the servers on which HP CSA and HP Operations Orchestration are installed.
7. Click **Save**.

Configure LDAP Users for Single Sign-On

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

To configure LDAP for HP Operations Orchestration, do the following:

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

Obscure Passwords in HP Operations Orchestration Flows (Optional)

Some HP Operations Orchestration flows included with HP CSA may show passwords in clear text when viewed in HP Operations Orchestration Central. You can obscure these passwords by modifying the flow in HP Operations Orchestration Studio.

Note: You must have HP Operations Orchestration Studio installed. HP Operations Orchestration Studio is supported on Windows platforms only and is not part of the embedded HP Operations Orchestration that is included with HP CSA. See the HP Operations Orchestration documentation, such as the *HP Operations Orchestration System Requirements*, for more information about HP Operations Orchestration Studio.

To obscure passwords in HP Operations Orchestration flows:

1. Open HP Operations Orchestration Studio.
2. Locate the flow to update.
3. Right-click on the flow and select **References > What uses this?**.

   A list of flows that use the flow is displayed (that is, the flow to update is a subflow of the flows displayed in the list).
4. Select a flow from the list of flows.
5. Locate the subflow (the flow to update).
6. Right-click on the subflow and select **Properties**.
7. Located the property to obscure (such as a password), enable it, but do not assign a value to it.
8. Save the flow.
9. Repeat this procedure for every flow from the list of flows.

Appendix F: Cross-Product Upgrade between HP Codar and HP CSA

This appendix shows the upgrade result if you have an existing HP Cloud Service Automation (HP CSA) 4.2x installation and you want to upgrade to HP CSA 4.50 with HP Codar 1.50. The upgrade result from HP CSA 4.2x will always be HP CSA 4.50, as shown in the table below.

For information about upgrading to HP CSA 4.50, see the *HP Cloud Service Automation Upgrade Guide*.

Existing installation	**Upgrade installer used**	**Upgraded to**
HP CSA 4.2x instant-on	HP Codar 1.50	HP CSA 4.50 instant-on
HP CSA 4.2x no license	HP Codar 1.50	HP CSA 4.50 no license
HP CSA 4.2x license	HP Codar 1.50	HP CSA 4.50 license
HP Codar 1.00 no license	HP CSA 4.50	HP Codar 1.50 no license
HP Codar 1.00 license	HP CSA 4.50	HP Codar 1.50 license
HP CSA 4.2x with HP CSA and HP Codar licenses	HP Codar 1.50	HP CSA 4.50 with HP CSA and HP Codar licenses
HP Codar 1.00 with HP CSA and HP Codar licenses	HP CSA 4.50	HP CSA 4.50 with HP CSA and HP Codar licenses

Send Documentation Feedback

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

Feedback on Configuration Guide (Cloud Service Automation 4.50)

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@hp.com.

We appreciate your feedback!

Java™
COMPATIBLE