HP Codar

Software Version: 1.50
Windows ® and Linux operating systems

Configuration Guide

Document Release Date: June 2015
Software Release Date: June 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

Overview 10

Getting started 12

Prepare LDAP for HP Codar 12

Configure HP Codar truststore properties 13

Location of HP Codar truststore 14

Request software licenses 15

Request software license 15

Request software license for clustered environment 16

Request software license for system with updated IP address 16

Enable TLS on your web browser 16

Update HP Codar service startup type 19

Update HP Codar service startup type on Windows 19

Update HP Codar service startup type on Linux 19

Location of JRE Installed with HP Codar on Windows 19

Secure connections 20

Configure secure connections for client browsers 20

Configure HP Codar to use trusted Certificate Authority-Signed or subordinate Certificate Authority-Signed certificate 21

Step 1: Create a keystore and self-signed certificate 22

Step 2: Create a Certificate Signing Request 23

Step 3: Submit the certificate signing request to a Certificate Authority 23

Step 4: Import the Certificate Authority's root certificate 23

Step 5: Import Certificate Authority-Signed certificate 24

Step 6: Configure the web server 25

Step 7: Configure client browsers 26

Step 8: Test secure connections 26

Configure HP Codar to use internal Certificate Authority-Signed certificate 27

Step 1: Import the Certificate Authority's root certificate 27

Step 2: Import internal Certificate Authority-Signed certificate 28

Step 3: Configure the web server 28

Step 4: Configure client browsers 30

Step 5: Test secure connections 30

Configure HP Codar to use self-signed certificate 30

Step 1: Create a keystore and self-signed certificate 31
Step 2: Export the self-signed certificate 32
Step 3: Import self-signed certificate as a trusted certificate 33
Step 4: Configure web server 33
Step 5: Configure client browsers (optional) 34
Step 6: Test secure connections 34

Configure secure connections for LDAP 35

Configure secure connections for SMTP 35

Configure secure connections for Oracle database 36

Configure secure connections for Microsoft SQL server 39

Configure secure connections for HP Operations Orchestration Load Balancer 40

HP Operations Orchestration 44

Configure HP Operations Orchestration for topology designs 44
Configure internal user 45
Deploy content packs 46
Configure HP Single Sign-On between HP Codar and HP Operations Orchestration 46
Configure and enable HP Single Sign-On 47
Configure LDAP users for single sign-on 47
Configure HP Operations Orchestration properties in csa.properties file 48
Configure secure connection between HP Codar and HP Operations Orchestration 49
Run component tool 49

Integrate with HP Operations Orchestration 53
Add JRE to system path 54
Install HP Codar content pack 55
Configure internal users 55
Deploy content packs required by HP Codar 56
Set up system accounts for HP Codar content pack 57
Set up system properties for HP Codar content pack 58
Configure HP Single Sign-On between HP Codar and HP Operations Orchestration 58
Configure and enable HP Single Sign-On 59
Configure LDAP users for single sign-on 59
Configure secure connection between HP Codar and HP Operations Orchestration 60

HP Codar Console 61

Roles in HP Codar 61
Application Architect role 61
Application Developer role 61

Application QA role 62
Application Release Manager role 62
Application Integration role 62
Configure provider organization 62
Add software license 63
Proxy configuration for resource providers outside the internal network 63
Customize HP Codar Console dashboard 66
Using predefined custom tile 66
Enabling other predefined dashboard tiles 67
Creating dashboard tile 68
Adding secondary dashboard 73
Modifying dashboard tile 76
Disabling dashboard tile 76
Dashboard configuration file syntax 76
Customize HP Codar Console font 78
Customize HP Codar Console title 78
Common HP Codar tasks 80
Launch HP Codar Console 80
Start HP Codar 80
Stop HP Codar 81
Restart HP Codar 81
Encrypt password 82
Clear web browser cache 83
Uninstall HP Codar 83
Uninstall HP Codar on Windows 83
Uninstall HP Codar on Linux 84
User administration 86
Allow non-administrator users to start and stop HP Codar service on Windows 86
Allow non-administrator users to start and stop HP Codar service 86
Add permissions to the HP Codar directory for non-administrator user 88
Allow HP Codar service to be run as non-administrator user on Windows 88
Create non-administrator users 89
Configure HP Codar service 90
Configure file system permissions for non-administrator users 90

Change HP Codar out-of-the-box user accounts for Windows and Linux 92
HP Codar Console user accounts 93

Configure IPv6 100
Launch the HP Codar Console 101

Common Access Card 102
Stop HP Codar 102
Update JBoss configuration to set up client authentication 102
Configure HP Codar Console 104
Configure certificate revocation 105
Configure HP Codar to use a Certificate Revocation List 106
Configure HP Codar to use Certificate Revocation List Distribution Point 106
Configure HP Codar to Use Online Certificate Status Protocol 107
Start HP Codar 107

Single Sign-On 108
Integrate with HP Single Sign-On 108
Enable HP Single Sign-On 108
Step 1: Configure the domain 109
Step 2: Set the HP Single Sign-On property 109
Step 3: Configure the Identity Management component 110
Step 4: Restart HP Codar 111
Disable HP Single Sign-On 111
Integrate HP Codar with single sign-on solution 111
Verify HP Codar provider organization's LDAP server configuration 112
Verify HP Codar consumer organization's LDAP server configuration 113
Configure custom single-sign-on server to work with HP Codar 114
Stop HP Codar 114
Configure HP Codar Console 114
Configure proxy mapping 114
Start HP Codar 114
Verify single-sign-on integration 115
Integrate HP Codar with CA SiteMinder 115
Configure HP Codar provider organization's LDAP server 116
Configure SiteMinder Policy Server for HP Codar integration 117
118
Configure the SiteMinder Web Agent for HP Codar integration 118

Configure HP Codar for SiteMinder integration 118

Stop HP Codar 118

Configure HP Codar Console 119

Start HP Codar 120

Customize Logout page (optional) 121

Database administration 122

Restart database and HP Codar service 122

Restart HP Codar service on Windows 122

Restart HP Codar service on Linux 122

Configure HP Codar reporting database user 123

Update HP Codar database system 124

Update HP Codar database user or password 126

Import large archives 128

Import large archives using HP Codar Content Archive Tool 128

Import large archives from HP Codar Console or through the REST API 128

Install HP Codar database schema 129

Upgrade or install database schema 130

Configure HP Codar to mitigate frequently dropped database connections 136

Appendix A: HP Codar Console properties 138

Appendix B: HP Operations Orchestration settings 157

Appendix C: Identity Management configuration 160

External configuration 160

Configure seeded authentication 162

Configure blacklist 162

Configure Java Relying Party Library 163

IdentityServiceConfig 163

IdentityAuthenticationProvider 163

HeaderAuthenticationProvider 164

Internal configuration 164

InfinispanTokenStore 164

JwtTokenFactory 165

ConvergedLdapAuthConfig 166

ConvergedActiveDirectoryAuthenticationProvider and ConvergedLdapAuthenticationProvider 167

SeededAuthenticationProvider 167
IdentityAuthenticationProvider 168
MultiTenantAuthenticationProvider 168
IdentityServiceImpl 169
IdentityController 170
KeystoneAuthenticationProvider 170
KeystoneConfig 171
KeystoneSecondaryAuthenticationProvider 172
RestTemplateFactoryImpl 173
TrustFactory 174

Send Documentation Feedback 175

Overview

This document provides information on how to set up the HP Codar Console and HP Codar in order to enable users to log in and use the HP Codar Console . Some tasks must be completed before you can start using HP Codar.

The user who sets up HP Codar 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 Codar.

Note: If you have added the HP Cloud Service Automation license, you have access to all of the HP Cloud Service Automation functionality, such as global search and reporting database user. For details see the *HP Cloud Service Automation Configuration Guide*.

The following information is provided in this document:

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

Secure Connections. Many of the components that interact with HP Codar may require communication over a secure connection. You may want to replace the HP Codar 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 Codar, HP Operations Orchestration must be integrated with HP Codar and sample flows must be imported before the flows can be executed.

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

Common HP Codar Tasks. Common tasks include launching the HP Codar Console, starting, stopping, or restarting HP Codar, encrypting an HP Codar password, and uninstalling HP Codar.

User Administration. User administration includes tasks such as changing the out-of-the-box users. On Windows, also allows non-administrator users to start and stop HP Codar services.

IPv6 Configuration. Configure HP Codar 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 Codar using a Personal Identity Verification card.

Single Sign-On. Enable or disable HP Single Sign-On that is included with HP Codar. Single sign-on can also be configured for the HP Codar Console 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 Codar reporting database user if you did not configure it during installation, updating HP Codar database system or users and passwords, importing large archives, purging service subscriptions, installing the HP Codar database schema, and configuring HP Codar to mitigate frequently dropped database connections.

HP Codar Console Properties. This is a reference to the HP Codar Console configurable properties.

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

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

See the following guides for more information:

- HP Codar: *HP Codar Concepts Guide*
- Supported components and versions: *HP Codar System and Software Support Matrix*
- Installation: *HP Codar Installation and Configuration Guide*
- Upgrade: *HP Codar Upgrade Guide*
- Configuration: *HP Codar Configuration Guide*
- HP Codar Console: : *HP Codar Console Help*

Getting started

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

Tasks include:

- "Prepare LDAP for HP Codar" below (required)
- "Configure HP Codar truststore properties" on the next page (required)
- "Request software licenses" on page 15 (required)
- "Enable TLS on your web browser" on page 16 (required)
- "Update HP Codar service startup type" on page 19 (optional)
- "Location of JRE Installed with HP Codar on Windows" on page 19

Prepare LDAP for HP Codar

HP Codar 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 Codar 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 Codar, LDAP is used to:

- Authenticate a user's login to the HP Codar Console.
- Authenticate a user's access to information.
- Authorize a user's access to information.
- Add user access control functionalities.
- Add users or a group from LDAP to a design for access control.

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

Before you configure LDAP for the HP Codar Console, 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 Codar 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 who is to receive 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.
- 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 HP Codar Console

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

Configure HP Codar truststore properties

You must configure information about the HP Codar's keystore.

To configure HP Codar truststore properties, complete the following steps:

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 Codar keystore that stores trusted Certificate Authority certificates. **Note:** Use only forward slashes (/) as your path separators.

Property	Description
`csaTruststorePassword`	Required. The encrypted password of the HP Codar keystore (see "Encrypt password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

For more information about these properties, see "HP Codar Console properties" on page 138.

3. Save and exit the file.

4. Restart HP Codar, see "Restart HP Codar" on page 81 .

Location of HP Codar truststore

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

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

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

  `CSA_HOME\openjre\lib\security\cacerts`

  `CSA_HOME` is the directory in which HP Codar is installed — on Windows `C:\Program Files\Hewlett-Packard\Codar` or on Linux `/usr/local/hp/codar/`.

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

  `JRE_HOME\lib\security\cacerts`

  For example:

  Windows: `C:\Program Files\Java\jre7\lib\security\cacerts`

  Linux: 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`

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

  `JAVA_HOME\lib\security\cacerts`

  For example:

  Windows: `C:\Program Files\Java\jdk1.7.0_71\lib\security\cacerts<JAVA_HOME>/lib/security/cacerts`

Linux: If you installed the Oracle JDK in `/usr/local/bin`: `/usr/local/bin/jdk1.7.0_71/lib/security/cacerts`

If you still cannot locate the HP Codar truststore, open the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file and look for the `csaTruststore` property. This property must be set to the location of the HP Codar truststore after installing HP Codar.

Request software licenses

HP Codar version 1.50 requires a software license. HP Codar licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP Codar version 1.50, when you log in to the HP Codar 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 you upgrade to HP Codar version 1.50, when you log in to the HP Codar Console, all HP Codar version 1.00 licenses are valid and are automatically added.

The following topics are covered in this section:

- "Request software license" below
- "Request software license for clustered environment" on the next page
- "Request software license for system with updated IP address" on the next page

For information on how to view, add, or delete a license, see the *HP Codar Console Help*.

Request 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.

See 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 Codar 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 software license for clustered environment

If you are configuring HP Codar in a clustered environment, use the IP address of the load balancer (in the examples given in the *Configuring an HP Codar Cluster for High Availability Using an Apache Web Server as a Proxy*, this is the APACHE_IP_ADDR; in the examples given in the *Configuring an HP Codar 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 software license for system with updated IP address

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

If you immediately add the new license without restarting HP Codar, the license will not be accepted. You must restart HP Codar before adding the new license, see "Restart HP Codar" on page 81. For more information about managing software licenses, see the *HP Codar Console Help*.

Enable TLS on your web browser

The HP Codar Console is configured to require https (http over a secure connection) for client browsers. Specifically, the HP Codar 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 on Windows:

1. Exit or kill all Chrome sessions.
2. If you added a shortcut to launch Chrome from the Taskbar, remove it: right-click the shortcut on the Taskbar and select **Unpin this program from taskbar**.
3. For every shortcut you use to launch Chrome, do the following:
    a. Right-click on the shortcut and select **Properties**.
    b. Select the **Shortcut** tab.
    c. At the end of the Target field, enter the following after the last quotation mark (and include a space after the last quotation mark but before the following content):

       --ssl-version-min=tls1

   d. Click **OK**.

   e. If asked for administrator privileges, click **Continue**.

4. If you deleted the shortcut from the Taskbar, right-click on any updated shortcut and select **Pin to Taskbar**.

5. If Chrome is your default browser, edit the registry:

   a. Click on the **Start** icon, enter **regedit** in the `Search programs and files` box, and press **Enter**.

   b. From the Registry Editor, select **HKEY_CLASSES_ROOT > http > shell > open > command**.

   c. Double-click **(Default)**.

   d. Adding the following at the end of the `Value data` field (and include a space before the following content):

      --ssl-version-min=tls1

   e. Click **OK**.

   f. Close the Registry Editor dialog.

Caution: Depending on how you launch Chrome, your browser session still may allow SSLv3 connections.

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**.

Update HP Codar service startup type

If you have services or applications installed on the same system as HP Codar that HP Codar requires to be available when HP Codar is started (such as the database), update the HP Codar service startup to be delayed. This allows those services time to start before HP Codar starts if the system is rebooted.

Update HP Codar service startup type on Windows

To delay the start of the HP Codar on system reboot, complete the following steps:

1. On the server that hosts HP Codar, navigate to **Start** > **Administrative Tools** > **Services**.
2. In the Service dialog, right-click on the HP Codar service and select **Properties**.
3. In the Properties dialog, locate the **Startup type** field and change the value to **Automatic (Delayed Start)**.
4. Click **OK**.

Update HP Codar service startup type on Linux

To delay the start of the HP Codar on system reboot, complete the following steps:

```
service codar restart
service codar-execution-service.sh restart
```

Location of JRE Installed with HP Codar on Windows

The location of the JRE installed with HP Codar (OpenJDK JRE) is located in the following location:

```
CSA_HOME\openjre
```

For example: `C:\Program Files\Hewlett-Packard\Codar\openjre`

Secure connections

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

Note: HP Codar 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 Codar.

Information includes:

- "Configure secure connections for client browsers" below (required when the HP Codar self-signed certificate expires)
- "Configure secure connections for LDAP" on page 35 (required if the LDAP server requires a secure connection)
- "Configure secure connections for SMTP" on page 35 (required if the SMTP server requires a secure connection)
- "Configure secure connections for Oracle database" on page 36 (required if the Oracle database requires a secure connection)
- "Configure secure connections for Microsoft SQL server" on page 39 (required if Microsoft SQL Server requires a secure connection)
- "Configure secure connections for HP Operations Orchestration Load Balancer" on page 40 (required if you are running the HP Operations Orchestration Load Balancer server and it requires a secure connection)

The function of the secure connection is configured by the `com.hp.csa.service.ssl.insecure` property in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file. That is, a secure connection can be configured to only authenticate the certificate root and verify that the certificate presented by another application or component has not been revoked (default). Or, a secure connection can be configured to authenticate the certificate root, verify that the certificate presented by another application or component has not been revoked, verify the certificate's validity (beginning and expiration dates), and validate the certificate's hostname (configured as the certificate's common name). See the *Secure Connections* section in "HP Codar Console properties" on page 138 for more information about the `com.hp.csa.service.ssl.insecure` property.

Configure secure connections for client browsers

The HP Codar 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 Codar server.

A self-signed certificate is created and configured when HP Codar 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 HP Codar Console and expires 120 days after HP Codar is installed.

When client browsers connect to the HP Codar 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 by configuring a trusted third-party Certificate Authority-signed or subordinate Certificate Authority-signed certificate (see "Configure HP Codar to use trusted Certificate Authority-Signed or subordinate Certificate Authority-Signed certificate" below) or by configuring an internal Certificate Authority-signed certificate (see "Configure HP Codar to use internal Certificate Authority-Signed certificate" on page 27). Or, you can replace this certificate by configuring a self-signed certificate (see "Configure HP Codar to use self-signed certificate" on page 30).

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.

Configure HP Codar to use 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 Codar. 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 Codar to use internal Certificate Authority-Signed certificate" on page 27.

"Step 1: Create a keystore and self-signed certificate" on the next page

"Step 2: Create a Certificate Signing Request" on page 23

"Step 3: Submit the certificate signing request to a Certificate Authority" on page 23

"Step 4: Import the Certificate Authority's root certificate" on page 23

"Step 5: Import Certificate Authority-Signed certificate" on page 24

"Step 6: Configure the web server" on page 25

"Step 7: Configure client browsers" on page 26

"Step 8: Test secure connections" on page 26

Note: In the following instructions, `CSA_HOME` is the directory in which HP Codar is installed (for example, on Windows, the directory is `C:\Program Files\Hewlett-Packard\Codar` and on Linux, the directory is `/usr/local/hp/codar`). 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 completing the following steps:

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

2. Run the following command:

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -genkeypair -alias codar_ca_signed
   -validity 365 -keyalg rsa -keysize 2048 -keystore
   .\jboss-as\standalone\configuration\.keystore_ca_signed
   ```

   Linux:

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

   `CSA_JRE_HOME` is the directory in which the JRE that is used by HP Codar 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 need 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 Codar 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 Codar.

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:

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -certreq -alias codar_ca_signed
   -file C:\codarcsr.txt -keystore .\jboss-as\standalone\configuration\.keystore_
   ca_signed
   ```

   Linux:

   ```
   CSA_JRE_HOME/bin/keytool -certreq -alias codar_ca_signed-file /tmp/codarcsr.txt
   -keystore ./jboss-as/standalone/configuration/.keystore_ca_signed
   ```

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 this example, it is assumed that the Certificate Authority's root certificate is named `codarca.crt`, the Certificate Authority-signed certificate is named `codar_ca_signed.crt`, and that both are located in `C:\` on Windows or `/tmp` on Linux.

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:

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -alias codarca -file C:\codarca.crt -
   trustcacerts -keystore "CSA_JRE_HOME\lib\security\cacerts"
   ```

   Linux:

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

3. When prompted enter the password for the keystore.

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

Step 5: Import Certificate Authority-Signed certificate

1. The Certificate Authority-signed certificate (`codar_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). 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:

     Windows:

     ```
     "CSA_JRE_HOME\bin\keytool" -importcert -alias codar_ca_signed
     -file C:\codar_ca_signed.crt -trustcacerts -keystore
     .\jboss-as\standalone\configuration\.keystore_ca_signed
     ```

     Linux:

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

Use the alias of the primary certificate (`codar_ca_signed`) and keystore name 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 web server

Configure the web server by completing the following steps:

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, follow the instructions at https://community.jboss.org/wiki/JBossAS7SecuringPasswords to create a password vault for JBoss.

   Note: If you are using the vault scripts, verify that the `JAVA_HOME` environment variable has been defined. Verify that `JAVA_HOME` has been set to the directory in which the JRE that is used by HP Codar is installed.

   Windows:

   If the directory path name includes a space, verify that the value has been enclosed in quotations marks. For example, to set `JAVA_HOME` to a directory path name that includes a space, from a command prompt, type
   `set JAVA_HOME="C:\Program Files\Hewlett-Packard\Codar\jre"`

> To verify that JAVA_HOME has been defined, from a command prompt, type:
> `echo %JAVA_HOME%`
>
> **Linux:**
>
> To verify that JAVA_HOME has been defined, from a command prompt, type:
> `echo $JAVA_HOME`

The following is an example of an encrypted password attribute using the JBoss password vault:

```
password="${VAULT::<vault_block_example>::password::N2NhZDzOMtES0ZGE4MmEtx0}"
```

4. Restart HP Codar service, see "Restart HP Codar" on page 81.

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 7: 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://<codarhostname>: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, see 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, see the browser's online documentation.

Step 8: Test secure connections

To test the connection to the HP Codar Console, on a client system, open a supported Web browser and navigate to `https://`*`<codarhostname>`*`:8444/csa` where *`<codarhostname>`* 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 Codar to use a Certificate Authority-signed certificate. If a certificate warning is displayed, review steps 1-7 to be sure they were followed as documented.

Configure HP Codar to use 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 Codar. 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:

"Step 1: Import the Certificate Authority's root certificate" below

"Step 2: Import internal Certificate Authority-Signed certificate" on the next page

"Step 3: Configure the web server" on the next page

"Step 4: Configure client browsers" on page 30

"Step 5: Test secure connections" on page 30

> **Note:** In the following instructions, `CSA_HOME` is the directory in which HP Codar is installed (for example, on Windows the directory is `C:\Program Files\Hewlett-Packard\Codar`) and on Linux the directory is `/usr/local/hp/codar`). The `keytool` utility is included with the JRE.

In this example, it is assumed that you are given an internal Certificate Authority-signed certificate (referred to as `codar_internalca_signed.crt`), an internal Certificate Authority's root certificate (referred to as `codarinternalca.crt`). Both certificates are located in C:\ on Windows or in /tmp on Linux.

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:

   On Windows:

```
"CSA_JRE_HOME\bin\keytool" -importcert -alias codarinternalca -file
C:\codarinternalca.crt -trustcacerts -keystore "CSA_JRE_
HOME\lib\security\cacerts"
```

On Linux:

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

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

3. When prompted enter the password for the keystore.

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

Step 2: Import internal Certificate Authority-Signed certificate

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

2. Run the following command:

   On Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -alias codar_internalca_signed
   -file C:\codar_internalca_signed.crt -trustcacerts -keystore
   .\jboss-as\standalone\configuration\.keystore_internalca_signed
   ```

   On Linux:

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

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

   Use this alias and keystore name when you configure the web server.

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

   Use this password when you configure the web server.

Step 3: Configure the web server

Configure the web server by completing the following steps:

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

2. Locate the following entry:

   ```
   <ssl name="ssl" key-alias="CODAR" certificate-key-file=
   "CSA_HOME\jboss-as\standalone\configuration\
   .keystore verify-client="false"/>
   ```

3. Add a new attribute named `password` with a value that corresponds to the password you selected for the keystore, change the name of the `key-alias` to the alias you used in step 2, and change the name of the `certificate-key-file` to the keystore you used in step 2.

   On Windows:

   ```
   <ssl name="ssl" key-alias="codar_self_signed" certificate-key-file="
   "CSA_HOME\jboss-as\standalone\configuration\
   .keystore_internalca_signed" password="keystorePassword"
   verify-client="false"/>
   ```

   On Linux:

   ```
   <ssl name="ssl" key-alias="codar_ca_signed" certificate-key-file=
   CSA_HOME/jboss-as/standalone/configuration/
   .keystore_ca_signed" password="keystorePassword"
   verify-client="false"/>
   ```

   Note: This example stores the password in clear text. If you want to use an encrypted password, follow the instructions at https://community.jboss.org/wiki/JBossAS7SecuringPasswords to create a password vault for JBoss.

   Note: If you are using the vault scripts, verify that the `JAVA_HOME` environment variable has been defined. Verify that `JAVA_HOME` has been set to the directory in which the JRE that is used by HP Codar is installed.

   Windows:

   If the directory path name includes a space, verify that the value has been enclosed in quotations marks. For example, to set `JAVA_HOME` to a directory path name that includes a space, from a command prompt, type
   `set JAVA_HOME="C:\Program Files\Hewlett-Packard\Codar\jre"`

   To verify that `JAVA_HOME` has been defined, from a command prompt, type:
   `echo %JAVA_HOME%`

   Linux:

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

The following is an example of an encrypted password attribute using the JBoss password vault:`password="${VAULT::`*`<vault_block_ example>`*`::password::N2NhZDzOMtES0ZGE4MmEtx0}"`

4. Restart the HP Codar service, see "Restart HP Codar" on page 81.

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 4: 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://<codarhostname>: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, see 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, see the browser's online documentation.

Step 5: Test secure connections

To test the connection to the HP Codar Console, on a client system, open a supported Web browser and navigate to `https://`*`<codarhostname>`*`:8444/csa` where *`<codarhostname>`* 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 Codar to use a Certificate Authority-signed certificate. If a certificate warning is displayed, review steps 1-4 to be sure they were followed as documented.

Configure HP Codar to use self-signed certificate

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

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

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

You should perform the following general steps:

"Step 1: Create a keystore and self-signed certificate" below

"Step 2: Export the self-signed certificate" on the next page

"Step 3: Import self-signed certificate as a trusted certificate" on page 33

"Step 4: Configure web server" on page 33

"Step 5: Configure client browsers (optional)" on page 34

"Step 6: Test secure connections" on page 34

> **Note:** In the following instructions, `CSA_HOME` is the directory in which HP Codar is installed (for example, on Windows, the directory is `C:\Program Files\Hewlett-Packard\Codar`) and on Linux the directory is `/usr/local/hp/codar`). The `keytool` utility is included with the JRE.

Step 1: Create a keystore and self-signed certificate

Create a self-signed certificate by completing the following steps:

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

   Windows:

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

   Linux:

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

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

Step 2: Export the self-signed certificate

Export the self-signed certificate completing the following steps:

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

2. Run the following command:

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -export -alias codar_self_signed
   -file C:\codar_self_signed.crt
   -keystore .\jboss-as\standalone\configuration\
   .keystore_self_signed
   ```

   Linux:

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

`CSA_JRE_HOME` is the directory in which the JRE that is used by HP Codar is installed

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

Step 3: Import self-signed certificate as a trusted certificate

This step configures the JRE to trust the self-signed certificate. Import the self-signed certificate by completing the following steps:

1. Open a command prompt.

2. Run the following command:

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -alias codar_self_signed
   -file C:\codar_self_signed.crt -trustcacerts
   -keystore "CSA_JRE_HOME\lib\security\cacerts"
   ```

   Linux:

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

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

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

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

Step 4: Configure web server

Configure the web server by completing the following steps:

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.

   Windows:

   ```
   <keystore path="<CSA_HOME>\jboss-as\standalone\configuration\.keystore_self_
   signed" keystore-password="keystorePassword"
   alias="csa_self_signed"/>
   ```

   Linux:

   ```
   <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, follow the instructions at https://community.jboss.org/wiki/JBossAS7SecuringPasswords to create a password vault for JBoss.

3. Restart the HP Codar service, see "Restart HP Codar" on page 81.

4. 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 (optional)

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

- **Microsoft Internet Explorer** and **Chrome**: From Windows Explorer, double-click on the `codar_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, see the browser's online documentation.

- **Firefox**: Add an exception by opening the browser and navigating to `https://<codarhostname>:8444/csa` where *`<codarhostname>`* is the fully-qualified domain name of the system on which HP Codar 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, see the browser's online documentation.

Step 6: Test secure connections

To test the connection to the HP Codar Console, on a client system, open a supported Web browser and navigate to `https://<codarhostname>:8444/csa` where *`<codarhostname>`* 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 Codar to use a Certificate Authority-signed certificate. If any other certificate warning is displayed, review steps 1-5 to be sure they were followed as documented.

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 Codar. 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.

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -trustcacerts -alias ldap
   -keystore "CSA_JRE_HOME\lib\security\cacerts"
   -file <c:\certfile_name.crt> -storepass <password>
   ```

   Linux:

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

   `<c:\certfile_name.crt>` on Windows or `</tmp/certfile_name.crt>` on Linux 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 Codar service, see "Restart HP Codar" on page 81.

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 Codar. 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.

   Windows:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -trustcacerts -alias smtp
   -keystore "CSA_JRE_HOME\lib\security\cacerts"
   -file <c:\certfile_name.crt> -storepass <password>
   ```

   Linux:

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

   `<c:\certfile_name.crt>` on Windows or `</tmp/certfile_name.crt>` on Linux 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 Codar service, see "Restart HP Codar" on page 81.

Configure secure connections for 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 Codar to check the database DN, complete the following steps:

     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>
     ```

     `<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 Codar.

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

B. On the HP Codar 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.

On Windows:

```
"CSA_JRE_HOME\bin\keytool" -importcert -trustcacerts
-alias oracledb
-keystore "CSA_JRE_HOME\lib\security\cacerts"
-file <c:\certfile_name.crt> -storepass <password>
```

On Linux:

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

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

`<c:\certfile_name.crt>` on Windows or `</tmp/certfile_name.crt>` on Linux 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`.

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

D. Press **Enter**.

E. Restart HP Codar, see "Restart HP Codar" on page 81.

- If you want to configure HP Codar to check the database DN, complete the following steps:

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>
```

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

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 Codar.

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

B. On the HP Codar 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.

On Windows:

```
"CSA_JRE_HOME\bin\keytool" -importcert -trustcacerts
-alias oracledb
-keystore "CSA_JRE_HOME\lib\security\cacerts"
-file <c:\certfile_name.crt> -storepass <password>
```

On Linux:

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

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

`<c:\certfile_name.crt>` on Windows or `</tmp/certfile_name.crt>` on Linux 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`.

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

D. Press **Enter**.

E. Restart HP Codar, see "Restart HP Codar" on page 81.

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

   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>" />
   ```

   `<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` on Windows or `CSA_HOME/jboss-as/standalone/configuration/.keystore` on Linux).

   `<certificate_key_file_password>` is the password to the keystore file.

   `<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 Codar'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 Codar.

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

   b. On the HP Codar 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.

      On Windows:

      ```
      "CSA_JRE_HOME\bin\keytool" -importcert -trustcacerts
      -alias mssqldb -keystore "CSA_JRE_HOME\lib\security\cacerts"
      -file <c:\certfile_name.crt> -storepass <password>
      ```

      On Linux:

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

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

      `<c:\certfile_name.crt>` on Windows or `</tmp/certfile_name.crt>` on Linux 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`.

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

   d. Press **Enter**.

   e. Restart HP Codar, see "Restart HP Codar" on page 81.

Configure secure connections for HP Operations Orchestration Load Balancer

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

For each system running HP Codar, import the root certificate of HP Operations Orchestration Load Balancer's Certificate Authority into HP Codar (you must first export HP Operations Orchestration

Load Balancer's certificate from HP Operations Orchestration Load Balancer's truststore and then import it into HP Codar's truststore).

1. Open HP Operations Orchestration Load Balancer in a Web browser (using https).

2. Export the certificate from the Web browser.

   If you are using a Chrome web browser, complete the following steps:

   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 Operations Orchestration Load Balancer on the same system as HP Codar, select the `CSA_JRE_HOME\lib\security` directory, enter **paslb.cer** as the file name, and click **Save**.

            - If you are running HP Operations Orchestration Load Balancer on a system that is not running HP Codar, 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, complete the following steps:

   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 Operations Orchestration Load Balancer on the same system as HP Codar, select the `CSA_JRE_HOME\lib\security` directory, enter **paslb.cer** as the file name, select **X.509 Certificate (PEM)** as the Type, and click **Save**.

        - If you are running HP Operations Orchestration Load Balancer on a system that is not running HP Codar, 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**.

   v. Click **Cancel**.

If you are using a Windows IE web browser, complete the following steps:

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 Operations Orchestration Load Balancer on the same system as HP Codar, select the `CSA_JRE_HOME\lib\security` directory, enter **paslb.cer** as the file name, and click **Save**.

         - If you are running HP Operations Orchestration Load Balancer on a system that is not running HP Codar, 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 Operations Orchestration Load Balancer on a system that is not running HP Codar, copy the `paslb.cer` file to the `CSA_JRE_HOME\lib\security` directory on the system running HP Codar.

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

   Windows:

   ```
   cd "CSA_JRE_HOME\lib\security"

   ..\..\bin\keytool -importcert -alias paslb -file paslb.cer
   -keystore cacerts -storepass <password>
   ```

   Linux:

   ```
   cd CSA_JRE_HOME/lib/security

   ../../bin/keytool  -importcert -alias paslb -file paslb.cer
   -keystore cacerts -storepass <password>
   ```

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

HP Operations Orchestration

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

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

In this release, you can install HP Operations Orchestration with HP Codar using the HP Codar 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 Codar, you may have configured multiple instances of HP Operations Orchestration for sequential designs. If you have upgraded from an earlier version of HP Codar 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 Codar that uses only a single instance of HP Operations Orchestration or are installing HP Codar 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
- "Integrate with HP Operations Orchestration " on page 53

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 Codar Installation and Configuration Guide* or *HP Codar Upgrade Guide* to configure HP Operations Orchestration, you should have already completed the tasks in this section to configure HP Operations Orchestration.

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

- "Configure internal user" on the next page
- "Deploy content packs" on page 46
- "Configure HP Single Sign-On between HP Codar and HP Operations Orchestration" on page 46

- "Configure HP Operations Orchestration properties in csa.properties file" on page 48
- "Configure secure connection between HP Codar and HP Operations Orchestration" on page 49
- "Run component tool" on page 49

Note: In the following instructions, `CSA_HOME` is the directory in which HP Codar is installed and `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 Codar System and Software Support Matrix*.

Configure internal user

Internal users can be used to configure HP Operations Orchestration for HP Codar. The user in these instructions is used for provisioning topology designs.

To configure an internal user, complete the following steps:

1. Log in to HP Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security** > **Internal Users**.
4. Click the **Add** button.
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. When HP Operations Orchestration is launched from the HP Codar 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. 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 the **Content Management** button.

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

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

4. In the Deploy New Content dialog, click the **Add files for deployment** icon.

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

6. Click the Add files for deployment icon.

7. Navigate to the `CSA_HOME\Tools\ComponentTool\contentpacks\` directory, select all the content packs, and click **Open**.

8. Click **Deploy**.

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

9. When the deployment succeeds, click Close to close the dialog.

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

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

HP Codar 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 Codar and HP Operations Orchestration, this user can be used for single sign-on. That is, if you are logged in to HP Codar as the admin user, you can launch HP Operations Orchestration from the HP Codar 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 Codar and the embedded HP Operations Orchestration to use the same LDAP source or, if HP Codar and the embedded HP Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the HP Codar user must be assigned to the Codar 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 Single Sign-On between HP Codar and HP Operations Orchestration, the systems on which HP Codar and HP Operations Orchestration are installed must be in the same domain.

Configure and enable HP Single Sign-On

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

1. Log in to HP Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security > SSO**.
4. Select the **Enable** check box.
5. Enter the **InitString**. This is the value to which the crypto InitString attribute is set in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEBINF\hpssoConfiguration.xml` file.

   For example, if the entry in the file is `crypto InitString="lOJisF9Slbf79hmLsd"`, copy `lOJisF9Slbf79hmLsd` to this field. 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 Codar 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 Codar and HP Operations Orchestration to use the same LDAP source or, if HP Codar and HP Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the HP Codar user and the HP Operations Orchestration user must be assigned any role that allows flows to be viewed.

For more information on configuring LDAP in HP Operations Orchestration, see the *HP Operations Orchestration Central Help*.

Note: One of the LDAP servers must be set to default in HP Operations Orchestration so that HP Codar can launch the HP Operations Orchestration page. Otherwise, an "access denied" error occurs.

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

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**.

Configure HP Operations Orchestration properties in 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 HP Codar 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 (HP Operations Orchestration version 10.21). Set this URL to the system on which HP Operations Orchestration version 10.21 is installed. For example, `https://<hostname>:8443`.
OOS_USERNAME	The username used to log in to HP Operations Orchestration Central. Set this username to admin.
OOS_PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log in to HP Operations Orchestration Central. Set this property to the encrypted value of the user defined in `OOS_USERNAME` (see "Encrypt password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

Configure secure connection between HP Codar 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).

Run component tool

The component tool imports the HP Operations Orchestration flows from the content packs installed with HP Codar (used only with HP Operations Orchestration version 10.21).

To run the component tool, complete the following steps:

1. Open a command prompt and change the directory to `CSA_HOME\Tools\ComponentTool`.

2. Generate the sample database properties files. Run the following command:

   Windows:

   ```
   "CSA_JRE_HOME\bin\java" -jar component-tool.jar -g
   ```

   Linux:

   ```
   CSA_JRE_HOME/bin/java -jar component-tool.jar -g
   ```

3. Make a copy of the appropriate sample database properties file, rename it to `config.properties`, and update the content, as needed.

Property Name	Description

jdbc.driverClassName	The JDBC driver class.
	Example
	`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.
	Example
	`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 example below).
	Example
	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 Codar 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 Codar 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/codardb`

Property Name	Description
jdbc. username	The user name of the database user you configured for HP Codar after installing the database.
jdbc. password	The password for the database user. The password should be encrypted (see the "Encrypt password" on page 82 for instructions on encrypting passwords). **Example** `jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)`

Example `config.properties` content

Oracle, TLS not enabled

```
jdbc.driverClassName=oracle.jdbc.driver.OracleDriver
jdbc.dialect=org.hibernate.dialect.OracleDialect
jdbc.databaseUrl=jdbc:oracle:thin:@127.0.0.1:1521:XE
jdbc.username=codar
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

MS SQL, TLS not enabled

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request
jdbc.username=codar
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

MS SQL, TLS enabled

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate
jdbc.username=codar
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

PostgreSQL

```
jdbc.driverClassName=org.postgresql.Driver
jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect
jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/codardb
jdbc.username=codardbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
```

4. Run the component tool:

- **Oracle**

  Windows:
  ```
  "CSA_JRE_HOME\bin\java" -jar component-tool.jar -c config.properties
  -cp contentpacks -m mappingFiles -me metainfo.txt -j <jdbc_driver_
  directory>\ojdbc.jar
  ```

  Linux:
  ```
  CSA_JRE_HOME/bin/java -jar component-tool.jar -c config.properties
  -cp contentpacks -m mappingFiles -me metainfo.txt -j <jdbc_driver_
  directory>/ojdbc.jar
  ```

- **MS SQL and PostgreSQL**

  Windows:
  ```
  "CSA_JRE_HOME\bin\java" -jar component-tool.jar -c config.properties
  -cp contentpacks -m mappingFiles -me metainfo.txt
  ```

  Linux:
  ```
  CSA_JRE_HOME/bin/java -jar component-tool.jar -c config.properties
  -cp contentpacks -m mappingFiles -me metainfo.txt
  ```

> **Note:** Do not edit the `metainfo.txt` file or the `contentpacks` and `mappingFiles` directories.

Integrate with HP Operations Orchestration

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

- "Add JRE to system path" on the next page
- "Install HP Codar content pack " on page 55
- "Configure internal users" on page 55
- "Deploy content packs required by HP Codar" on page 56
- "Set up system accounts for HP Codar content pack" on page 57
- "Set up system properties for HP Codar content pack" on page 58
- "Configure HP Single Sign-On between HP Codar and HP Operations Orchestration" on page 58
- "Configure secure connection between HP Codar and HP Operations Orchestration" on page 60

> **Note:** In the following instructions, `CSA_HOME` is the directory in which HP Codar is installed and

`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 Codar System and Software Support Matrix*.

Add JRE to system path

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

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

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

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

   ```
   ICONCLUDE_HOME\java\bin
   ```

   or

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

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

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

Open a shell and enter one of the following commands:

- If HP Operations Orchestration and HP Codar are installed on the same system, enter this command:

  ```
  export PATH=$PATH:$ICONCLUDE_HOME/java/bin
  ```
- If HP Operations Orchestration and HP Codar are installed on different systems, enter this

command:

```
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 Codar (depending on the path you configured and if it is the only path or the first path set to a JRE in the system path). If you need to run another JRE with an application, you must type in the relative path to that JRE in order to run it (for example, when you configure TLS).

Install HP Codar content pack

If HP Codar 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` file from the HP Codar system to the HP Operations Orchestration system (where `CSA_HOME` is the directory in which HP Codar is installed).

Configure internal users

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

To configure an internal user, complete the following steps:

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	codaroouser
Password	cloud
Roles	ADMINISTRATOR, SYSTEM, ADMIN

   The codaroouser 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. Enable authentication by selecting the **Enable Authentication** check box.
8. Click **OK** in the confirmation dialog.
9. Click the **Add** button.
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. When HP Operations Orchestration is launched from the HP Codar 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. Enable authentication by selecting the **Enable Authentication** check box.
13. Click **OK** in the confirmation dialog.
14. Log out of HP Operations Orchestration Central and log back in as the codaroouser.

Deploy content packs required by HP Codar

To deploy content packs required by HP Codar, complete the following steps:

1. Log in to HP Operations Orchestration Central.
2. Click the **Content Management** button.
3. Click the **Content Packs** tab.
4. Click the **Deploy New Content** icon.
5. In the **Deploy New Content** dialog, click the **Add files for deployment** icon.
6. Click the **Deploy New Content** icon.
7. Click the **Add files for deployment** icon.
8. Navigate to the `CSA_HOME/CSAKit-4.2/OOFlowContent/10X` directory, select all content packs to

be deployed, and click **Open**.

9. Click **Deploy**.

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

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

Set up system accounts for HP Codar content pack

Set up system accounts for the HP Codar content pack by completing the following steps:

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

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

> **Note:** The **User Name** configured for the CSA_REST_CREDENTIALS System Account setting must match the **Override Value** (HP Operations Orchestration version 10.21) configured for the CODAR_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
Passwords	<*leave_blank*>_

9. Click **Save**.

Set up system properties for HP Codar content pack

Set up the following system properties for the HP Codar content pack by completing the following steps:

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

Field	Recommended value
Name	`CSA_REST_URI`
Override Value	https://<*codar_hostname*>:8444/csa/rest

6. Click **Save**.

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

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

HP Codar 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 Codar and HP Operations Orchestration, this user can be used for single sign-on. That is, if you are logged in to HP Codar 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 Codar and the embedded HP Operations Orchestration to use the name LDAP source or, if HP Codar and the embedded HP Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the HP Codar user must be signed to the Codar 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 Single Sign-On between HP Codar and HP Operations Orchestration, the systems on which HP Codar and HP Operations Orchestration are installed must be in the same domain.

Configure and enable HP Single Sign-On

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

1. Log in to HP Operations Orchestration Central.
2. Click the **System Configuration** button.
3. Select **Security > SSO**.
4. Select the **Enable** check box.
5. Enter the **InitString**. This is the value to which the `crypto InitString` attribute is set in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\hpssoConfiguration.xml` file. For example, if the entry in the file is `cryptoInitString="lOJisF9Slbf79hmLsd"`, copy `lOJisF9Slbf79hmLsd` to this field. 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 Codar 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 Codar and HP Operations Orchestration to use the same LDAP source or, if HP Codar and HP Operations Orchestration use different LDAP sources, configure the same users in both sources. In either case, the HP Codar user and the HP Operations Orchestration user must be assigned any role that allows flows to be viewed.

For more information on configuring LDAP in HP Operations Orchestration, see the *HP Operations Orchestration Central Help*.

Note: One of the LDAP servers must be set to default in HP Operations Orchestration so that HP Codar can launch the HP Operations Orchestration page. Otherwise, an "access denied" error occurs.

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

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**.

Configure secure connection between HP Codar 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).

HP Codar Console

This chapter provides information about the tasks needed to prepare and set up the HP Codar Console in order to start using HP Codar. You must complete the required tasks before you can start to use the HP Codar Console. Organization roles provide authorization for members to perform these tasks.

The roles and tasks are included in the following topics:

- "Roles in HP Codar" below
- "Configure provider organization" on the next page (required)
- "Add software license" on page 63 (required)
- "Proxy configuration for resource providers outside the internal network" on page 63 (optional)
- "Customize HP Codar Console dashboard" on page 66 (optional)
- "Customize HP Codar Console title" on page 78 (optional)

Roles in HP Codar

The HP Codar roles are configured and assigned by the administrator. Users with the Administrator role have access to all areas.

Application Architect role

Users with this role can

- Create packages.
- View packages in any stage.
- Deploy, update, and delete packages in Development stage only.
- Embrace components.
- Create, update, and delete applications and application versions.

Users with this role cannot promote or reject packages in any stage.

Application Developer role

Users with this role can:

- Create packages.
- View packages in any stage.
- Deploy, update, and delete packages in Development stage only.
- Promote packages from Development to Testing stage.

Application QA role

Users with this role can:

- View packages in any stage.
- Deploy, update, reject, and delete packages in Testing stage.
- Promote packages from Testing to Staging stage.
- Deploy, update, reject, and delete packages in Staging stage.

Application Release Manager role

Users with this role can:

- View packages in any stage.
- Deploy, update, reject, and delete packages in Staging stage.
- Promote packages from Staging to Production stage.
- Deploy, update, reject, and delete packages in Production stage.

Application Integration role

Users with this role:

• Can be used to integrate HP Codar with external systems.

• Will not be able to use any functionality in the UI or use any APIs.

Configure provider organization

1. Launch the HP Codar Console by typing the following URL in a supported web browser: `https://`*`<codarhostname>`*`:8444/csa` where *`<codarhostname>`* is the fully-qualified domain

name of the system on which the HP Codar Console resides.

2. Log in to the HP Codar Console as an Administrator (see the *HP Codar Concepts Guide* and *HP Codar Console Help* for more information about the Codar 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 (CODAR-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). For details about the fields in each section, see the *HP Codar Console Help*.

Add software license

HP Codar version 1.50 requires a software license. HP Codar licensing is based on the number of operating system instances (OSIs) being used in current, active subscriptions.

After initial installation of HP Codar version 1.50, when you log in to the HP Codar 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 you upgrade to HP Codar version 1.50, when you log in to the HP Codar Console, all HP Codar version 1.00 licenses are valid and are automatically added.

Before you can add a software license, you must request a license using the licensing portal. See "Request software licenses" on page 15.

For more information about managing HP Codar licenses, see the *HP Codar 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 Codar 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 Codar - 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 Codar and HP Operations Orchestration, complete the following steps:

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

   On Windows:

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

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

   rem # HTTP/HTTPS hosts not handled by the proxy
   set "JAVA_OPTS=%JAVA_OPTS% -
   Dhttp.nonProxyHosts=mycodarserver^^^|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.

   On Ubuntu Linux:

   ```
    # 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=mycodarserver\|localhost\|127.*|10.*"
```

<*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 ^^^| on Windows or \| on Linux is the separator used when defining more than one non-proxy host.

Red Hat Enterprise Linux

In the if-else block, 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=localhost\|127.*\|10.* "
```

<*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 Codar service, see "Restart HP Codar" on page 81.

5. If you have integrated with HP Operations Orchestration version 10.21, 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	`CODAR_Proxy_Host`
Override Value	The fully-qualified domain name of the proxy server.
Name	`CODAR_Proxy_Port`
Override Value	The port used to communicate with the proxy server.

f. Click **Save**.

Customize HP Codar Console dashboard

The HP Codar 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 predefined custom tile" below
- "Creating dashboard tile" on page 68
- "Adding secondary dashboard" on page 73
- "Modifying dashboard tile" on page 76
- "Disabling dashboard tile" on page 76

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

A disabled predefined custom tile definition, disabled sample tile definitions, and a disabled sample secondary dashboard definition are provided in HP Codar 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 predefined custom tile

By default, HP Codar 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 Codar.

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

If you are not upgrading from an older version of HP Codar, 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 Codar, do the following:

1. Create a folder called `custom-content` in the `CSA_HOME\jboss-as\standalone\deployments\csa.war` directory. 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.

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 HP Codar Console to view the tile. If you are already logged in, log out and log back in. 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, see "Creating dashboard tile" on the next page.

Enabling other predefined dashboard tiles

HP Codar 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.

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 HP Codar Console to view the tile. If you are already logged in, log out and log back in.

   To modify the tile, see "Creating dashboard tile" below.

Creating dashboard tile

The HP Codar 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 HP Codar 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 secondary dashboard" on page 73 for more information about how to add a secondary dashboard.

To create a HP Codar Console dashboard tile, complete the following steps:

1. Make a backup of the `CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json` dashboard configuration file.

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 HP Codar Console dashboard. The second tile definition is the Resources tile and it is the second tile displayed in the HP Codar 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\common` 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\common` 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.

Attribute	Description
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**.
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 **/codar/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 **/codar/administration/index.jsp**.

Attribute	Description
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 to display the tile in the dashboard. Only the Administrator and Application Architect roles have access to the Design tile and the migration feature to enable an HP-compatible product in the HP Codar Console. Users with other roles can access designs in the Release Pipeline tile if they have been granted access. 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, "ADMINISTRATOR", "APPLICATION_ARCHITECT"). If no roles are specified, the tile can be seen by all users. Values include: ○ **ADMINISTRATOR** - The Administrator role has access to all functionality in the HP Codar Console. ○ **APPLICATION_ARCHITECT** - The Application Architect role can create packages, view packages in any stage; deploy, update, and delete packages in the Development stage only; embrace components; create, update, and delete applications and application versions. The Application Architect cannot promote packages from Development to Testing stage. ○ **APPLICATION_DEVELOPER** - The Developer role can create packages, view packages in any stage; deploy, update, and delete packages in Development stage only; and promote packages from Development to Testing stage. ○ **APPLICATION_QA** - The QA role can view packages in any stage; deploy, update, and delete packages in Testing stage; promote packages from Testing to Staging stage; and deploy, update, reject, and delete packages in the Staging stage. ○ **APPLICATION_RELEASE_MANAGER** - The Release Manager role can view packages in any stage; deploy, update, and delete packages in the Staging stage; promote packages from Staging to Production stage; deploy, update, reject, and delete packages in Production stage. ○ **INTEGRATION_USER** - The Integration user Architect role can create packages, view packages in any stage; deploy, update, and delete packages in all stages. See "Roles in HP Codar" in the *HP Codar Console Help* for more information about these roles.

c. Save and exit the file.

3. Log in to the HP Codar Console to view the tile. If you are already logged in, log out and log back in.

Adding secondary dashboard

Tiles in the HP Codar Console dashboard can be configured to launch a secondary dashboard. For example, in the default configuration of the HP Codar 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 HP Codar 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, complete the following steps:

1. Make a backup of the `CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json` dashboard configuration file.

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 dashboard tile" on page 68).

   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 dashboard tile" on page 68).

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\common\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 Codar and successfully logging into the HP Codar 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 to display the tile in the dashboard. Only the Administrator and Application Architect roles have access to the Design tile and the migration feature to enable an HP-compatible product in the HP Codar Console. Users with other roles can access designs in the Release Pipeline tile if they have been granted access. 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, "ADMINISTRATOR", "APPLICATION_ARCHITECT"). If no roles are specified, the tile can be seen by all users. Values include: ○ **ADMINISTRATOR** - The Administrator role has access to all functionality in the HP Codar Console. ○ **APPLICATION_ARCHITECT** - The Application Architect role can create packages, view packages in any stage; deploy, update, and delete packages in the Development stage only; embrace components; create, update, and delete applications and application versions. The Application Architect cannot promote packages from Development to Testing stage. ○ **APPLICATION_DEVELOPER** - The Developer role can create packages, view packages in any stage; deploy, update, and delete packages in Development stage only; and promote packages from Development to Testing stage. ○ **APPLICATION_QA** - The QA role can view packages in any stage; deploy, update, and delete packages in Testing stage; promote packages from Testing to Staging stage; and deploy, update, reject, and delete packages in the Staging stage. ○ **APPLICATION_RELEASE_MANAGER** - The Release Manager role can view packages in any stage; deploy, update, and delete packages in the Staging stage; promote packages from Staging to Production stage; deploy, update, reject, and delete packages in Production stage. ○ **INTEGRATION_USER** - The Integration user Architect role can create packages, view packages in any stage; deploy, update, and delete packages in all stages. See "Roles in HP Codar" in the *HP Codar Console Help* for more information about these roles.

Attribute	Description
tiles	Tile definition. At least one tile must be configured (see "Creating dashboard tile" on page 68.

d. Save and exit the file.

3. Log in to the HP Codar Console to view the dashboard. If you are already logged in, log out and log back in.

Modifying dashboard tile

To modify an existing dashboard tile, edit the `CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json` file:

1. Locate the tile definition that you want to modify.

2. Update one or more attributes. For a description of the attributes, see "Creating dashboard tile" on page 68.

3. Save and exit the file.

Disabling dashboard tile

To disable a dashboard tile, edit the `CSA_HOME\jboss-as\standalone\deployments\csa.war\dashboard\config.json` file:

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", "CODAR_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 HP Codar Console font

The font used by the HP Codar Console can be customized. You can change the font if you are a user who has access to the system on which HP Codar is running. To change the font, on the system running HP Codar, do the following:

1. Open the `CSA_HOME\jboss-as\standalone\deployments\csa.war\custom\custom.css` file in a text editor.

2. At the end of the file, add the following:

   ```
   html, body {
   font-family: <font_name>;
   }
   ```

   <font_name> is the font used by the HP Codar 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. Restart HP Codar service, see "Restart HP Codar" on page 81.

Customize HP Codar Console title

The HP Codar Console title appears at the top of the HP Codar Console next to the HP logo. By default, the title is "HP Codar."

You can change the title if you are a user who has access to the system on which HP Codar is running. To change the title, on the system running HP Codar, complete the following:

1. Open the `CSA_HOME\jboss-as\standalone\deployments\csa.war\custom\messages.properties` file in a text editor.

2. Add the following attribute and value:

   `codar_title=`<*title*>

   <*title*> is the title that displays at the top of the HP Codar Console.

   For example, to change the title to "HP CloudSystem," add the following to the file:

   ```
   codar_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.

Common HP Codar tasks

This chapter provides information on how to perform common HP Codar tasks.

Tasks include:

- "Launch HP Codar Console" below
- "Start HP Codar" below
- "Stop HP Codar" on the next page
- "Restart HP Codar" on the next page
- "Encrypt password" on page 82
- "Clear web browser cache" on page 83
- "Uninstall HP Codar" on page 83

Launch HP Codar Console

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

Launch the HP Codar Console using an IPv6address by typing the following URL in a supported web browser:

```
https://<ipv6_address>:8444/csa/login
```

Start HP Codar

To start HP Codar on Windows, complete the following steps:

1. On the server that hosts HP Codar, navigate to **Start** > **Administrative Tools** > **Services**.
2. Right-click on the HP Codar service and select **Start**.
3. If you installed an embedded HP Operations Orchestration instance, right-click on the HP Operations Orchestration Central service and select **Start**.

To start HP Codar on Linux, complete the following steps:

1. On the server that hosts HP Codar, type the following:

   ```
   service codar start
   ```

2. If you installed an embedded HP Operations Orchestration instance, as the root user (the HP Operations Orchestration Central service must be started as the root user because an HP Matrix Operating Environment flow needs to write to the root directory), type:

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

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

Stop HP Codar

To stop HP Codar on Windows, complete the following steps:

1. On the server that hosts HP Codar, navigate to **Start** > **Administrative Tools** > **Services**.

2. Right-click on the HP Codar service and select **Stop**.

3. If you installed an embedded HP Operations Orchestration instance, right-click on the HP Operations Orchestration Central service and select **Stop**.

To stop HP Codar on Linux, complete the following steps:

1. Type the following command on the server that hosts HP Codar:

   ```
   service codar stop
   ```

2. If you installed an embedded HP Operations Orchestration instance, as the root user, type:

   `<embeddedHPOOinstallation>/central/bin/central stop`.

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

Restart HP Codar

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

1. On the server that hosts HP Codar, navigate to **Start** > **Administrative Tools** > **Services**.

2. Right-click on the HP Codar service and select **Restart**.

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

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

1. On the server that hosts HP Codar, type the following:

   ```
   service codar restart
   ```

2. If you installed an embedded HP Operations Orchestration instance, as the root user, type:

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

   For example, type

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

Encrypt password

Encrypt a password for use with HP Codar configuration only.

To encrypt a password, complete the following steps:

1. Open a command prompt and change to the `CSA_HOME\Tools\PasswordUtil` directory. For example:

   Windows:

   ```
   C:\Program Files\Hewlett-Packard\Codar\Tools\PasswordUtil
   ```

   Linux:

   ```
   /usr/local/hp/codar/Tools/PasswordUtil
   ```

2. Run the following command:

   Windows:

   ```
   "CSA_JRE_HOME\bin\java" -jar passwordUtil-standalone.jar encrypt <myPassword>
   ```

   If you used different names for the keystore, alias, or encrypted symmetric key file, here is an example of the command without using the example names:

   ```
   "CSA_JRE_HOME\bin\java" -jar "CSA_HOME\Tools\PasswordUtil\passwordUtil-
   standalone.jar" encrypt <password> JsafeJCE <HP Codar encryption keystore>
   <HP Codar encryption keystore password>
   <HP Codar encryption keystore alias>
   <location and name of the encrypted symmetric key>
   ```

Note: If you use path separators in the `passwordUtil-standalone.jar` script options, use either a single forward slash (/) or double backward slashes (\\) as your path separator.

Linux:

```
CSA_JRE_HOME/bin/java -jar passwordUtil-standalone.jar encrypt <myPassword>
```

Clear web browser cache

It may be necessary to clear your web browser cache on systems that previously accessed the HP Codar Console after upgrading HP Codar.

Uninstall HP Codar

Uninstalling HP Codar removes the `CSA_HOME` directory and all of its contents. If all the contents in `CSA_HOME` are not deleted, you must manually delete them and the `CSA_HOME` directory.

If you installed an embedded HP Operations Orchestration instance with HP Codar (you installed HP Operations Orchestration with HP Codar using the HP Codar installer), the embedded HP Operations Orchestration instance is removed. If you are using HP Codar with an external HP Operations Orchestration instance (you installed HP Operations Orchestration separately from HP Codar), the external HP Operations Orchestration instance is not removed.

Note: The HP Codar database is NOT updated or uninstalled.

Uninstall HP Codar on Windows

To uninstall HP Codar on Windows, complete the following steps:

1. Log in as the user who installed HP Codar (for example, `codaruser`).
2. Stop the .HP Codar service:
   a. On the server that hosts HP Codar, navigate to **Start >Administrative Tools > Services**.
   b. Right-click on the HP Codar service and select **Stop**.
   c. If you installed an embedded HP Operations Orchestration instance, right-click on the HP Operations Orchestration Central service and select **Stop**.
3. Verify that the services were stopped.

If the HP Codar service is still running, open a command prompt, navigate to `CSA_HOME\jboss-as\bin`, and run the following command:

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

4. Close all instances of Windows Explorer, close all command prompts, and exit all programs that are running on the system.
5. Navigate to **Control Panel > Uninstall a program**.
6. Right-click on **HP Codar** and select **Uninstall/Change**.
7. Click **Uninstall**.
8. Delete the `CSA_HOME` directory and any remaining contents, if they exist.
9. If they exist, delete all HP Codar entries from the following file:

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

Uninstall HP Codar on Linux

To uninstall HP Codar on Linux, complete the following steps:

1. Log in as the user who installed HP Codar (for example, `codaruser`).
2. Stop the HP Codar service, by typing:

   ```
   service codar stop
   ```

3. If you installed an embedded HP Operations Orchestration instance, as the root user, type:

   <embeddedHPOOinstallation>`/central/bin/central stop`.

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

4. Verify that the services were stopped. For example, if HP Codar was installed in `/usr/local/hp/codar`, enter the following:

   ```
   ps -ef | grep /usr/local/hp/codar
   ps -ef | grep central
   ```

   If there are HP Codar or HP Operations Orchestration services running, repeat step 2 or kill the HP Codar and HP Operations Orchestration services.

5. Go to the `CSA_HOME/_HP_CODAR_1_50_0_installation` directory, and enter the following:

   ```
   cd CSA_HOME/_HP_CODAR_1_50_0_installation
   ```

6. Uninstall HP Codar. Enter the following:

   ```
   ./Change\ HP\ Cloud\ Service\ Automation\ Installation
   ```

7. Confirm that you want to uninstall HP Codar.

8. 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 Codar service scripts. Enter the following:

      ```
      rm /etc/init.d/codar
      ```

   c. If they exist, delete all HP Codar entries from the following file:

      ```
      /home/codaruser/.com.zerog.registry.xml
      ```

   d. Optionally, remove the `codaruser` user and `codargrp` group.

User administration

This chapter provides information for additional administration and configuration tasks.

Tasks include:

- "Allow non-administrator users to start and stop HP Codar service on Windows" below (optional)
- "Allow HP Codar service to be run as non-administrator user on Windows" on page 88 (optional)
- "Change HP Codar out-of-the-box user accounts for Windows and Linux" on page 92 (optional)

Allow non-administrator users to start and stop HP Codar service on Windows

When running HP Codar on Windows, by default, only users with administrator privileges can start or stop the HP Codar services. This procedure explains how to grant permissions to non-administrator users to start and stop these services. This process involves the following tasks:

- Create a non-administrator user account, if one does not exist.
- Determine the security identifier (SID) of the non-administrator user.
- Set the security descriptor for the services to allow the non-administrator user to start and stop them.
- Add necessary permissions to the HP Codar installation directory for the non-administrator user.

Allow non-administrator users to start and stop HP Codar service

To allow non-administrator users to start and stop the HP Codar service, complete the following steps:

1. Start the Control Panel on the HP Codar system and click **Add or remove user accounts** that is under **User Accounts**.
2. Click **Create a new account** in the Manage Accounts window that appears.
3. Enter a name for the user, select the **Standard user** radio button if it is not selected, and then click the **Create Account** button to create the user account.

   In this procedure we will use the user account name "CODARUser."

4. Open a command prompt window and run the following command, as is applicable, to display the security descriptor for the HP Codar service:

   ```
   sc sdshow codar
   ```

   The command returns a security descriptor in Security Descriptor Definition Language (SDDL), like the following example for the HP Codar service:

   ```
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
   (A;;CCLCSWLOCRRC;;;IU)(A;;;CCLCSWLOCRRC;;;SU)S:
   (AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
   ```

5. Copy the security descriptor that was returned by the above command to a text editor such as Notepad.

6. Run the following command to display the names and SIDs for all existing user accounts:

   ```
   wmic useraccount get name,sid
   ```

7. From the command output, copy the SID for the non-administrator user to the text editor.

   The SID is usually in a format like `S-1-5-21-3637136161-1358011849-3560387905-1014`.

8. Add `(A;;RPWPCR;;;`*`<SID of non-admin user>`*`)` before the `S:(AU;`... portion of the security descriptor that you copied to a text editor earlier in this procedure.

   Using the security descriptor and SID from our example, the result would be as follows, with the added text shown against a gray background:

   ```
   D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
   (A;;CCLCSWLOCRRC;;;IU)(A;;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;S-1-5-21-3637136161-
   1358011849-3560387905-1014)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
   ```

9. Run the following command, as is applicable, to set the security descriptor for the HP Codar service to the new value:

   ```
   -sc sdset codar "<new security descriptor>"
   ```

   This message `[SC] SetServiceObjectSecurity SUCCESS` is returned if the command completes successfully.

> **Note:** Repeat steps 4 through 9 as necessary so that the security descriptor is changed for both services.

Add permissions to the HP Codar directory for non-administrator user

The non-administrator user now has the permissions necessary to start and stop the HP Codar service. As a test, you can log in using the non-administrator user account and start and stop the HP Codar service.

The final steps below will add necessary permissions to the HP Codar directory for the non-administrator user.

To add permissions to the HP Codar directory for the non-administrator user, complete the following steps:

1. Log into the HP Codar machine as administrator.
2. In Windows Explorer, navigate to the HP Codar installation directory (for example, `C:\Program Files\Hewlett-Packard\Codar`), right-click on the folder, and select **Properties** in the menu that appears to open the Codar Properties dialog box.
3. Click the **Security** tab in the Codar Properties dialog box.
4. Check if the user is listed in the Group or user names list in the dialog box, and if it is not listed, continue with the next step. If the user is listed, go to Step 7 to continue.
5. Click the **Edit...** button, click the **Add...** button in the dialog box that appears, enter the non-administrator user name in the **Enter the object names to select** field, and then click the **Check Names** button.
6. Select the name, and then click **OK** to add the user to the Group or user names list.
7. Select the user name, select the **Allow** check box for the following permissions, and then click **OK**.
   - Read &execute
   - List folder contents
   - Read
   - Write

Allow HP Codar service to be run as non-administrator user on Windows

When running HP Codar on Windows, by default, the HP Codar service is run as the service user. This section explains how to configure HP Codar so that the HP Codar service can be run by non-administrator users. This process involves the following tasks:

- "Create non-administrator users" below
- "Configure HP Codar service" on the next page
- "Configure file system permissions for non-administrator users" on the next page

Caution: If the HP Codar service is run as a non-administrator user, you will not be able to do the following:

- Upgrade HP Codar
- Deploy hotfixes
- Install patches
- Use external tools such as the component tool, content archive tool, database purge tool, process definition tool, provider tool, schema installation tool, and support tool.
- Modify Autopass license data

Note: Certificates must be replaced and regenerated as the Administrator user.

Create non-administrator users

The following example shows how to create two non-administrator user accounts, one for the HP Codar service to run as and the other for the Marketplace Portal service to run as. Alternatively, but not documented, you may also create a single non-administrator user to run as for both services.

1. Log in as the Administrator.
2. Start the Control Panel on the HP Codar system and click **Add or remove user accounts** that is under **User Accounts**.
3. Click **Create a new account** in the Manage Accounts window that appears.
4. Enter a name for the user, select the **Standard user** radio button if it is not selected, and then click the **Create Account** button to create the user account.

   Create a user account: **CodarUser**.

Configure HP Codar service

1. Log in as the Administrator.
2. Stop HP Codar, see "Stop HP Codar" on page 81.
3. Back up and then delete the log files in the `CSA_HOME\jboss-as\standalone\log\` directory.
4. Delete all files in the `CSA_HOME\jboss-as\standalone\tmp\` directory.
5. Configure the HP Codar service to be run as CodarUser:
   a. Navigate to **Start** > **Administrative Tools** > **Services**.
   b. Right-click on the HP Codar service and select **Properties**.
   c. Select the **Log On** tab.
   d. Select **This account**.
   e. In the first field, enter **CodarUser**.
   f. Enter the password for CodarUser, confirm the password, and click **OK**.

Configure file system permissions for non-administrator users

Assign permissions to each user for the specified directories in the HP Codar file system.

1. Log in as the Administrator.
2. Open the File Explorer.
3. For each of the directories listed in the following table, do the following (where `C:\Program Files\Hewlett-Packard\Codar` is the directory in which HP Codar has been installed):
   a. Right-click on the directory and select **Properties**.
   b. Click the **Security** tab.
   c. Click **Edit**.
   d. Select a user (CodarUser) and select the permissions listed in the table.

e. Click **OK** to exit the Permissions dialog.

f. Click **OK** to exit the Properties dialog.

Directory	User(s)	Allowed Permission(s)
C:\	CodarUser	Full Control Modify Read & execute List folder contents Read Write
C:\Program Files\Hewlett-Packard	CodarUser	Full Control Modify Read & execute List folder contents Read Write
C:\Program Files\Hewlett-Packard\Codar	CodarUser	Full Control Modify Read & execute List folder contents Read Write
C:\Program Files\Hewlett-Packard\Codar\Autopass	CodarUser	Full Control Read
C:\Program Files\Hewlett-Packard\Codar\jboss-as	CodarUser	Read
C:\Program Files\Hewlett-Packard\Codar\jboss-as\bin	CodarUser	Write
C:\Program Files\Hewlett-Packard\Codar\CONTENT_IMPORT_LOGS	CodarUser	Write
C:\Program Files\Hewlett-Packard\Codar\jboss-as\standalone	CodarUser	Write

Directory	User(s)	Allowed Permission(s)
C:\Program Files\Hewlett-Packard\Codar\jboss-as\standalone\deployments	CodarUser	Modify Read & execute List folder contents Read Write
C:Program Files\Hewlett-Packard\Codar\jboss-as\standalone\configuration	CodarUser	Modify Read & execute List folder contents Read Write
C:\Program Files\Hewlett-Packard\Codar\openjre* *This is the JRE used by HP Codar. If you are using a different JRE, set the permissions to that JRE's directory.	CodarUser	Read & execute List folder contents Read Write
C:\Program Files\Hewlett-Packard\Codar\scripts	CodarUser	Read
C:\Program Files\Hewlett-Packard\Codar\security	CodarUser	Read
C:\Program Files\Hewlett-Packard\Codar\Tools	CodarUser	Read

4. Start HP Codar, see "Start HP Codar" on page 80.

5. Examine the `CSA_HOME\jboss-as\standalone\log\server.log` file and verify the changes deployed correctly.

Change HP Codar out-of-the-box user accounts for Windows and Linux

HP Codar 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 user names).

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

HP Codar Console user accounts

The following users ship out-of-the-box and are used with the HP Codar Console:

admin User: HP Codar Console

Username	admin
Default Password	cloud
Default Role	ROLE_REST
Usage	This account is used to initially log in to the HP Codar Console to configure the provider organization.
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 Codar. By default, the unencrypted value of this property is: cloud,ROLE_REST,enabled See "Encrypt password" on page 82 for instructions). 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.

admin User: HP Codar 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 `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 password" on page 82). 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. **Note:** This property not only contains the password, but also the roles that control access to HP Codar 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 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 Codar, see "Restart HP Codar" on page 81 .

idmTransportUser User: HP Codar Console

Username	idmTransportUser
Default Password	idmTransportUser
Default Roles	ROLE_AMIN, PERM_IMPERSONATE
Usage	This account is used to authenticate REST API calls.
To Disable	Do not disable this account.

idmTransportUser User: HP Codar 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 and the `idmTransportUser` property in the `integrationusers.properties` 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 and update the value of the `securityIdmTransportUserPassword` property. Determine a suitable new password (see "Encrypt password" on page 82). 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 Codar 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 password" on page 82). 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.
	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 web browser cache" on page 83 for information on how to clear the web browser cache. **Restarting HP Codar** After making these changes, restart HP Codar, see "Restart HP Codar" on page 81.

ooInboundUser User: HP Codar Console

Username	ooInboundUser

ooInboundUser User: HP Codar Console, continued

Default Password	cloud
Default Role	ROLE_REST
Usage	This account is used by HP Operations Orchestration to authenticate REST API calls with HP Codar.
To Disable	Do not disable this account.

ooInboundUser User: HP Codar 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 password" on page 82 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 Codar 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 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 Codar, see "Restart HP Codar" on page 81 .

codarintegrationUser: HP Codar Console

Username	codarintegrationUser
Default Password	cloud

codarintegrationUser: HP Codar Console, continued

Default Role	codarintegrationUser
Usage	This account is used in the Jenkins plug-in for integrating with HP Codar.
To Disable	It is recommended to enable this account so that Jenkins integration will work.
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 `securitycodarintegrationUserPassword` 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 codarintegrationUser 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 `codarintegrationUser` value and encrypt the entire value, including the roles and account status (see "Encrypt password" on page 82). 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. **Note:** This property not only contains the password, but also the roles that control access to HP Codar 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 securitycodarintegrationUserPassword property in csa.properties** If you change the password to this account, you must update the value of the `securitycodarintegrationUserPassword` property in `csa.properties`. You must also update and use the same password in `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 and update the value of the `securitycodarintegrationUserPassword` property. Use the same encrypted password that you entered for the `codarintegrationUser` property in the `csa-provider-users.properties` file. After modifying the `csa.properties` file, restart HP Codar, see "Restart HP Codar" on page 81 .

Note: The codarintegrationUser user account is for the purpose of integrating HP Codar with external interfaces such as Jenkins. It is highly recommended that you manage this account in LDAP and to do this you need to add this user account to LDAP. For more details, see "Prepare LDAP for HP Codar" on page 12.

Configure IPv6

This chapter explains how to configure HP Codar to support IPv6 (both dual-stack and IPv6-only). Make sure that IPv6 has been implemented on the system on which HP Codar 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 Codar 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>
   ```

2. Replace `127.0.0.1` with `[::1]`. For example, `<wsdl-host>${jboss.bind.address:[::1]}</wsdl-host>`

3. Locate the following lines:

   ```
   <interface name="management">

   <inet-address value="127.0.0.1" />

   </interface>
   ```

4. Replace `127.0.0.1` with `[::1]`. For example,

   ```
   <interface name="management">

   <inet-address value="[::1]" />

   </interface>
   ```

5. Locatethe following lines:

   ```
   <interface name="public">

   <inet-address value="0.0.0.0" />

   </interface>
   ```

6. Replace `0.0.0.0` with `[::]`. For example,

   ```
   <interface name="public">

   <inet-address value="[::]" />

   </interface>
   ```

7. Locate the following lines:

```
<interface name="unsecure">

<inet-address value="${jboss.bind.address.unsecure:127.0.0.1}" />

</interface>
```

8. Replace `127.0.0.1` with `[::1]`. For example,

```
<interface name="public">

<inet-address value="${jboss.bind.address.unsecure:[::1]}" />

</interface>
```

To configure HP Codar tools (such as the process definition tool, purge tool, schema installation tool, provider tool, or content archive tool) to support IPv6, do the following:

When you configure 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 HP Codar Console

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

Common Access Card

This chapter provides information about the integration between a Common Access Card (CAC) and HP Codar, where Common Access Card is used as the user authentication mechanism. By configuring Common Access Card, you are able to log into HP Codar using a Personal Identity Verification card.

After integrating HP Codar with Common Access Card, the following log in rules apply:

- You can log in to the HP Codar Console using a Personal Identity Verification card with a valid certificate.

- You can log in to the HP Codar Console using an HP Codar out-of-the-box user account without a Personal Identity Verification card.

- You can only log in to the HP Codar Console as a valid LDAP user, **with** a Personal Identity Verification card.

Caution: For the HP Codar Console, single sign-on (SSO) cannot be enabled at the same time as Common Access Card.

Complete the following steps to integrate HP Codar with Common Access Card:

- Stop HP Codar

- "Update JBoss configuration to set up client authentication" below

- "Configure HP Codar Console" on page 104

- "Configure certificate revocation" on page 105

- "Start HP Codar" on page 107

Stop HP Codar

If HP Codar is running, stop HP Codar. See "Stop HP Codar" on page 81 for instructions.

Update JBoss configuration to set up client authentication

To update the JBoss configuration, complete the following steps:

1. Download the CA certificate for the digital certificate from the Personal Identity Verification card.

2. Import the CA certificate into a new truststore.

   Windows:

   The truststore type is determined by the HP Codar environment. That is, if HP Codar is running in a standard environment, the truststore type must be JKS.

   For example, in a standard environment, if you named the CA certificate from step 1 `CACcert.cer`, saved it in C:\ and wanted to create a truststore named `CSA_HOME\jboss-as\standalone\configuration\.piv_keystore`, run the following command:

   ```
   "CSA_JRE_HOME\bin\keytool" -importcert -file C:\CACcert.cer -alias caccert -
   keystore CSA_HOME\jboss-as\standalone\configuration\.piv_keystore -storepass
   <password>
   ```

   Linux:

   The truststore type must be JKS.

   For example, if you named the CA certificate from step 1 `CACcert.cer`, saved it in `/tmp`, and wanted 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
   <password>
   ```

3. In the `CSA_HOME\jboss-as\standalone\configuration\standalone.xml` file, add the `ca-certificate-file=<location of truststore>` and `ca-certificate-password=<truststore password>` attributes to the `<ssl>` element and update the `verify-client` parameter in the `<ssl>` element to `want`.

   For example, change the following from:

   ```
   <ssl name="ssl" key-alias="CODAR" certificate-key-file="CSA_HOME\
   jboss-as\standalone\configuration\.keystore"
   verify-client="false"/>
   ```

   to

   ```
   <ssl name="ssl" key-alias="CODAR" certificate-key-file="CSA_HOME\
   jboss-as\standalone\configuration\.keystore"
   ca-certificate-file=" ca-certificate-password="TruststorePassword"
    verify-client="~~false~~want" />
   ```

   > **Note:** This example stores the password in clear text. If you want to use an encrypted password, follow the instructions at

https://community.jboss.org/wiki/JBossAS7SecuringPasswords to create a password vault for JBoss.

Note: If you are using the vault scripts, verify that the `JAVA_HOME` environment variable has been defined. Verify that `JAVA_HOME` has been set to the directory in which the JRE that is used by HP Codar is installed.

Windows:

If the directory path name includes a space, verify that the value has been enclosed in quotations marks. For example, to set `JAVA_HOME` to a directory path name that includes a space, from a command prompt, type

```
set JAVA_HOME="C:\Program Files\Hewlett-Packard\Codar\jre"
```

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

```
echo %JAVA_HOME%
```

Linux:

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

```
echo $JAVA_HOME
```

The following is an example of an encrypted password attribute using the JBoss password vault:

```
password="${VAULT::<vault_block_example>::password::N2NhZDzOMtES0ZGE4MmEtx0}"
```

Configure HP Codar Console

Complete the following steps to integrate the HP Codar Console with the Common Access Card:

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 the `IDM Authentication` comment and comment out the content that follows it:

   ```
   <!--<security:authentication-provider ref="idmAuthProvider"/>-->
   ```

b. Locate the `x509 and custom filter config for CAC` comment and uncomment 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 user name of the user to load the user details. If the user name is not stored as the CN in the certificate, you can change the regex to pick it up from the relevant field.

c. Locate and uncomment 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.

d. Locate the `Below is logout filter definition` comment.

Verify that `<beans:constructor-arg value="/logout.jsp"/>` is commented out. If it is not, comment it out.

Uncomment the following content:

```
<beans:constructor-arg value="http://www.hp.com"/>
```

Update the value to point to a URL of your choice (outside of the HP Codar application URLs).

> **Note:** The URL must start with `http://` and cannot start with just `www`.

e. Locate the `Bean definitions for CAC` comment 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 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 Codar to use a Certificate Revocation List" below
- "Configure HP Codar to use Certificate Revocation List Distribution Point" below
- "Configure HP Codar to Use Online Certificate Status Protocol" on the next page

Configure HP Codar 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 Codar is installed and point to its location using the `ca-revocation-url` parameters.

1. Copy the CRL file to the system where HP Codar 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_directory>*`"` attribute to the `<ssl>` element.

   For example, change the following from:

   ```
   <ssl name="ssl" key-alias="CSA" certificate-key-file="CSA_HOME\
   jboss-as\standalone\configuration\.keystore"
   ca-certificate-file="CSA_JRE_HOME\lib\security\cacerts"
   verify-client="want"/>
   ```

   to

   ```
   <ssl name="ssl" key-alias="CSA" certificate-key-file="CSA_HOME\
   jboss-as\standalone\configuration\.keystore"
   ca-certificate-file="CSA_JRE_HOME\lib\security\cacerts"
   verify-client="want" ca-revocation-url="<crl_file_directory>” />
   ```

3. Restart HP Codar service, see "Restart HP Codar" on page 81.

4. Log in to the HP Codar Console using a revoked certificate. The `Secure Connection Failed` message should display in the browser.

Configure HP Codar to use Certificate Revocation List Distribution Point

To enable a Certificate Revocation List Distribution Point (CRL DP), do the following:

1. 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"/>
   ```

2. Restart HP Codar service, see "Restart HP Codar" on page 81.

Configure HP Codar to Use Online Certificate Status Protocol

To enable the Online Certificate Status Protocol (OCSP), complete the following steps:

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:

   ```
   ocsp.enable=true
   ```

3. Restart HP Codar service, see "Restart HP Codar" on page 81.

Start HP Codar

See "Start HP Codar" on page 80 for instructions.

Single Sign-On

This chapter provides information about integrating HP Codar with a single sign-on solution.

Tasks include:

- "Integrate with HP Single Sign-On" below
- "Integrate HP Codar with single sign-on solution" on page 111
- "Integrate HP Codar with CA SiteMinder" on page 115

Integrate with HP Single Sign-On

HP Single Sign-On is included with HP Codar and can be used only from the HP Codar Console when launching an application from the HP Codar Console. HP Single Sign-On must be installed and configured on the application before single sign-on can be integrated between it and HP Codar.

Details on how to integrate HP Single Sign-On between HP Codar and HP Operations Orchestration are included in the documentation for HP Codar. Information regarding HP Operations Orchestration can be found in this guide (the tasks are located in "HP Operations Orchestration" on page 44).

If you want to integrate HP Single Sign-On between HP Codar and another application (the application must be launched from the HP Codar Console), you must use HP Codar's `crypto InitString` attribute value. This value can be found in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\hpssoConfiguration.xml` file. Information on how to integrate HP Single Sign-On between HP Codar and other applications is not provided in this guide.

The following sections describe how to enable HP Single Sign-On if it was not enabled during installation and how to disable HP Single Sign-On.

Enable HP Single Sign-On

HP Codar installs HP Single Sign-On during installation which may have been enabled or disabled. If HP Single Sign-On was not enabled during installation and you want to start using HP Single Sign-On, complete the following tasks:

> **Note:** If you enabled HP Single Sign-On during the installation of HP Codar, you do not need to complete these tasks.

> **Caution:** If HP Single Sign-On and CA SiteMinder are both configured for HP Codar, and if only HP Single Sign-On is enabled for another application, a user logging out from the other application will not be logged out from HP Codar. For example, if HP Single Sign-On is enabled between

HP Codar and HP Operations Orchestration, when a user logs out from HP Operations Orchestration Central, the user will not be logged out from the HP Codar Console.

"Step 1: Configure the domain" below

"Step 2: Set the HP Single Sign-On property" below

"Step 3: Configure the Identity Management component" on the next page

"Step 4: Restart HP Codar" on page 111

Step 1: Configure the domain

Configure the domain name of the network of the server on which HP Codar is installed. Applications launched from the HP Codar Console with which you want to use HP Single Sign-On must be installed on systems that belong to this domain.

To configure the domain, complete the following steps:

1. Navigate to the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF` directory.

2. Make a backup copy of the `hpssoConfiguration.xml` file.

3. Open the `hpssoConfiguration.xml` file in a text editor.

4. Locate the following content:

   ```
   <creationDomains>
      <domain>sso.domain</domain>
   </creationDomains>
   ```

5. Change `sso.domain` to domain name of the network of the server on which HP Codar is installed. Applications launched from the HP Codar Console with which you want to use HP Single Sign-On must be installed on systems that belong to this domain.

   For example, if your system host name is `codar_system.xyz.com`, enter `xyz.com` as the domain name.

6. Save and exit the file.

Step 2: Set the HP Single Sign-On property

To set the HP Single Sign-On property, complete the following steps:

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. Uncomment this line.

6. Save and exit the file.

7. Optionally, change the value of the `initString` setting for the HP Codar 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 must 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 and open it in an editor.

   c. Locate the `crypto` element and replace the value of `initString`.

   d. Save and exit the file.

Step 3: Configure the Identity Management component

To configure the Identity Management component, complete the following steps:

1. Navigate to the `CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF` directory.

2. Open the `web.xml` file in a text editor.

3. Locate the following comment (near the end of the file):

   ```
   <!-- START HP SSO Configuration -->
   ```

4. 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>C:\Program Files\Hewlett-Packard\Codar\jboss-as-7.1.1.Final\
   standalone\deployments\idm-service.war\WEB-INF\hpssoConfig.xml</param-value>
   </context-param>
   ```

5. Update the directory path name in `<param-value>` from "jboss-as-7.1.1.Final" to "jboss-as." For example, change

   ```
   CSA_HOME\jboss-as-7.1.1.Final\
   standalone\deployments\idm-service.war\WEB-INF\hpssoConfig.xml</param-value>
   ```

   to

   ```
   CSA_HOME\jboss-as\standalone\
   deployments\idm-service.war\WEB-INF\hpssoConfig.xml</param-value>.
   ```

6. Save and exit the file.

Step 4: Restart HP Codar

See "Restart HP Codar" on page 81 for instructions.

Disable HP Single Sign-On

If you no longer want to use HP Single Sign-On, you can disable it.

To disable HP Single Sign-On, complete the following steps:

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 Codar, see "Restart HP Codar" on page 81.

Integrate HP Codar with single sign-on solution

While HP Codar provides a single-sign-on solution using CA SiteMinder, there are a variety of scenarios where you may need to perform the integration with HP Codar using single-sign-on solution. For example, you may be using:

- An implementation where you need to authenticate with a single-sign-on vendor other than CA SiteMinder.
- A different deployment architecture than what is provided by HP Codar.
- A different version of CA SiteMinder than what is supported by HP Codar.
- An entirely different architecture than that which is supported.

In such cases it makes sense to create a custom single-sign-on solution so that you can extend the HP-provided implementation to your own.

For the HP Codar Console, single-sign-on cannot be enabled at the same time as Common Access Card.

The following sections describe how to integrate HP Codar with a single sign-on solution.

- "Verify HP Codar provider organization's LDAP server configuration" below
- "Verify HP Codar consumer organization's LDAP server configuration" on the next page
- "Configure custom single-sign-on server to work with HP Codar" on page 114
- "Stop HP Codar" on page 114
- "Configure HP Codar Console" on page 114
- "Configure proxy mapping" on page 114
- "Start HP Codar" on page 114
- "Verify single-sign-on integration" on page 115

Verify HP Codar provider organization's LDAP server configuration

You should verify that an LDAP user can log into the HP Codar 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 HP Codar Console, which is the interface from which you perform all administration tasks for *both* the HP Codar Console and the Marketplace Portal.

> Note: You must configure the HP Codar Provider organization to use the same LDAP server used by the custom single sign-on server. If you do not configure this access point, no one will be able to access the HP Codar Console.

To configure or update the provider organization's LDAP server, complete the following steps:

1. Launch the HP Codar Console by typing the following URL in a supported web browser: `https://<codarhostname>:8444/csa` where *<codarhostname>* is the fully-qualified domain name of the system on which the HP Codar Console resides.
2. Log in to the HP Codar Console as a Codar 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 HP Codar consumer organization's LDAP server configuration

Note: The same LDAP server must be used by the HP Codar Provider organization, HP Codar consumer organization and custom single sign-on server.

To configure or update the consumer organization's LDAP server, complete the following steps:

1. Launch the HP Codar Console by typing the following URL in a supported web browser: `https://<codarhostname>:8444/csa` where *<codarhostname>* is the fully-qualified domain name of the system on which the HP Codar Console resides.
2. Log in to the HP Codar Console as the Codar 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 Codar.

Only the `/codar` context is supported (this is required by the single sign-on proxy setup).

Configure custom single-sign-on server to work with HP Codar

To configure your custom single-sign-on server to work with HP Codar, follow the instructions provided with your single-sign-on application.

Stop HP Codar

See "Stop HP Codar" on page 81 for instructions.

Configure HP Codar Console

To configure the HP Codar Console, complete the following steps:

1. Update the `applicationContext-security.xml` file as appropriate for your custom single sign-on 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 proxy mapping

To configure proxy mapping, complete the following steps:

1. Map the `/codar` proxy to the HP Codar deployment.

   Caution: Use only `/codar` as the alias. Using another alias may cause HP Codar to fail.

   For example, when configuring the alias in an Apache proxy server, set the following:

   ```
   ProxyPass /codar/ https://<codarhostname>:8444/csa/
   ProxyPassReverse /codar/ https://<codarhostname>:8444/csa/
   ```

2. Map the `/idm-service` proxy to the identity management (IdM) deployment.

Start HP Codar

See "Start HP Codar" on page 80 for instructions.

Verify single-sign-on integration

You should verify that the single-sign-on integration works by logging into the HP Codar Console using the newly-integrated single-sign-on solution.

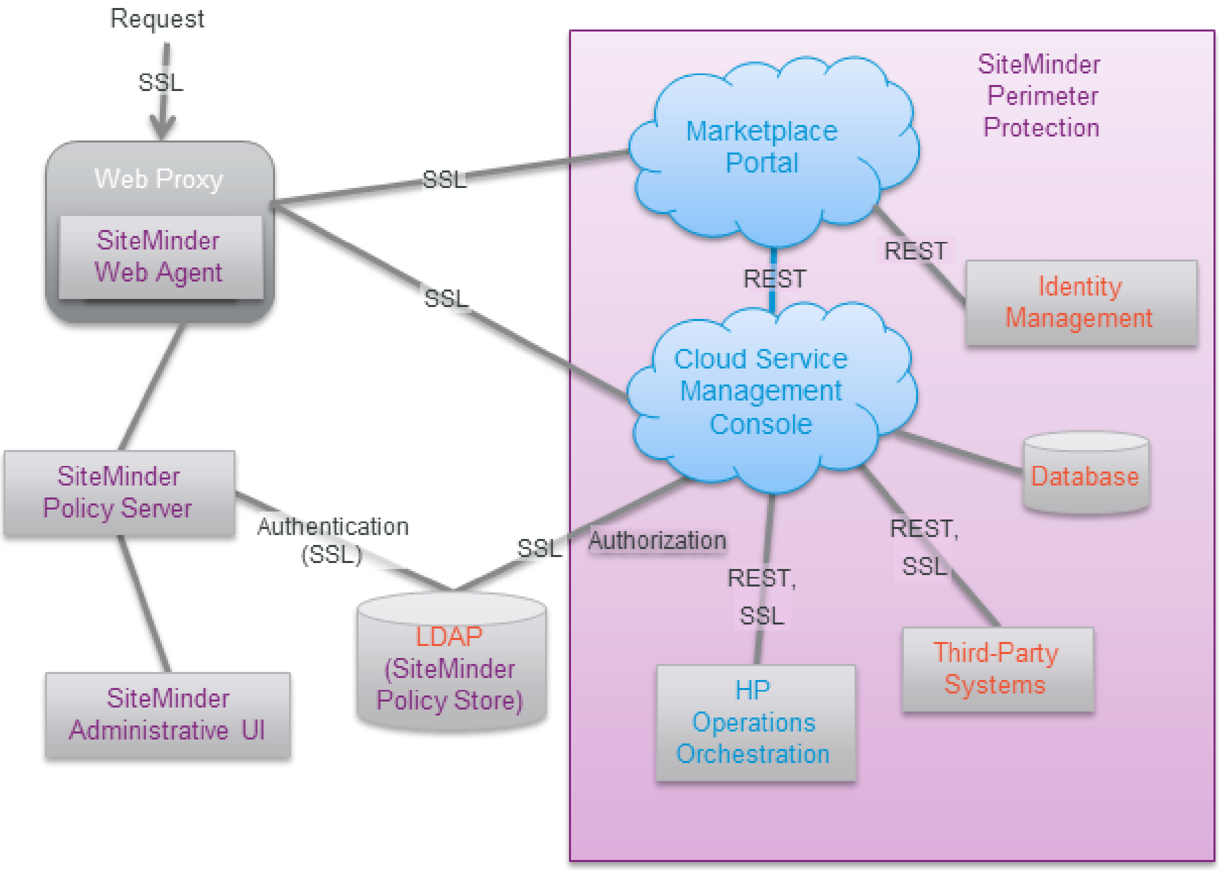
Integrate HP Codar with CA SiteMinder

HP Codar, 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 Codar and SiteMinder must be configured for the HP Codar provider and consumer organization (from the HP Codar Console) before integration between HP Codar and SiteMinder is started.

SiteMinder is made up of several components that work with HP Codar and your LDAP server to provide secure access. The information provided in this section configures HP Codar to work with a reverse proxy solution, as shown in the following diagram.

> **Note:** The Marketplace Portal will only be available if you have both HP Cloud Service Automation and HP Codar licenses. For details on the Marketplace Portal, see the *HP Cloud Service Automation Configuration Guide*.

Supported SiteMinder Deployment Architecture



For more information about how to install and configure CA SiteMinder for a reverse proxy solution, see 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

The following sections describe how to integrate HP Codar and SiteMinder:

- "Configure HP provider organization's LDAP server" on page 1
- "Configure SiteMinder Policy Server for HP integration" on page 1
- "Configure HP for SiteMinder integration" on page 1
- "Customize Logout page (optional)" on page 1

Configure HP Codar provider organization's LDAP server

You must configure the HP Codar 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 Codar and SiteMinder, you will not be able to access HP Codar after integration.

Caution: LDAP must be configured for the HP Codar provider organization before you begin the integration between HP Codar and SiteMinder. After integrating HP Codar and SiteMinder, you can only log in to the HP Codar Console via SiteMinder using a valid user from this LDAP directory. The out-of-the-box HP Codar users can no longer be used to log in to HP Codar.

When using the REST API, the out-of-the-box HP Codar users are still valid after integration.

To configure the provider organization's LDAP server, do the following:

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

2. Log in to the HP Codar Console as a Codar 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 SiteMinder Policy Server for HP Codar integration

To configure the SiteMinder Policy Server for HP Codar integration, complete the following steps:

1. Navigate to **Start** > **Administrative Tools** > **Services**.

2. Configure the SiteMinder Policy Server to use the LDAP server that will be shared between HP Codar and SiteMinder.

3. Configure the SiteMinder Policy Server idle timeout and the HP Codar Console 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 HP Codar Console is 60 minutes.

   The session timeout for the HP Codar 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>
   ...
   ```

4. 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.

5. If you have both HP Cloud Service Automation and HP Codar licenses, do the following:

   a. Navigate to **Start** > **Administrative Tools** > **Services**.

   b. Right-click on the **HP Marketplace Portal service** and select **Start**.

Configure the SiteMinder Web Agent for HP Codar integration

Configure proxy mapping for the SiteMinder Web Agent. To configure proxy mapping:

1. Map the `/codar` proxy to the HP Codar deployment. Use only `/codar` as the alias. Using another alias may cause HP Codar to fail.

   For example:

   ```
   ProxyPass /codar/ https://<codarhostname>:8444/csa/

   ProxyPassReverse /codar/ https://<codarhostname>:8444/csa/
   ```

2. Map the `/idm-service` proxy to the Identity Management component deployment. For example:

   ```
   ProxyPass /idm-service/ https://<codarhostname>:8444/idm-service/

   ProxyPassReverse /idm-service/ https://<codarhostname>:8444/idm-service/
   ```

Configure HP Codar for SiteMinder integration

To configure HP Codar for SiteMinder integration, you must do the following:

- "Stop HP Codar" below
- "Configure HP Codar Console" on the next page
- "Start HP Codar" on page 120

Stop HP Codar

See "Stop HP Codar" on page 81 for instructions.

Configure HP Codar Console

Configure the HP Codar Console for a SiteMinder reverse proxy solution. Update the `applicationContext-security.xml` file.

To configure HP Codar Console, complete the following steps:

1. Navigate to the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF` directory.

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 `SSO Authentication Provider` comment and uncomment the following content that appears after this comment:

   ```
   <security:authentication-provider ref='ssoAuthenticationProvider' />
   ```

5. Locate the `custom filter config for SSO` comment and uncomment the following content that appears after this comment:

   ```
   <custom-filter position="PRE_AUTH_FILTER" ref="ssoSiteminderFilter" />
   ```

6. Locate the `Below is logout filter definition` comment 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:

   ```
   <beans:constructor-arg value="/logout.jsp"/>
   ```

8. Locate the `Bean definitions for SSO` comment 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 HP Codar Console:

    ```
    codar.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 HP Codar Console), and `orgName` (the organization name of the selected organization in the browser). For example, if the client URL is `https://codar-server.company.com:8444/csa`, for a selected organization named `devteam`, then after the token replacement, the client displays a URL of `https://codar-server.company.com:8089/#/login/devteam`. No port is defined.

13. Locate the `Needed for SSO` comment and uncomment the following content:

    ```
    enableSSO=true
    ```

14. Save and exit the file.

Start HP Codar

See "Start HP Codar" on page 80 for instructions.

Customize Logout page (optional)

After clicking the `Log out` link from the HP Codar Console, 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 HP Codar Console.

- HP Codar Console:

  ```
  CSA_HOME\jboss-as\standalone\deployments\csa.war\ssologout.jsp
  ```

> **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.

Database administration

This chapter provides miscellaneous information about maintaining the database.

Tasks include:

- "Restart database and HP Codar service" below
- "Configure HP Codar reporting database user" on the next page
- "Update HP Codar database user or password" on page 126 (required if you change the database user or password)
- "Import large archives" on page 128
- "Install HP Codar database schema" on page 129
- "Configure HP Codar to mitigate frequently dropped database connections" on page 136

Restart database and HP Codar service

If you restart the database, you must restart the HP Codar service. If you do not restart the service, you may not be able to log in to the HP Codar Console.

Restart HP Codar service on Windows

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

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

Restart HP Codar service on Linux

To restart the HP Codar service on Linux:

On the server that hosts HP Codar, type the following:

```
service codar start
```

Configure HP Codar reporting database user

This section explains how to configure the Codar 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 Codar.

If you already configured the Codar reporting database user and role and defined the Codar reporting database user when running the installer or upgrade installer, you do not need to repeat these steps (the Codar reporting database user is already configured).

If you installed or upgraded HP Codar but did not configure the Codar reporting database user during the installation or upgrade and want to use the reporting capabilities of HP Codar, complete the tasks in this section.

To configure the Codar reporting database user, complete the following steps:

1. Create a read-only user.

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

   For example, do one of the following, based on the database you are using with HP Codar:

   Oracle

   Run the following commands to create the CodarReportingDBRole role and CodarReportingDBUser user:

   ```
   Create user CodarReportingDBUser identified by CodarReportingDBUser;
   Create role CodarReportingDBRole;
   Grant CREATE SESSION to CodarReportingDBUser;
   Grant CodarReportingDBRole to CodarReportingDBUser;
   Alter user CodarReportingDBUser default role CodarReportingDBRole;
   ```

   You will also need to add the CREATE ANY SYNONYM privilege to the HP Codar database user. This allows the HP Codar database user to create synonyms for the HP Codar reporting (read-only) database user.

   For example, if the HP Codar database user is named CodarDBUser, run the following command:

   ```
   Grant CREATE ANY SYNONYM to CodarDBUser
   ```

   Microsoft SQL

   Add a reporting database user (CodarReportingDBUser) to the HP Codar database with no roles:

```
CREATE LOGIN CodarReportingDBUser WITH PASSWORD = '<codarreportingdbuser_
password>';
CREATE USER CodarReportingDBUser FOR LOGIN CodarReportingDBUser WITH DEFAULT_
SCHEMA = codar;
```

PostgreSQL

From the psql prompt, enter the following:

```
CREATE ROLE CodarReportingDBUser LOGIN PASSWORD '<codarreportingdbuser_
password>' NOSUPERUSER NOCREATEDB NOCREATEROLE INHERIT;
GRANT CONNECT ON DATABASE codardb to CodarReportingDBUser;
```

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 Codar. See "Restart HP Codar" on page 81 for instructions.

4. The Codar reporting database user can access the data using the following view:

   `RPT_RSC_CAPACITY_V`

Update HP Codar database system

If you changed the hostname, domain, IP address, or port of the system on which the database used by HP Codar is installed, you must update the HP Codar configuration files that store this information.

1. If HP Codar is running, stop HP Codar. See "Stop HP Codar" on page 81.

2. On the system running HP Codar, open a command prompt and change to the `CSA_HOME\jboss-as\standalone\configuration` directory.

3. In a text editor, open the `standalone.xml` file.

4. In the file, locate the `<datasource>` element of the HP Codar database and the system information to be updated. For example:

Microsoft SQL Server

```
<datasource jndi-name="java:jboss/datasources/codarDS" pool-name="mssqlDS">
   <connection-
url>jdbc:jtds:sqlserver://127.0.0.1:1433/codardb;ssl=request</connection-url>
   <driver>mssqlDriver</driver>
.
.
.
</datasource>
```

Oracle

```
<datasource jndi-name="java:jboss/datasources/codarDS" pool-name="OracleDS">
   <connection-url>jdbc:oracle:thin://127.0.0.1:1521/codardb</connection-url>
   <driver>oracleDriver</driver>
.
.
.
</datasource>
```

PostgreSQL

```
<datasource enabled="true" jndi-name="java:jboss/datasources/codarDS"
jta="true"
pool-name="codarPostgresDS" use-ccm="true" user-java-context="true">
   <connection-url>jdbc:postgresql://127.0.0.1:5432/codardb</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 Codar service, see "Restart HP Codar" on page 81.

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 HP Codar database user or password

If you changed the user or password of the database used by HP Codar, you must update the JBoss DataSource and other files that store this information.

1. On the system running HP Codar, open a command prompt and change to the `CSA_HOME\jboss-as` directory.

2. Run the following command to generate an encoded version of the new database password:

   Windows:

   ```
   "CSA_JRE_HOME\bin\java" -cp "modules\org\jboss\logging\main\
   jboss-logging-3.1.2.GA.jar;modules\org\picketbox\main\
   picketbox-4.0.13.Final.jar"
   org.picketbox.datasource.security.SecureIdentityLoginModule <password>
   ```

   Linux:

   ```
   CSA_JRE_HOME/bin/java -cp "modules/org/jboss/logging/main/
   jboss-logging-3.1.2.GA.jar;modules/org/picketbox/main/
   picketbox-4.0.13.Final.jar"
   org.picketbox.datasource.security.SecureIdentityLoginModule <password>
   ```

   Copy the encoded password value that is returned (do not include spaces).

3. Stop the HP Codar service, see "Stop HP Codar" on page 81.

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="codar-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="codar-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="codar-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 the HP Codar service, see "Restart HP Codar" on page 81.

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 password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

Import large archives

Archives exported from HP Codar can be imported to install artifacts or update existing artifacts in HP Codar. Archives can be imported using the HP Codar Content Archive Tool, the HP Codar 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 HP Codar 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 Codar). When you reconfigure the JVM heap size for the tool, you do not need to restart HP Codar and HP Codar 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
```

> **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, see the *HP Codar Content Archive Tool* guide.

Import large archives from HP Codar Console or through the REST API

If you want to import an archive larger than 1.5 MB, HP recommends using the Content Archive Tool. If you must use the HP Codar Console or REST API to import a large archive, you must update the JVM heap size for HP Codar which requires HP Codar to be restarted. Also, importing a large archive from the HP Codar Console or through the REST API may slow the performance of HP Codar.

To increase the JVM heap size before importing a large archive from the HP Codar Console or through the REST API, complete the following steps:

1. If HP Codar is running, stop HP Codar. See "Stop HP Codar" on page 81.

2. Increase the JVM heap size for HP Codar.

    a. Open the `CSA_HOME\jboss-as\bin\standalone.conf.bat` file in a text editor.

    b. Locate the following line:

    ```
    set "JAVA_OPTS=%JAVA_OPTS%$JAVA_OPT -Xms2048M -Xmx2048M -
    XX:ReservedCodeCacheSize=256M
    -XX:MaxPermSize=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_OPTS%$JAVA_OPT -Xms3072M -Xmx3072M -
    XX:ReservedCodeCacheSize=256M"
    ```

    d. Save and close the file.

3. Start HP Codar, see "Start HP Codar" on page 80.

For more information about importing archives from the HP Codar Console, see the HP Codar Console Help. For more information about importing archives through the REST API, see the *HP Codar API Reference* guide.

Install HP Codar database schema

The schema installation tool is used to upgrade the existing HP Codar database schema or install a fresh database schema without re-installing HP Codar. Use this tool if you did not install HP Codar 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 Codar 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 Codar 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 Codar or if you upgraded the database schema when you upgraded HP Codar.

If you run this tool on an existing schema (where HP Codar 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.

Upgrade or install database schema

To upgrade or install a fresh HP Codar database schema, complete the following steps:

1. If HP Codar is running, stop HP Codar. See "Stop HP Codar" on page 81.
2. Change to the `CSA_HOME\Tools\SchemaInstallationTool\` directory.
3. During upgrade or installation of HP Codar, a file named `db.properties` is 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 Codar 1.50, you must update the `driverFiles` property value. The properties defined in `db.properties` are described in the following table.

Property Name	Description
dbScriptsDir	The location of database scripts installed with HP Codar used by the tool. If you are running a fresh installation of HP Codar 1.50 (you did not upgrade to HP Codar 1.50), you do not need to change these values. If you have upgraded to HP Codar 1.50 and want to upgrade the existing schema, you do not need to change these values. If you have upgraded to HP Codar 1.50, 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) `dbScriptsDir=CSA_HOME\scripts\freshinstallscripts\oracle` **PostgreSQL:** (upgrade and dropped schema only) `dbScriptsDir=CSA_HOME\scripts\freshinstallscripts\postgresql` **Microsoft SQL:** (upgrade and dropped schema only) `dbScriptsDir=CSA_HOME\scripts\freshinstallscripts\mssql`

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 Codar 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 Codar 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/codardb`

Property Name	Description
dbUserName	The user name of the database user you configured for HP Codar after installing the database.
dbPassword	The password for the database user. The password should be encrypted (see "Encrypt password" on page 82). 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.
	■ You do not need to change these values if:
	○ You are running a fresh installation of HP Codar 1.50 (you did not upgrade to HP Codar 1.50).
	○ You upgraded to HP Codar 1.50 and want to upgrade the existing schema.
	■ You must update this value to the value shown below, if you upgraded to HP Codar 1.50, dropped the existing database schema, and are installing a fresh database schema:
	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.sql,`
	`On Linux only:`
	`CSA_HOME\scripts\reporting\mssql\`
	`install_views_driver.sql,`
	`CSA_HOME\scripts\reporting\mssql\`
	`grant-reporting-user.sql`

Property Name	Description
	Note: Add the `grant-reporting-user.sql` file only if you have created the reporting database user for HP Codar.

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:

   Windows:

   - **Oracle (TLS not enabled), MS SQL, and PostgreSQL**

     ```
     "CSA_JRE_HOME\bin\java" -jar schema-installation-tool.jar
     ```

   - **Oracle (TLS enabled, HP Codar 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
     ```

     `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.

     `certificate_key_file_type` is the keystore type (for example, JKS or PKCS12).

   - **Oracle (TLS enabled, HP Codar 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
     ```

- **Oracle (TLS enabled, HP Codar 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
  ```

  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.

  certificate_key_file_type is the keystore type (for example, JKS or PKCS12).

- **Oracle (TLS enabled, HP Codar 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
  ```

Linux:

- **Oracle (TLS not enabled), MS SQL, and PostgreSQL**
  ```
  CSA_JRE_HOME/bin/java -jar schema-installation-tool.jar
  ```

- **Oracle (TLS enabled, HP Codar 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
  ```

  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.

  certificate_key_file_type is the keystore type (for example, JKS or PKCS12).

- **Oracle (TLS enabled, HP Codar 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
  ```

- **Oracle (TLS enabled, HP Codar 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
```

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.

certificate_key_file_type is the keystore type (for example, JKS or PKCS12).

- **Oracle (TLS enabled, HP Codar 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
  ```

Configure HP Codar 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, complete the following steps:

1. Stop the HP Codar service, see "Stop HP Codar" on page 81.

2. Edit the `CSA_HOME\jboss-as\standalone\configuration\standalone.xml` file:

   a. Find the `dataSource` tag which is used for HP Codar 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 Codar service, see "Start HP Codar" on page 80.

In a clustered environment, complete the following steps:

1. Stop the HP Codar service, see "Stop HP Codar" on page 81.
2. Edit the `CSA_HOME\jboss-as\domain\configuration\domain.xml` file:
   a. Find the `dataSource` tag which is used for HP Codar 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 Codar service, see "Start HP Codar" on page 80.

Appendix A: HP Codar Console properties

This section lists and describes the properties that can be configured for the HP Codar 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`

The following areas contain properties that can be configured (for many properties, default values are provided):

- Authentication
- "Security banner attributes" on page 1
- Security
- HP Codar keystore
- Service request processor scheduler
- Auditing
- Process execution manager
- Lifecycle engine
- Approval engine scheduler
- LDAP cache scheduler
- Clustering
- Dynamic property
- "Group approval" on page 1
- Common access card
- Single sign-on
- HP Single Sign-On
- Process executor delegate

- Miscellaneous
- HP Operations Orchestration
- "HP API authentication" on page 1
- Topology designer
- Session timeout

After modifying the `csa.properties` file, restart HP Codar, see "Restart HP Codar" on page 81 .

Authentication

These properties are used for authentication. These properties are configured in `csa.properties`.

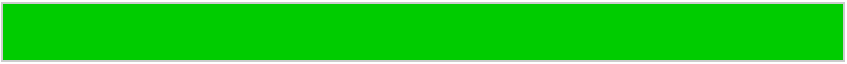
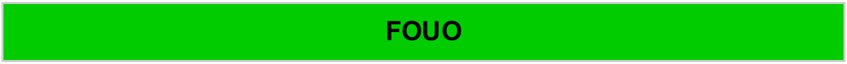
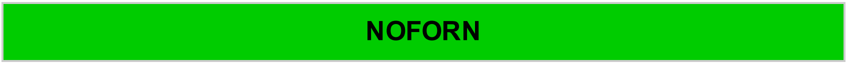
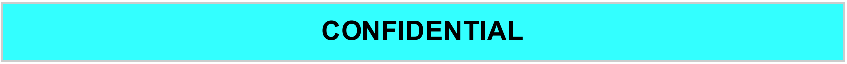
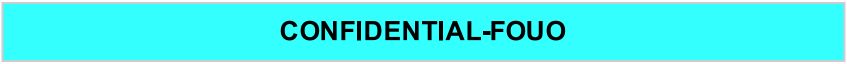
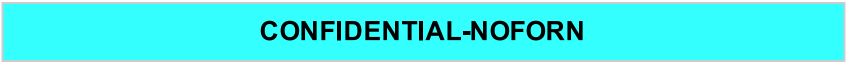
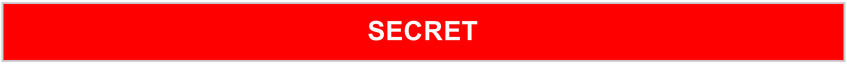
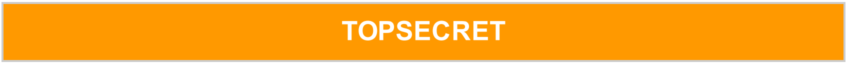
Property	Description
`csa.provider.hostname`	Required. The fully-qualified domain name of the system on which HP Codar is running. If you change this hostname, you must update the value of the `idm.codar.hostname` property in the `CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\spring\applicationContext.properties` file.
`csa.provider.port`	Required. The port used to connect to the system on which HP Codar is running. If you change this port, you must update the value of the `idm.codar.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 Codar is running. This attribute must be set to **https**. If you change this protocol, you must update the value of the `idm.codar.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 HP Codar Console. This attribute must be set to **`CSA-Provider.`**

Security banner attributes

The attributes in the following table are used by the HP Codar Console to enable or disable the display of a disclaimer upon logging in to the HP Codar Console and a color-coded banner that appears at the top and bottom of the HP Codar 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 HP Codar 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.

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 HP Codar 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.  FOUO • UNCLASSIFIED_NOFORN. Not releasable to foreign nationals. The banner is light green and displays the text "NOFORN." An example is shown below.  NOFORN • CONFIDENTIAL. The banner is light blue and displays the text "CONFIDENTIAL." An example is shown below.  CONFIDENTIAL • CONFIDENTIAL_FOUO. The banner is light blue and displays the text "CONFIDENTIAL-FOUO." An example is shown below.  CONFIDENTIAL-FOUO • CONFIDENTIAL_NOFORN. The banner is light blue and displays the text "CONFIDENTIAL-NOFORN." An example is shown below.  CONFIDENTIAL-NOFORN • SECRET. The banner is red and displays the text "SECRET." An example is shown below.  SECRET • TOPSECRET. The banner is orange and displays the text "TOPSECRET." An example is shown below.  TOPSECRET To edit the banner content, edit the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\msgs\messages_en.properties` file.

Security

These properties are used to configure encrypted passwords (see "Encrypt password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

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\csa.war\WEB-INF\applicationContext-security.xml` file). The admin user account is used for initial login to the HP Codar Console and can also be used to authenticate REST API calls. The password should be encrypted (see "Encrypt password" on page 82 for instructions on encrypting passwords). 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, see the *HP Codar API and CLI Reference Guide*.
securityCsaReporting UserPassword	Required. The encrypted password used by the out-of-the-box `csaReportingUser` user (defined in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-security.xml` 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 Codar to determine the values that will appear in the list. This account has read-only access to HP Codar. The password should be encrypted (see "Encrypt password" on page 82 for instructions). 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, see the *HP Codar API and CLI Reference Guide*.

Property	Description
securityTransport UserName	Required. The out-of-the-box user used to authenticate REST API calls between the Marketplace Portal and HP Codar Console (it should not be used to log in to the HP Codar 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 Codar out-of-the-box user accounts for Windows and Linux" on page 92. For more information about the REST APIs, see the *HP Codar API and CLI Reference Guide*.
securityTransportPassword	Required only if both the HP Cloud Service Automation and HP Codar licenses are used. 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 HP Codar Console (it should not be used to log in to the HP Codar Console). The password should be encrypted (see "Encrypt password" on page 82 for instructions). If you change this password, you must update the value of the `idm.codar.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 Codar out-of-the-box user accounts for Windows and Linux" on page 92. For more information about the REST APIs, see the *HP Codar API and CLI Reference Guide*.

Property	Description
securityOoInbound UserPassword	Required. The encrypted password used by the out-of-the-box `ooInboundUser` user (defined in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-securIty.xml` file). The ooInboundUser user account is used by HP Operations Orchestration to authenticate REST API calls with HP Codar (it should not be used to log in to the HP Codar Console). The password should be encrypted (see "Encrypt password" on page 82 for instructions). 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 (see "HP Operations Orchestration settings" on page 157 and the *HP Codar Installation and Configuration Guide*).
securityCdaInbound UserPassword	Required. The encrypted password used by the out-of-the-box `cdaInboundUser` user (defined in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-securIty.xml` file). The `cdaInboundUser` user account is used by HP Continuous Delivery Automation to authenticate REST API calls with HP Codar (it should not be used to log in to the HP Codar Console). The password should be encrypted (see "Encrypt password" on page 82 for instructions). If you change this password, you must also update and use the same password in HP Continuous Delivery Automation. For more information about this user account, see "Change HP Codar out-of-the-box user accounts for Windows and Linux" on page 92.

Property	Description
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 HP Codar Console). The password should be encrypted (see "Encrypt password" on page 82 for instructions). If you change this password, you must also update the following passwords (you must use the same password): • `idmTransportUser` property in the `CSA_HOME\jboss-as\standalone\deployments\idm-service.war\WEB-INF\classes\integrationusers.properties` file. • Password of any REST API calls that use this password. For more information about this user account, see "Change HP Codar out-of-the-box user accounts for Windows and Linux" on page 92.
securityCatalog AggregationTransport UserPassword	Required. The encrypted password used by the out-of-the-box `codarCatalogAggregationTransportUser` user (defined in the `CSA_HOME\jboss-as\standalone\deployments\csa.war\WEB-INF\applicationContext-security.xml` file). The codarCatalogAggregationTransportUser user account is used to authenticate catalog aggregation REST API calls with HP Codar (it should not be used to log in to the HP Codar Console). The password should be encrypted (see "Encrypt password" on page 82 for instructions). 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 Codar out-of-the-box user accounts for Windows and Linux" on page 92.

Property	Description
securityEncrypted SigningKey	HP Codar's encrypted signing key used to encrypt and decrypt authentication data passed between HP Codar 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 password" on page 82for instructions. 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 HP Codar Console. Default: exe,bat,com,cmd
csa.additionalSupported ExtensionsForImport	A comma-delimited list of the file extensions that designate the types of documents or files that can be uploaded to the HP Codar Console. The file extensions listed can be the sole extension of the file (for example, `mydocument.txt`, where `txt` is one of the listed file extensions) or the start of the file extension (for example, `mydocument.txt_3491767613`). Files can be uploaded using the HP Codar Console, the content archive tool, or the import API. See the *HP Codar Console Help* or *HP Codar API and CLI Reference Guide* 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 Codar system using the HP Codar 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 Codar keystore

These properties are used to configure information about HP Codar's keystore.

These properties are configured in `csa.properties`.

Property	Description
csaTruststore	Required. The HP Codar keystore that stores trusted Certificate Authority certificates. Default: No default specified **Example** `CSA_JRE_HOME/lib/security/cacerts` **Note:** Use only forward slashes (/) as your path separators.
csaTruststorePassword	Required. The encrypted password of the HP Codar keystore (see "Encrypt password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses. Default: No default specified **Example** `ENC(9eC7TTnB0uGOGK5U648UITcEV5AuV5T)`

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 Codar service was stopped. Used for auditing purposes. Default: `CSA_HOME/jboss-as/bin/shutdown.log` **Note:** Use only forward slashes (/) as your path separators.

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 Codar starts an HP Operations Orchestration flow. Default: `CSA_PROCESS_ID`

Property	Description
`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

This property is 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_WAKEUP_TIME`	Optional. How often, in minutes, the approval engine scheduler checks for completion of an approval process to determine if an approval process should be approved or denied. Default: 1

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 HP Codar Console, certain actions require authorization (verification if the user belongs to a group). When authorization is requested for a user, HP Codar 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 Codar is running (single or clustered). When set to `single`, HP Codar runs in standalone mode (on a single instance) and all HP Codar services are run on this instance. When set to `clustered`, HP Codar runs in domain mode (in a clustered environment) and all HP Codar services are run on the master node. If you are using Microsoft SQL Server as your database, this property must be set to `single`. If you are running on Linux, this property must be set to `single`. 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 Codar attempts to fetch or retrieve data for dynamic properties. Default: 3000 (3 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

Common Access Card

This property is used to enable integration between Common Access Card and HP Codar.

This property is configured in `csa.properties`.

Property	Description
enableCAC	Optional. Enable integration between Common Access Card (CAC) and HP Codar, where the Common Access Card 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 Codar.

This property is configured in `csa.properties`.

Property	Description
enableSSO	Optional. Enable integration between CA SiteMinder and HP Codar, 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 Single Sign-On) and the HP Codar Console. HP Single Sign-On can be used when launching an application, such as the embedded HP Operations Orchestration, from the HP Codar Console. If you have installed or plan to integrate another single sign-on application or common access card with HP Codar, additional configuration to integrate with the HP Single Sign-On is required.

This property is configured in `csa.properties`.

Property	Description
enableHPSSO	Optional. Enable integration between HP Single Sign-On and the HP Codar 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 is a miscellaneous property that does not fall under any specific category.

This property is configured in `csa.properties`.

HP Operations Orchestration

These properties are configured in `csa.properties`.

The following properties configure the interaction between the HP Codar Console and HP Operations Orchestration. In the subscription event overview section of the **Operations** area in the HP Codar 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 (HP Operations Orchestration version 10.21). Set this URL to the system on which HP Operations Orchestration version 10.21 is installed. For example, `https://<hostname>:8443`.
OOS_ USERNAME	The username used to log in to HP Operations Orchestration Central. Set this username to admin.
OOS_ PASSWORD	The encrypted password used by the user defined in `OOS_USERNAME` to log in to HP Operations Orchestration Central. Set this property to the encrypted value of the user defined in `OOS_USERNAME` (see "Encrypt password" on page 82). An encrypted password is preceded by `ENC` without any separating spaces and is enclosed in parentheses.

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 Codar keeps a socket open for SOAP-based communication with HP Operations Orchestration. Default: 60000
`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

HP Codar API authentication

These properties are used to configure authentication for the HP Codar 1.50 API. For details, see the *HP Codar API and CLI Reference Guide*.

Topology designer

These properties are used to configure the features of topology designs. Topology designs are built using components supported by various resource provider types and each component is bound to a specific provider type.

These properties are configured in `csa.properties`.

Property	Description
TopologyDesignProvisioning. TIMEOUT	Optional. The amount of time, in seconds, HP Codar attempts to provision or de-provision a topology design that is not based on an HP Helion OpenStack® provider (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 HP Codar Console, the subscription (to a service offering that is created from a topology design that is not based on an HP Helion OpenStack® provider) 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 the resource provider selection option (displaying or not displaying this option to a subscriber) for topology designs that are not based on an HP Helion OpenStack® provider. Default: true (enabled)
`csa.topology.expressDesignEnabled`	Optional. Enable or disable express designs in the topology designer. Express designs simplify the process of creating basic HP Helion OpenStack® topology designs. Default: false

Property	Description
`csa.topology.calloutsEnabled`	Optional. Enable or disable the `Pre-create Callout` and `Post-create Callout` properties of the Server Group Type component in the topology designer. See the *HP Codar Console Help* for more information about these properties. Default: false
`csa.topology.CloudOsSpecEnabled`	Optional. Enable or disable the **HP Helion OpenStack** tab in the Create new design dialog in the topology designer. The tab allows the designer to select an HP Helion OpenStack provider when creating a topology design. Default: false

Session timeout

This property is used to configure the HP Codar Console session.

This property is configured in `web.xml`.

Property	Description
session-timeout	Optional. The amount of inactivity, in minutes, that causes the HP Codar Console session to time out. Default: 60

Restart HP Codar service

After modifying the `csa.properties` file, restart HP Codar, see "Restart HP Codar" on page 81 .

Appendix B: HP Operations Orchestration settings

This section is provided as a reference only. The listed HP Operations Orchestration settings are configured in HP Operations Orchestration Studio and are used to integrate HP Operations Orchestration and HP Codar. These settings should have been configured as part of installing HP Codar. Information on how to configure these settings can be found in the *HP Codar Installation and Configuration Guide*.

The following areas contain settings that can be configured from HP Operations Orchestration Studio:

- "Remote action services" below
- "System accounts" on the next page
- "System properties" on the next page

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 Codar 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 **Override Value** (HP Operations Orchestration version 10.21) 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 Codar. 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 Codar. Default Property Value: HPN Delete Vlan

System properties, continued

Setting	Description
`CSA_OO_USER`	Required. The user that communicates with HP Codar using the REST API. Default Property Value: ooInboundUser **Note:** The **Override Value** (HP Operations Orchestration version 10.21) 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 Codar using the REST API. HP recommends the following Property Value: `https://`*`<codar_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: Codar 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 C: 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.

The following sections describe configuring the identity service and its components:

"External configuration" below

"Configure seeded authentication" on page 162

"Configure blacklist" on page 162

"Configure Java Relying Party Library" on page 163

"Internal configuration" on page 164

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 you can edit the `standaloneconf.bat` file on Windows or `standalone.conf` file on Linux in `CSA_HOME\jboss-as\bin\` to add the JVM argument to `JAVA_OPTS` for the HP Codar 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 "ConvergedLdapAuthConfig" on page 166) must match the HP Codar 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 Codar instance: `http` or `https`
`idm.csa.hostname`	The hostname or IP address of the HP Codar server
`idm.csa.port`	The port number used by the HP Codar server
`idm.csa.username`	The user name for the HP Codar integration account
`idm.csa.password`	The password for the HP Codar 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 user name for the integration account used to communicate with Keystone and perform HP Helion OpenStack® or OpenStack operations.
`idm.keystone.transportPassword`	The password for the integration account used to communicate with Keystone and perform HP Helion OpenStack® or OpenStack operations. For improved security, this value should be encrypted.

Property Name	Description
`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 Codar organization ID used to log in — including case (for example, a Keystone project name of `project_name` will not match an HP Codar 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 Codar 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 user name, 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 blacklist

The blacklist contains users whom the identity service should never attempt to authenticate. In general, these are the HP Codar transport users and seeded HP Codar provider organization users, but you can edit this list. In the file, the blacklisted user name is associated with a Boolean value that indicates whether the user name is actually on the blacklist. A user might be temporarily removed from the blacklist by setting the Boolean value to `false`, but the value should generally be `true`. Following is the general format of each line in the file.

```
<username>= true
```

In the default configuration, the file contains the following contents.

```
admin = true
csaTransportUser = true
ooInboundUser = true
```

```
csaReportingUser = true
cdaInboundUser = true
csaCatalogAggregationTransportUser = true
```

This file should be updated to reflect any changes to the set of HP Codar transport users or seeded HP Codar provider organization users.

Configure 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 Codar. 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 "Internal configuration" on the next page) 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

Property Name	Description
`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.

InfinispanTokenStore

Defines the persistence mechanism for request tokens. Most attributes of this object define how the identity service behaves in high availability (HA) or clustered deployments.

Class: `com.hp.ccue.identity.ha.InfinispanTokenStore`

Property Name	Description

`lifetimeSeconds`
`lifetimeMinutes`
`lifetimeHours`
	Required. Time (in seconds, minutes, or hours) that an entry is permitted to remain in the token store. These properties determine the amount of time that the login page is valid. The lifetime as installed is 60 minutes. More permissive organizations should use a larger value; more restrictive organizations should use a smaller value.
	Default value: (None)
	Externalized: No

`clusterEnabled`	Required in a clustered environment. A flag indicating whether clustering should be enabled: `true` or `false` Default value: `false` Externalized: No
`clusterConfigFile`	Required in a clustered environment. The file name of the `jgroups.xml` configuration file that defines the cluster. Setting this property forces the `clusterEnabled` property to `true`. Default value: (None) Externalized: No
`configFile`	Required in a clustered environment. The file name of the Infinispan XML configuration file. The settings in this configuration file override the values in the `clusterEnabled` and `clusterConfigFile` properties. Default value: (None) Externalized: No

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

Property Name	Description
`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 Codar 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 Codar 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 Codar instance Default value: (None) Externalized: `idm.csa.protocol`
`providerHostname`	Required if using ActiveDirectory or LDAP. Hostname or IP address of the HP Codar server Default value: (None) Externalized: `idm.csa.hostname`

Property Name	Description
`providerPort`	Required if using ActiveDirectory or LDAP. Port number used by the HP Codar server Default value: (None) Externalized: `idm.csa.port`
`securityTransportUsername`	Required if using ActiveDirectory or LDAP. Username for the HP Codar integration account Default value: (None) Externalized: `idm.csa.username`
`securityTransportPassword`	Required if using ActiveDirectory or LDAP. Password for the HP Codar 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 Codar server to use to get the LDAP configuration for each organization Default value: (None) Externalized: No
`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
`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

Property Name	Description
`tokenFactory`	Required. The token factory for creating identity tokens in response to successful authentications Default value: (None) Externalized: No
`blacklist`	A map associating usernames to Boolean values indicating whether they are blacklisted Default value: (None) Externalized: No
`blacklistFile`	The file containing the blacklist Default value: `blacklist.properties` 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
`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 Codar 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
`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

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 (Codar 1.50)

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