Codar

Software Version: 1.90

For Linux operating system

Administer

Document Release Date: September 2017

Software Release Date: September 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Documentation Updates

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

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

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

Support

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

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

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

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

Contents

Administer

Administer

The following topics help you, as an Administrator, manage Codar.

- "Roles" on the next page
- Organization
- Content Store
- Content Store Settings
- Providers
- Orchestration
- Cloud Optimizer

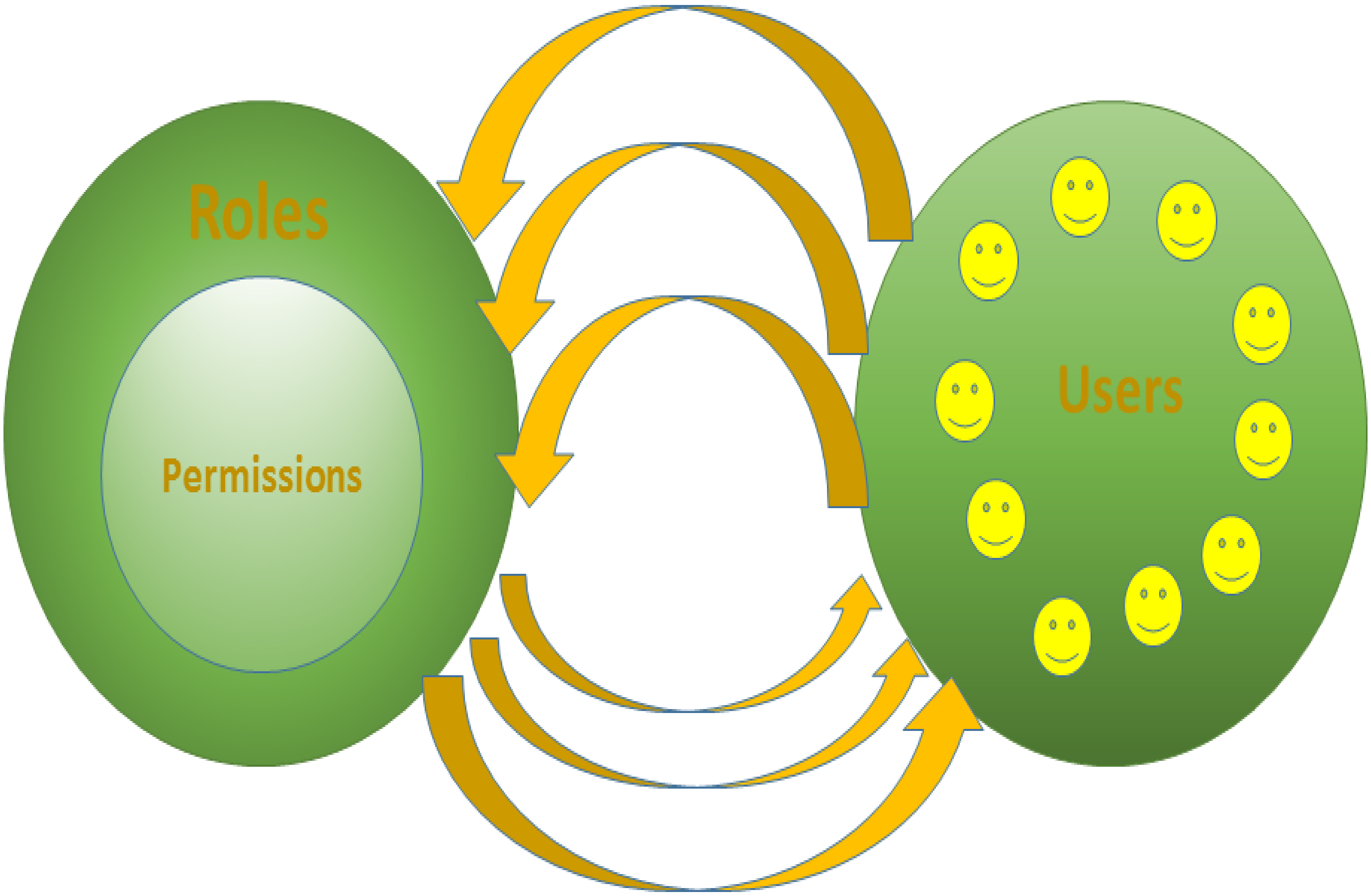
Roles

Every user in Codar is assigned one or multiple roles. Roles determine the permissions or activities that a Codar user can perform on the product. Codar contains some out-of-the-box roles; however, users can also create their own roles and then assign permissions to the roles they create. Only Codar users belonging to the following roles have the right to create roles:

- Administrator
- Application Architect
- Application Release Manager

Out-of-the-box roles can be edited but not deleted. This allows administrators or architects to add or remove permissions to these roles. Roles that are created can be edited or deleted.

All roles (out-of-the-box roles and roles created by Codar users) are displayed in the Roles page. Roles and users follow a many-to-many relationship. That is, multiple users can have multiple roles and multiple roles can be assigned to one or more users. The following diagram depicts the many-to-many relationship between users and roles.



For more information, refer to the following topics:

- "Out-of-the-box roles in Codar" on the next page
- Roles in Codar
- "Create, edit, and delete roles " on page 10

Out-of-the-box roles in Codar

Out-of-the-box roles provide authorization for members to perform tasks. These roles can be edited but not deleted.

Users with the Administrator role have access to all areas.

Summary of access by role

The following table shows the predefined roles and the tasks to which each has access.

Permissions	Application Architect	Application Developer	Application QA	Release Manager	Application Operations Manager	Codar Integration User
Design create	Yes					
Package create	Yes	Yes				Yes
Package update	Yes	Yes	Yes	Yes	Yes	Yes
Package delete	Yes	Yes	Yes	Yes	Yes	Yes
Package deploy	Yes	Yes	Yes	Yes	Yes	Yes
Package promote		Yes	Yes	Yes	Yes	Yes
Package reject		Yes	Yes	Yes	Yes	Yes
Dashboard view	Yes			Yes		
Custom role and stage create	Yes			Yes		
Application release gate	Yes			Yes		
Application release gate approve	Yes			Yes		

By default, the Codar Application Architect role has been configured to add release gate actions in Development stage only. Similarly, the Codar Application Release manager role has been configured to add release gate actions in Production stage only.

If both of these roles should be able to add release gate actions across lifecycle stages, then the Administrator must associate these roles with the respective lifecycle stage(s).

Create, edit, and delete roles

To create a role in Codar:

1. In the Codar Console, click the **Release Automation** > **Pipeline Configurations** sidebar menu item.
2. Click **Roles**.
3. Click the **Create Role** button in the Roles page. This button is enabled only for users belonging to the Administrators, Application Architect, Application Release Manager, and other roles that have the "Custom role and stage create" permission.
4. Enter information as per the following table:

Field	Description
Display Name	Name of the role
Description	Description of the role
Permission	Permissions that you want to assign to the role. You can select more than one permission.
Image	Browse and select an image that you want to associate with the role. The image is displayed next the role in the Roles page.

5. Click **Create**.

The role that you created is displayed in the Roles page and the permissions assigned to the role are displayed below the role. You can update or delete the role by clicking the wheel icon next to the role.

Edit a role

To edit an existing role in Codar:

1. Click the wheel icon next to the role you want to edit and click **Edit**.
2. In the Edit Role dialog box, edit the role name, description, or the permissions associated with the role. You can add or remove permissions. You can also change the image associated with the role.
3. Click **Save**.

The updated role with your changes is reflected in the Roles page.

> If you update a role by modifying its permissions, you must relogin to Codar to see the updated permissions.

Delete a role

To delete an existing role in Codar:

1. Click the wheel icon next to the role you want to edit and click **Delete**.
2. Click **Yes** in the Confirmation Required dialog box.

The role is removed from the Roles page.

> If you delete a role that is associated with a lifecycle stage, the role is removed from the lifecycle stage.

Organizations

Use the **Organizations** area to manage organizations. From this section, in the upper left corner, you can view the total number of organizations created, including the provider organization.

Using the organizations interface

Item	Description
	Reload the data in this view.
	Delete a group DN from a role.
	Display a tooltip for the associated field by placing the cursor over this icon.

Informational icons

Icon	Description
	When this icon is adjacent to an organization, it denotes the provider organization. There can be only one provider organization and it is automatically configured. You may modify the provider organization, as needed. However, you cannot delete it.
*	Indicates the field is required, and you must enter information in order to successfully complete the organization's configuration.

View an organization

1. In the left navigation frame, select the organization.
2. In the organization's navigation frame, select **Summary** to view a summary of the organization. Select any of the other sections to view more detailed information.

Configure an organization

1. In the left navigation frame, select the organization.
2. In the organization's navigation frame, select a section in which you can configure information about the organization.

See the following topics for specific configuration tasks:

- "Organization summary" on the next page
- "Organization general information" on page 16
- "Configure LDAP for an organization" on page 17
- "Organization access control" on page 23

Organization summary

View a summary of the selected organization's configuration. To configure or update this information, in the organization's navigation frame, select the appropriate section such as LDAP, Access Control, or Email Notifications.

Viewable summary information

Section	Displayed summary information
LDAP	• Hostname - The host name used to connect to the LDAP server. • Port - The port used to connect to the LDAP server.
Access Control	• List of roles - Roles in the organization to which group DNs can be assigned.
Email Notifications	• Sender Email Address - Email address that appears as the sender of email notifications. • Port - The port used to connect to the mail server when sending email notifications. Email notification is not supported by Codar.

Organization general information

General information appears at the top of the organization's page.

To configure general information for an organization

1. In the organization's navigation frame, select **General Information**.
2. Provide or update the following information:

Item	Description
Organization Identifier	A unique name that Codar assigns to the organization. This cannot be changed.
Organization Display Name	A unique name that identifies the organization.
Description	A description of the organization.
Organization Logo	An image that represents the logo of the organization. The logo appears in the top left of an organization's page. Click **Upload Image** to add your own image. Supported file extensions include `.jpg`, `.jpeg`, `.gif`, and `.png`. The recommended image size is 256 by 256 pixels, and the image will be scaled to the appropriate size. The images are stored in the `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\images\library` folder of the Codar server.

3. Click **Save**.

Configure LDAP for an organization

LDAP (Lightweight Directory Access Protocol) is configured in the Managment Console.

To completely configure access to Codar, you must configure LDAP to

- Authenticate a user's credentials
- Allow an organization to authenticate a user's access to information
- Allow an organization to authorize a user's access to information

From this page you can:

- Configure LDAP for authentication to log in to Codar.
- Configure LDAP for access control in Codar.

When you configure LDAP for the provider organization, you are configuring the set of users who can log in and be authenticated to perform actions in the Managment Console.

To configure authorization to access information in Codar for organizations, see "Organization access control" on page 23.

To configure LDAP

1. In the organization's navigation frame, select **LDAP**.
2. Provide or update the following information:

   LDAP Server Information

   Configure the LDAP server and a user with access to the server.

Item	Description
Hostname	The fully-qualified LDAP server domain name (server.domain.com) or IP address. Example: `ldap.xyz.com`
Port	The port used to connect to the LDAP server (by default, 389). Example: `389`
Connection Security	If the LDAP server is configured to require ldaps (LDAP over SSL), select the **SSL** checkbox.

Item	Description
Base DN	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search. Example: `o=xyz.com`
User ID (Full DN)	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. Example: `uid=admin@xyz.com,ou=People,o=xyz.com`
Password	Password of the User ID. If the LDAP server does not reacquire a User ID or password for authentication, this value can be omitted.

LDAP Attributes

Enter the names of the attributes whose values are used for email notifications and authentication.

Item	Description
User Email	The name of the attribute of a user object that designates the email address of the user. The email address is used for notifications. If a value for this attribute does not exist for a user, the user does not receive email notifications. Default: `mail`
Group Membership	The name of the attribute(s) of a group object that identifies a user as belonging to the group. If multiple attributes convey group membership, the attribute names should be separated by a comma. Default: `member,uniqueMember`
Manager Identifier	The name of the attribute of a user object that identifies the manager of the user. Default: `manager`
Manager Identifier Value	The name of the attribute of a user object that describes the value of the Manager Identifier's attribute. For example, if the value of the Manager Identifier attribute is a distinguished name (such as `cn=John Smith, ou=People, o=xyz.com`) then the value of this field could be `dn` (distinguished name). Or, if the Manager Identifier is an email address (such as `admin@xyz.com`) then the value of this field could be `email`. Default: `dn`
User Avatar	LDAP attribute whose value is the URL to a user avatar image that will display for the user. If no avatar is specified, a default avatar will be used.

User Information

Codar uses a user search-based log-in method to authenticate access to information.

Item	Description
User Name Attribute	The name of the attribute of a user object that contains the user name that will be used to log in. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. Often, you will want a **User Name Attribute** whose value in a user object is an email address. Examples: userPrincipalName or sAMAccountName or uid
User Search Base	The location in the LDAP directory where users' records are located. This location should be specified relative to the Base DN. If users are not located in a common directory under the Base DN, leave this field blank. Examples: cn=Users or ou=People
User Search Filter	Specifies the general form of the LDAP query used to identify users during login. It must include the pattern {0}, which represents the user name entered by the user when logging in. The filter is generally of the form <attribute>= 0}, with <attribute> typically corresponding to the value entered for **User Name Attribute**. Examples: userPrincipalName={0} or sAMAccountName={0} or uid={0}
Search Option (Search Subtree)	When a user logs in, the LDAP directory is queried to find the user’s account. The **Search Subtree** setting controls the depth of the search under **User Search Base**. If you want to search for a matching user in the **User Search Base** and all subtrees under the **User Search Base**, leave **Search Subtree** selected. If you want to restrict the search for a matching user to only the **User Search Base**, excluding any subtrees, unselect **Search Subtree**.

3. Click **Save**.

Example LDIF content record

The following is a sample LDIF (LDAP Data Interchange Format) content record that shows the uniqueMember group membership attribute being used to define users cn=User1,ou=providers,ou=users,ou=system and cn=Manager1,ou=managers,ou=users,ou=system as members of the group cn=ResourceSupplyManagers,ou=providergrp,ou=groups,ou=system.

```
dn: cn=ResourceSupplyManagers,ou=providergrp,ou=groups,ou=system
objectclass: groupOfUniqueNames
objectclass: top
cn: ResourceSupplyManagers
```

```
uniqueMember: cn=User1,ou=providers,ou=users,ou=system
uniqueMember: cn=Manager1,ou=managers,ou=users,ou=system
```

To assign this group or DN to the Resource Supply Manager Role, go to the Access Control section of the Organizations area and add the `cn=ResourceSupplyManagers,ou=providergrp,ou=groups,ou=system` DN to the Resource Supply Manager role.

Look up a user

The **Look Up User** button allows for the displaying of common LDAP attribute values for a specified user. Also, this button validates the User Login Information (User Name Attribute, User Search Base, and User Search Filter).

Provide the user name attribute value of a user to display that user's DN, common name, display name, email address, and manager.

The lookup also validates the User Name Attribute, User Search Base, and User Search Filter (if attribute information is displayed, these fields are correctly defined).

To look up a user:

1. In the organization's navigation frame, select **LDAP**.
2. Provide all the required LDAP service access information.
3. Click **Save**.
4. Click **Look Up User**.
5. Provide the user name attribute value of a user to look up.
6. Click **Search**.

SAML

SAML (Security Assertion Markup Language) used by Codar is configured in the Management Console.

SAML is used to enable Single Sign-On, which is important for implementing scalable, secure, centralized identities across organizations.

To add SAML support for an organization, click the Organization sidebar menu item and select an organization. In the organization console, select SAML. Enter the SAML URL defined during SAML configuration and save the setting.

For more information about configuring SAML, see the *Configuration Guide*.

For more information about Organizations, see "Organizations" on page 12.

Organization access control

Roles control what a user can accessCodar. For more information about available roles, see "Roles in " on page 1.

Adding a DN to the roles authorizes members of the LDAP directory organizational units access to Codar.

Access control allows you to add or remove directory service groups or organization units (ou) to a Codar role by associating the ou's distinguished name (DN) to the desired role. Authenticated LDAP users, who are members of a group or organization unit that is assigned to a predefined role, can perform specific tasks and access specific parts of Codar .

Only members of a group or organization unit are assigned to the role. To ensure secure role assignment, access control inheritance stops at the assigned organizational unit. This does not follow the traditional directory service pattern where inheritance flows down the organizational unit's hierarchy. Instead, assignments to roles must be assigned to individual organizational units (ou).

A group or organization unit DN can be assigned to more than one role.

LDAP must be configured in order to authenticate users so that they can log in. See "Configure LDAP for an organization" on page 17 for more information.

To add a DN to a role

1. Locate the role to which you want to add a DN.
2. Below the role, click **Add DN**.
3. Provide the following information, and click **Save**:

   To select an existing named DN:

Item	Description
Select from existing named DNs	Select an existing named DN (that identifies a group or organization unit DN) to add to the role. If there are no existing named DNs, this item is not selectable. In order to use the approval process in Codar, you must select a group DN. A group DN is capable of holding members list, from which you can select the users during approval process. Organization unit DNs are not capable of holding members list.

To add a new named DN:

Item	Description
Enter a name for the group or organization unit DN	Enter a name to identify the DN.
Enter a group or organization unit DN	Enter the group or organization unit DN to add to the role. This DN must be relative to the Base DN you configured in the LDAP section of this organization. If the base DN is empty, supply the full DN of the group.

To update a name or DN in a role

1. Locate the role whose DN you want to update.
2. Below the role, locate the DN you want to update.
3. Move your cursor over the DN and click the **Edit** button.
4. In the **Update DN** dialog, update the DN name and/or the DN.
5. Click **Update**.

To remove a named DN from a role

> **Note:** The named DN (group) is not deleted; instead, it is disassociated from the role. You will still see the group when you click **Add DN** and then click **Select from existing named DNs**.

1. Locate the role from which you want to remove a named DN.
2. Below the role, locate the group you want to remove.
3. Click the **Remove DN** icon.
4. Click **Yes**.

Content Store

Use the **Content Store** area in the Management Console to consume and deploy the content from the Codar platform directly, instead of downloading the Content SDK available from Codar.

The content store has access to the latest Codar content offerings published on ITOM Marketplace and the extended community, the same way you access them externally.

Roles

The Content Store area is available for the Content Manager and Administrator.

Capsule Display

The capsules are displayed by the latest updated content offering. Capsules that were updated in the last 30 days have a **New** tag.

The capsules shown in the Content Store depend on which of the following Content Types are selected:

Content Type	Description
HPE	Created by HPE and supported via HPE Software Support, with a ticket filed against the associated product.
Partner	Created and supported by Partners.
Community	Created by Community Contributor and supported by HPE Software customers.

> **Note:** The HPE Content Type is selected by default. The capsules are filtered to be compatible to your version of Codar.

Each Capsule tile shows the following detail:

- Name of the Capsule
- Description about the capsule
- Provider Name (HPE)
- Signature and Certification details of the installed Capsule
- Rating by the user
- Number of Downloads

Prerequisites

1. The Content Store area is only available with the validation of the HPE Passport credentials and proxy connection details (if any). See "Content Store Settings" on page 30
2. Certificate validation for a Capsule (Optional): If you wish to decide the level of certification validation for your chosen Capsule, you may want to edit the configuration property `contentInstallation.contentSignatureVerificationLevel` in the `csa.properties` file located at `JBOSS_HOME\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` to enable or disable. Following are the 3 types of certification validation:
   a. **ALLOW_NOT_SIGNED** - This will allow any capsule including unsecured content without certification to continue the installation process. It is the lowest security level. For example: `contentInstallation.contentSignatureVerificationLevel=ALLOW_NOT_SIGNED`
   b. **ALLOW_SIGNED** - This will allow the Capsule having digital certificate to install irrespective of it stored in Truststore of content-store (Where Capsule certificates of trustworthy sources are added and marked as trusted).
   For example: `contentInstallation.contentSignatureVerificationLevel=ALLOW_SIGNED`
   c. **ALLOW_TRUSTED** - This will allow the Capsule to continue installation only if it has a digital certificate and present in Truststore of content-store. This is the highest level of security as it allows only trusted content to install.
   For example: `contentInstallation.contentSignatureVerificationLevel=ALLOW_TRUSTED`

Tasks

You can perform the following tasks in this area:

- **Search for capsules:** Enter the **Keyword** (name of the capsule/version) in the **Keywords** text box in the left panel. Matching capsules are displayed. If no capsules match the keyword, a **No results found** message is displayed.
- **Install an existing capsule**: Click **Install** in the capsule you want to download, select the version from **Available versions** and click **Install**. After the download and install process completes the installed version appears on the tile. You can then mouse-over on the Certificate icon of the installed Capsule tile to view the Signature and Certification details as shown in the below table:

Capsule Status	Certificate Icon Color	Security Information Example
Signed	Green - Indicates that the certificate signature is successful.	**Certificate status : Trusted Signedby : AddTrust External CA Root**
Not Signed	Gray - Indicates that the certificate signature failed.	**No digital signature**

> **Important:** During upgrade of Codar from 1.70 to 1.80 version, the signature information of the capsules installed in 1.70 will be represented in grayed certificate icon to indicate **<No digital signature>** status.

> **Note:** The **Available versions** drop-down displays the capsule versions published in HPLN. Once you have installed a particular version of the capsule, you will be able to re-install the same version, update to a latest version, but cannot downgrade to a lower version.

- **Update an existing Capsule:** The existing Capsules can be updated to latest versions.

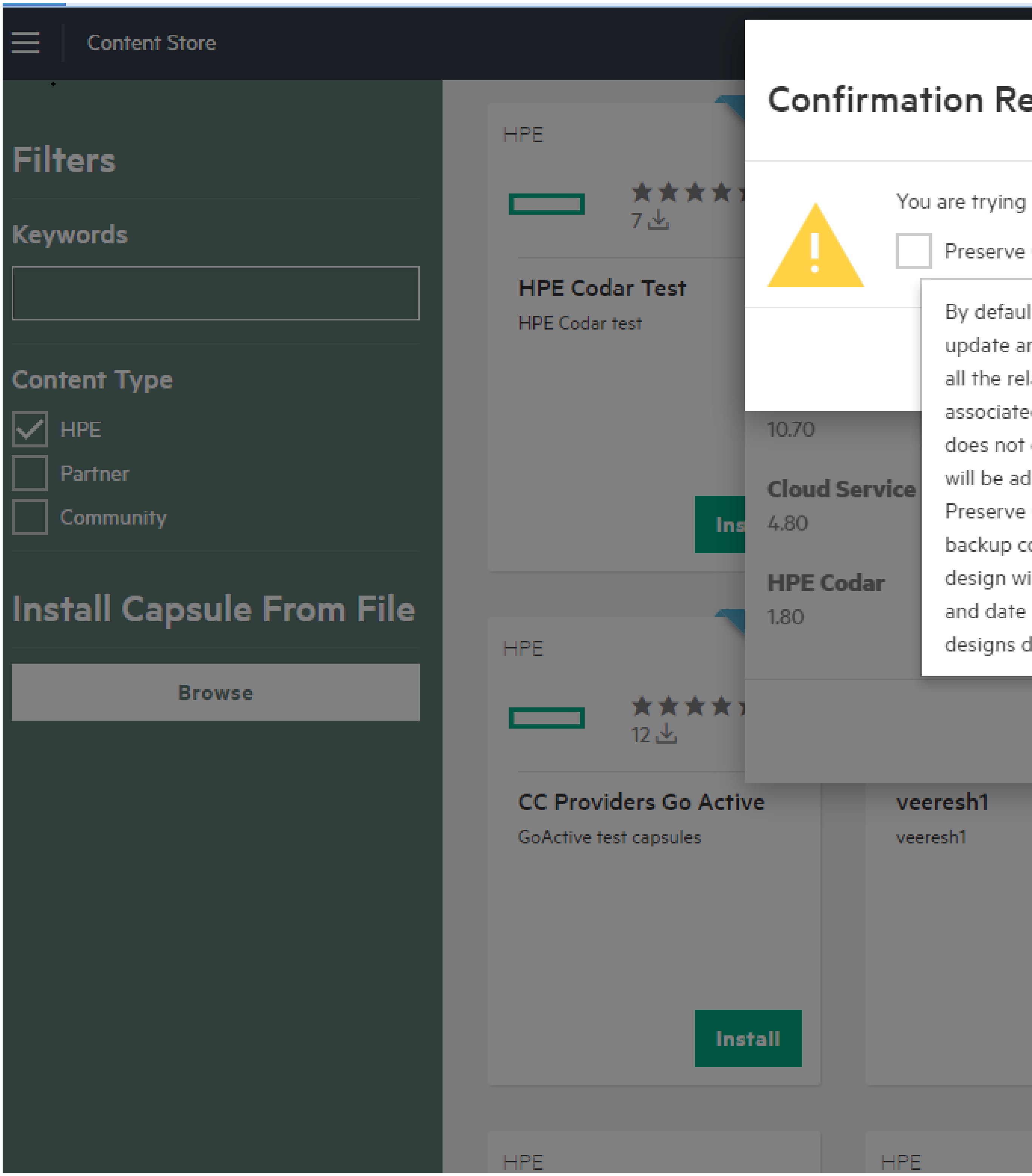
  To update to new version: Click **Update**, select the latest version from **Available versions** and click **Update**.

  > **Note:** The **Update** button is visible for capsules that have later versions available.

- **Reinstall an existing Capsule:** Click **Update**, select the same version from **Available versions** and click **Update**.

  For example: If the existing capsule version is 1.7. You must select the same 1.7 version from the list of Available versions.

  The **Confirmation Required** dialog window will pop-up with **Preserve Originals** option as shown in the below image:


Content Store
Filters
Keywords
Content Type
HPE
Partner
Community
Install Capsule From File
Browse
HPE
7
HPE Codar Test
HPE Codar test
HPE
12
CC Providers Go Active
GoActive test capsules
Install
veeresh1
veeresh1
HPE
HPE
Confirmation Re
You are trying
Preserve
By defaul
update ar
all the rel
associate
does not
will be ad
Preserve
backup co
design wi
and date
designs d
10.70
Cloud Service
4.80
HPE Codar
1.80

- If you check the **Preserve Originals** option and click **OK**. The backup copy of the existing service design will be saved with "Superseded" and date appended to the service designs display name.
- If you choose to continue without checking **Preserve Originals** option and click **OK**. By default, the update operation will update an existing service design and all the related resource offerings associated with it. If the service design does not exist, then the service design will be added to the system.
- If you choose to dis-continue the update process, click **Cancel**.

- **Install a Capsule From File:** You can install the downloaded capsule from your local machine.
  - Click **Browse** and navigate to select the downloaded capsule file.
  - Select the appropriate file and click **Open** to upload it. The uploaded Capsule will appear as a tile for installation.
  - Click **Install** in the capsule that you just uploaded, select the version from **Available versions** and click **Install**

  > **Note:** The selected capsule must be compatible with the 1.80 installer.

- **Update an existing Capsule from a local machine:** If you have downloaded same version or latest versions of a particular Capsule in your local machine, you can update or re-install capsules using the below procedures:
  - To update to latest version: Click **Update**, select the latest version from **Available versions** and click **Yes**.
  - To Re-install the same version: Click **Update**, select the same version from **Available versions** and click **Yes**.

  > **Note:** The pop-up window with an option **Preserve Originals** will not display for updating and Re-installing Capsules from local machine. It is applicable only for Capsules available on ITOM Marketplace.

Locating Content Store Log Files

The Content Store writes operational information to a dedicated log file with the `.log` extension. To view the log files and to help you troubleshoot a specific scenario, navigate to `JBOSS_HOME\standalone\log\contentstore.log`.

Content Store Settings

The **Content Store** section of the **Settings** tile allows you to configure a valid **Marketplace** connection to enable ITOM Marketplace from the Content Store tile. You must have the Administrator role to access and configure these settings.

When this configuration is validated, the Codar Content Manager role can access the Content Store sidebar menu item. See "Content Store" on page 25.

To configure the Content Store settings:

1. In the Settings navigation frame, select **Content Store**.
2. Provide or update the following information:

HPE Passport Credentials

Item	Description
User Name	The HPE Passport account user ID. To register for a Passport ID, go to: https://hpp12.passport.hp.com/hppcf/createuser.do.
Password	The password for the HPE Passport account.

Connection to HPLN

Item	Description
Service Access Point	The URL for connecting to the ITOM Marketplace service: https://marketplace.saas.hpe.com/hpln
Connection Timeout (s)	The time in seconds that the connection remains until a timeout occurs. **Default**: 10
Proxy Server	Specify a proxy server URL, including the port number, only if a proxy is needed to reach ITOM Marketplace.
Proxy User Name	The proxy server user name, if the proxy server needs to be authenticated.
Proxy Password	The password for the proxy server.

3. Click **Validate**.

   The validations pass/fail message appears at the top of the window.

   Validation passed - the settings are all valid and the Content Store sidebar menu item can be enabled.

   Validation failed - one or more settings are not valid and the Content Store remains disabled.

> **Note:** If the validation fails, check the following:
>
> - You have access to the internet through the proxy information you provided.
> - Your HPE Passport credentials are correct.
> - You have permission to access the Codar product page on ITOM Marketplace.

4. Click **Save** when the configuration is validated to enable the Content Store sidebar menu item. See "Content Store" on page 25.

Providers

Providers are management platforms that offer centralized control over the infrastructure and resources used in a cloud computing environment. For example, a provider such as infrastructure orchestration can deploy virtual machines, while a provider such as HPE SiteScope can monitor applications.

A provider corresponds to the specific instance of an application that Codar can integrate with to help instantiate service designs. For example, to enable service designs that target infrastructure orchestration, you must first create a provider (with a provider type of HPE Matrix Operating Environment (Matrix OE)).

Provider types

A provider type allows you to classify providers for improved filtering and identification. CodarCodar includes some predefined, out-of-the-box provider types. Each instance of a provider can have a single provider type, and each instance of a resource offering can also have a single provider type. In addition, resource offerings can be associated only with providers that share the same provider type.

Tasks

You can perform the following tasks in this area:

- **View providers by type.** In the drop-down box, select to view providers **By Type**. Provider types are listed in the left pane. The list of providers contained by the type displays in the right pane. Disabled providers are indicated by the disabled icon and will not be selected when provisioning new services.
- **Manage provider types.** In the drop-down box, select **By Type**. Select the manage icon. For more information, see "Manage provider types" on page 35.
- **Create a Provider.** In the drop-down box, select **By Type**. In the left pane, select **All Providers**, or select the type for which you want to create a provider. In the right pane, select the **Providers** tab. Click **Create** to add a provider with the selected provider type. See "Provider overview" on page 37 for more information about configuring a provider.
- **See more information about a provider.** Click a provider to see more information about the provider.

Best practices

- Locked items cannot be deleted.
- You can select whether to see the content in card view or table view.

Components (per provider type)

The components tab for a selected resource provider type shows all the components available for that provider type. When components are imported into CodarCodar, they are associated with a single provider type, and all provider instances of that type support the component.

> **Note:** Provider components are applicable only to topology designs and are not applicable to sequenced designs.

Tasks

- **View components associated with the selected provider type** - See the list of components in the right pane.
- **Launch the component management area** - Click a component. Or click the **Manage** button (or the **Manage Components** button if no components exist). You must have Service Designer role access to perform this task.

Manage provider types

You can perform the following tasks in this area:

- **Create a provider type.** Provide the information listed in the table below.
- **Edit a provider type.** See the table below for the items you can edit.
- **Delete a provider type.** A provider type cannot be deleted if any resource offerings or providers of that provider type exist. Out-of-the-box provider types also cannot be deleted.

Item	Description
Name	A name that is automatically generated by Codar, and which may be needed when importing components for topology designs.
Display Name	The display name you provide for the provider type.
Description	The description you provide for the provider type.
Image	An image that displays for the provider type. Click **Change Image**. Choose the image you want, and click **Select**. Click **Upload Image** to add your own image. Supported file extensions include `.jpg`, `.jpeg`, `.gif`, and `.png`. The recommended image size is 256 by 256 pixels, and the image will be scaled to the appropriate size. The images are stored in the `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\images\library` folder of the Codar server.

Provider information

Provider overview

You can perform the following tasks:

- **Create or Edit a provider.** In the right pane, select the **Providers** tab. Click **Create** in the main Providers area or click **Edit** in the **Overview** tab. See the table below for the items you can edit.
- **Delete a provider.** Click **Delete**. A provider referenced by topology designs or by topology or sequenced service instances cannot be deleted. All other providers can be deleted, and their associations (to environments and to resource offerings) are automatically removed on deletion. When deleting providers, make sure that any resource offerings referenced by the provider and used in a service design are still associated with at least one provider that can provision the resource offering.

Item	Description
Provider Type	The type selected for this provider. Note that the **Provider Type** cannot be changed after a provider is created.
Display Name	The name you provide for the provider.
Description	The description you provide for the provider.
User ID	The user ID for the specified Service Access Point.
Password	The password for the specified Service Access Point. Re-type the password in the **Confirm Password** field.
Service Access Point	Specify a URL for connecting to the provider. The following examples show how to connect to some common resource providers: • Matrix OE - `https://<MOE server IP>:51443/hpio/controller/soap/<v1/v2/v3>` • HPE Server Automation - `https://<SA server IP>:443` • SiteScope - `http://<SiteScope server IP>:8080` • HPE Universal CMDB - `http://<UCMB server IP>:8080` • VMware vCenter - `https://<vCenter server IP>:443` • Chef - `https://<Chef Server IP>:443` • GitHub - `https://<api.github.com>:443` • GitHub Enterprise - `https://<GitHub Enterprise server IP >/api/v3/:443` • Cloud Management Platform (CMP) - `https://<Cloud Service Automation server>:<CSA port>` When creating or updating a provider, Codar attempts to contact the provider at the

Item	Description
	URL you specify. Codar uses a six (6) second timeout to attempt to validate the provider URL (for HTTP and HTTPS only). If the URL is not successfully contacted before the timeout expires, a validation failure message displays, and you have the option to ignore the validation failure or to correct the URL and try again. Note: User credentials are not validated at this time.
Image	Select an image to be displayed with the provider.
Enabled	This value determines whether the provider will be selected when provisioning a new service. The setting is either **Enabled** (when checked) or **Disabled** (when not checked). When **Disabled**, the provider will not be selected when provisioning new services. Disabling a provider will have no effect on existing services that are using that provider.

Provider properties

Custom properties on a provider can be used to capture additional configuration information about a particular provider. For example, you can use custom properties to model provider resources, such as datacenters, hypervisors, and datastores for a specific VMware vCenter provider.

When a topology design is provisioned, an Operations Orchestration flow can read and write provider property values.

Tasks

Custom properties are optional, and are needed only if the provisioning process requires them. For example, provider properties may be used by HPEOperations Orchestration flows during service provisioning.

- **Create provider properties.** Click **Create**. Provide the information listed in the following table.
- **View property description.** Click the information icon.
- **Edit provider properties.** Click the edit icon. See the following table for the properties you can edit.
- **Delete provider properties.** Click the delete icon.

Item	Description
Type	Select one of the following: • **Boolean** - A property whose value is True or False. • **List** - A property whose value is a list of String values. • **Integer** - A property whose value is a positive or negative whole number or zero. • **String** - A property whose value is a sequence of characters. You cannot change the type of a property after it is created.
	Configure the following items for each property type: ***For Boolean properties:*** • **Name** - A unique name for the property. • **Display Name** - The display name for the property. • **Description** - A description of the property. • **Property Value** - Select **True** or **False**.

Item	Description
	For list properties: • **Name** - A unique name for the property. • **Display Name** - The display name for the property. • **Description** - A description of the property. • **Property Value** - Click the **Add Item** icon to add a new value. Click the **Edit Item** icon to edit the selected value. Or click the **Remove Item** icon to remove a selected value. ***For integer properties***: • **Name** - A unique name for the property. • **Display Name** - The display name for the property. • **Description** - A description of the property. • **Property Value** - Select or type a positive or negative whole number or zero. If you enter a decimal number, the value will be truncated to the nearest integer. The maximum allowed integer value is 2147483647 and the minimum is -2147483648; if you enter a value outside these bounds the value will be automatically converted to the closest maximum or minimum value. ***For string properties:*** • **Name** - A unique name for the property. • **Display Name** - The display name for the property. • **Description** - A description of the property. • **Property Value** - Type a string of characters. • **Confidential Data** - Select this box to mask the values so that they cannot be read in the user interface; no encryption of the value is performed.

Provider environments

You can perform the following tasks:

- **View environments associated with the selected provider.** See the list of environments.
- **Select a resource environment.** Click **Select**. In the dialog box, add or remove resource environments to or from the resource provider.

Resource Offerings

For information about resource providers, see "Providers" on page 32.

> **Note:** Resource offerings are for use with sequenced designs only and are not applicable to topology designs.

Tasks

- **View resource offerings associated with the selected provider** - See the list of resource offerings.
- **Select a resource offering** - Click **Select**. In the dialog box, add or remove resource offerings to or from the resource provider.

Resource Pools

Resource pools create an association between resources that can be provisioned by a provider and subscriptions. You can create a resource pool on a provider to represent a pool of resources associated with that provider. For example, you can create a resource pool on a VMware vCenter resource provider that corresponds to a VMware cluster. You can also model an Matrix Operating Environment infrastructure orchestration resource pool (a pool of CPU, memory, storage, and networking) as a CSA resource pool. You can decide which provider concepts, if any, you wish to model as CSA resource pools; the resource pool concept may not be applicable to all provider types.

When you model resources on a provider in resource pools, you should model them in one of the two fashions described below:

- A single resource pool on a resource provider that models all resources that can be allocated to CSA on this provider
- Multiple resource pools on a resource provider, each of which models its own portion of the total available resources on the provider. For example, if a provider has 2000 GB of Storage available, the sum of the Total Available To CSA for each resource of type Storage on all resource pools associated with the provider should be no greater than 2000 GB.

Tasks

- **View resource pools for the selected provider** - See the list of resource pools and their descriptions. Disabled resource pools are indicated by the **Disabled** label and will not participate in resource allocation processing for new subscriptions.
- **Create a resource pool** - Click **Create**. Provide the information listed in the following table.
- **See more information about a resource pool** - Click the resource pool whose information you want to view.

Item	Description
Display Name	The name you provide for the resource pool.
Description	The description you provide for the resource pool.
Known By Provider As	The name this resource pool is known by in the associated resource provider. For example, if this resource pool corresponds to a VMware vCenter cluster, this value would be the exact cluster name configured in VMware vCenter.
Resource Synchronization	An action that updates the resources in the resource pool by communicating with the associated resource provider. For example, you can use this action to update

Item	Description
Action	the **Total Available To CSA** field of each resource configured on the resource pool based on the actual capacity of each resource as configured on the associated resource provider. For more information, see "Resources for a Resource Pool" on page 46. Click **Select** and search for flows or actions by name (when searching for a flow, the folders searched in the Operations Orchestration library are determined by a property configured in the `csa.properties` file; see the "Action Selection Wizard" property description section in the **Configuration Guide** for more information) or select the process engine from which to select a flow or action. Then, locate and select the flow or action. The **Last Synchronized** field in the **Overview** tab of the resource pool indicates the last time (local client time) a resource synchronization action on a resource pool completed successfully.
Enabled	The availability is either **Enabled** or **Disabled**. When **Disabled**, the resource pool will not be available for allocation of resources for new subscriptions, but disabling a resource pool will have no effect on existing subscriptions.

Best Practices

In the **Overview** tab of the resource pool property sheet, hover your cursor over the **Resource Synchronization Action** value to see the full path of the selected process definition in Operations Orchestration.

Overview for a Resource Pool

You can perform the following tasks:

- **Edit a resource pool** - Click the gear icon and select **Edit**. See the table in "Resource Pools" on page 43 for the items you can edit.
- **Delete a resource pool** - Click the gear icon and select **Delete**. A resource pool cannot be deleted unless the **Current CSA Utilization** for each resource configured on the pool is zero.
- **Refresh a resource pool** - Click the gear icon and select **Refresh**.
- **Synchronize a resource pool** - Click the gear icon and select **Synchronize**. This action automatically updates the **Resources** tab information with the latest information. The **Synchronize** action is available only when a **Resource Synchronization Action** is configured. Resource synchronization does not occur automatically and is performed only on demand. The default timeout for a resource synchronization action to complete is one hour. The timeout is not configurable.

> **Note:** The **Last Synchronized** field in the **Overview** tab of the resource pool indicates the last time (local client time) a resource synchronization action on a resource pool completed successfully. Content in this screen does not automatically update. You must refresh this screen after the resource synchronization action completes.

Resources for a Resource Pool

You can associate the following types of resources with a resource pool. You can also set capacity for the resources listed in the following table:

Resource	Unit of Measurement
CPU	Number of CPUs.
IPv4 Address	Number of IP version 4 addresses.
IPv6 Address	Number of IP version 6 addresses.
License	Number of license keys.
Memory	Megabytes (MB) of memory.
Physical Server	Number of physical servers.
Power	Kilowatts (KW) of power.
Storage	Gigabytes (GB) of disk storage.
Subnet	Number of IPv4 or IPv6 subnets.
VLAN	Number of virtual LAN identifiers.
Virtual Server	Number of virtual servers.

Tasks

- **View resources for a resource pool** - See the list of resources, as well as availability and capacity.
- **Add a resource to a resource pool** - Click **Add**. Provide the information listed in the following table.
- **Edit a resource** - Click the gear icon and select **Edit**. See the following table for the items you can edit.
- **Delete a resource from a resource pool** - Click the gear icon for the resource andselect **Delete**. You cannot delete a resource that is currently in use by CSA—that is, a resource that has a **Current CSA Utilization** value other than zero (0).

Item	Description
Resource Type	Select a resource type to be included in this resource pool. Each resource type can be added to a resource pool one time; after a resource type is added to a pool, then it no longer appears in the drop-down list. Note that you cannot edit this value after the resource has been created.
Resource Availability	Select one of the following: **Available** - Resource is available for selection during provisioning of a service. **Unavailable** - Resource is not available for selection during provisioning of a service. **Unlimited** - Resource is available for use with no restrictions on the number of allocations of this resource.
Total Available to CSA	Type a whole number to indicate the maximum capacity of this resource as provided to CSA by the provider. See "Resources for a Resource Pool" on the previous page for a list of resources and their associated units of measurement. You cannot set this value if **Resource Availability** is set to **Unlimited**.
Current CSA Utilization	Type a whole number to indicate the current CSA utilization of this resource. CSA automatically adjusts this value as allocations occur, but you can also set this value manually if desired. You cannot set this value higher than the value specified for **Total Available to** CSA. See "Resources for a Resource Pool" on the previous page for a list of resources and their associated units of measurement. **Note:** If the **Current CSA Utilization** for a resource is not zero (0), you will not be able to delete this resource or its associated resource pool. Also, you cannot edit this value when a new resource is initially created; however, you can edit it for an existing resource.

Components (per provider instance)

> **Note:** Provider components are applicable only to topology designs and are not applicable to sequenced designs.

Tasks

You can perform the following tasks in this area:

- **View components associated with the selected provider instance.** See the list of components in the right pane.
- **Launch the component management area.** Click a component. Or click the **Manage** button (or the **Manage Components** button if no components exist). You must have Service Designer role access to perform this task.

Environments

Environments are optional and provide a mechanism for grouping providers. The most common grouping patterns include grouping by geographical location, organizational structure, or production readiness. For example, you may want to group providers geographically and create environments such as *East Coast* or *South America*. Or you may want to group providers by their production readiness and create environments such as *Production*, *Development*, and *Test*.

Resource environments restrict the set of resource providers that can be chosen in the package workflow (release pipeline). When provider selection occurs during deployment, only providers belonging to one or more of the environments associated will be eligible for selection. If no environments are associated, provider selection is not restricted based on environment membership.

Tasks

You can perform the following tasks in this area:

- **View providers by environment.** In the drop-down box, select to view providers **By Environment**. Environments are listed in the left pane. The list of providers contained by the environment is displayed in the right pane. Disabled providers are indicated by the disabled icon and will not be selected when provisioning new services.
- **Manage environments.** In the drop-down box, select **By Environment**. Select the manage icon. For more information, see "Manage environments" on the next page.
- **Select providers to include in an environment.** In the drop-down box, select **By Environment**. Select the environment in which you want to include a provider. Click the **Select** button. In the dialog box, add or remove resource providers to or from the environment. If desired, use the drop-down box in the dialog to filter the resource provider list by provider type.

Best practices

- Locked items cannot be deleted.
- You can select whether to see the content in card view or table view.

Manage environments

You can perform the following tasks in this area:

- **Create a resource environment.** Provide the information listed in the table below.
- **Edit a resource environment.** See the table below for the items you can edit.
- **Delete a resource environment.** An environment can be deleted only if it is not associated with a lifecycle stage. When an environment is deleted, its associations to providers are automatically removed.

Item	Description
Display Name	The display name you provide for the environment.
Description	The description you provide for the environment.
Image	An image that displays for the environment. Click **Change Image**. Choose the image you want, and click **Select**. Click **Upload Image** to add your own image. Supported file extensions include `.jpg`, `.jpeg`, `.gif`, and `.png`. The recommended image size is 256 by 256 pixels, and the image will be scaled to the appropriate size. The images are stored in the `%CSA_HOME%\jboss-as\standalone\deployments\csa.war\images\library` folder of the Codar server.

Orchestration

This sidebar menu item launches Operations Orchestration Central.

Cloud Optimizer

Cloud Optimizer is a web-based analysis and visualization tool that analyzes performance trends of elements in virtualized environments. When Cloud Optimizer is integrated with Codar, you can monitor the performance and analyze the capacity, usage, and forecast trends of the virtualized infrastructure.

Tasks

Prerequisites

- You must have Cloud Optimizer installed and properly configured in your Codar environment.

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 Administer (Codar 1.90)

Just add your feedback to the email and click send.

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

We appreciate your feedback!