Cloud Service Automation

Software Version: 4.90

For Linux operating systems

Administer

Document Release Date: May 2017

Software Release Date: May 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

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

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

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

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

Documentation Updates

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

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

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

Support

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

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

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

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

Contents

Organizations

An organization determines a member's entry point into the cloud system and associates its members with services and resources. An organization can be a company, business unit, department, or group.

Membership in an organization is determined by the organization's LDAP (Lightweight Directory Access Protocol) directory. When a user logs in to the Cloud Service Management Console or Marketplace Portal, LDAP authenticates the login credentials by verifying that the user name and password match an existing user in the LDAP directory. The LDAP server used to authenticate users to the Cloud Service Management Console or Marketplace Portal must be set up and configured before authorization can be given to specific roles within CSA. See the *Cloud Service Automation Configuration Guide* for more information.

Configuring the organization's LDAP setting is done in the LDAP tab.

Authorization or abilities of a member of an organization (such as creating a service design or managing cloud resources) are determined by predefined roles in CSA that require assigning group DNs in the LDAP directory. Membership to these group DNs in LDAP automatically gives permission to that role in CSA. These permissions are assigned in the **Access Control tab** for the organization.

There are two types of organizations in CSA:

- **Provider organization** - The provider organization hosts CSA, manages consumer organizations, and manages resources and services, including those offered by third-party or public clouds.

  Using the Cloud Service Management Console, members of the provider organization can create one or more consumer organizations, manage configured organizations, and manage resources and services (such as designing, offering, and publishing resources and services for consumption).

  The organizations, resources, and services that can be managed are determined by the role(s) assigned to the members of the provider organization. For example, the CSA Administrator manages all organizations, resources, and services, while the Consumer Service Administrator manages only consumer organizations. Additional roles include the Resource Supply Manager who manages resource providers and resource offerings, the Service Designer who manages service components and service designs, the Service Business Manager who manages service offerings and service catalogs, and the Service Operations Manager who manages subscriptions and service instances. All of these roles can be found in the Provider Organization's **Access Control** tab.

  There is only one provider organization for each instance of CSA and it is automatically set up during installation. You can modify the provider organization, as needed. You cannot delete the provider organization.

- **Consumer organization** - The consumer organization, using the Marketplace Portal, subscribes to or consumes the resources and services provided by the provider organization. There can be multiple consumer organizations configured by the provider organization. However, each consumer or subscriber sees only the information in the consumer organization of which he is a member. Membership to a consumer organization is determined by the LDAP configuration of the consumer organization.

  At installation, a single consumer organization is set up. Use the Administration tile in the Cloud Service Management Console to modify this default consumer organization, as needed.

See "LDAP" on page 14 and the *Cloud Service Automation Configuration Guide* for more information about configuring LDAP for the provider and consumer organizations.

Administration

In the Cloud Service Management Console, use the Administration tile to manage organizations. This includes the configuration of CSA integration to LDAP for authentication and access control. It is also where you configure customizations to the Marketplace Portal for each organization. From this section, in the upper left corner, you can view the total number of organizations created, including the provider organization.

Informational Icons

Icon	Description
	When this icon is adjacent to an organization, it indicates the provider organization. There can be only one provider organization and it is automatically configured. You can modify the provider organization, as needed. You cannot delete the provider organization. When this icon is adjacent to a catalog, it denotes the global catalog. There can be only one global catalog and it is visible to all organizations. You may modify the global catalog, 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.

Create an organization

Only consumer organizations may be created. To create an organization:

1. Click **Create Organization** in the left navigation frame and enter a name for the organization.
2. Click **Create**.
3. "Create an organization".

   You may need to configure additional steps to configure the Marketplace Portal for this organization. Refer to the *Cloud Service Automation Configuration Guide* for more information.

View an organization

This summary view shows each of the basic areas of configuration for an organization, including which areas need configuration and which have already been configured.

To 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

To 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.

Navigate through following topics for detailed information:

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 Portal Customization, LDAP, Access Control, or Email Notifications.

Viewable Summary Information

Section	Displayed Summary Information
Portal Customization	Application Name- The name of the organization that appears in the Marketplace Portal. This section is not available to the provider organization.
LDAP	• Hostname - The hostname used to connect to the LDAP server. This can be the fully qualified domain name of the server, the IP address, or the hostname needed for the CSA server to resolve the host where the LDAP service is running. • 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.

General information

General information appears at the top of the organization's page in the Cloud Service Management Console. To change the appearance of the Marketplace Portal, click the **Portal Customization** section (see "Portal customization" on the next page).

To configure general information about 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 CSA assigns to the organization. For a consumer organization, this name is based on the name entered when the organization was created. This identifier is used in the URL used to access the Marketplace Portal, as seen in the next field. See the *Cloud Service Automation Configuration Guide* for

Item	Description
	more information.
Organization URL	A URL for connecting to the Marketplace Portal for the organization.
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 may appear in the following locations: ◦ The **Cloud Service Management Console** - Top left of an organization's page. ◦ The **Marketplace Portal** - Top left of the login screen and top left of each portal page. From the **Select Image** screen, 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 CSA server.

3. Click **Save**.

Portal customization

Portal customization allows you to customize an organization's Marketplace Portal.

> **Note:** This section is not available to the provider organization.

To customize the Marketplace Portal

1. In the organization's navigation frame, select **Portal Customization**.
2. Provide or update the following information for portal customization:

Application Labeling

Item	Description
Application Name	Type a name that displays on the login screen and header of your organization's Marketplace Portal.
Portal Welcome Message	Type a welcome message that displays below the Application Name when a user logs into your organization's Marketplace Portal.
Copyright Statement	Type a copyright statement that displays on the login page below the Log In button of your organization's Marketplace Portal.

External Organization Links

Item	Description
Privacy Statement Link	Type the link to your organization's privacy statement that appears on the login page below the copyright statement.
Show Privacy Statement on Marketplace Portal	Check the box to display the privacy statement link on the login page of your organization's Marketplace Portal.
Terms and Conditions Link	Type the link to your organization's terms and conditions statement that appears when a subscriber is ordering a service.
Show Terms and Conditions on Marketplace Portal	Check the box to display the terms and conditions link when a subscriber is ordering a service.

Application Enhancements

Item	Description
Featured Category	Select a featured category to use when displaying service offerings in the Marketplace Portal. Service offerings in this category will display in the Featured Services tile of the Marketplace Portal.
Subscription End Date Options	◦ **Allow Recurring Subscriptions** - Check the box to allow recurring subscriptions, rather than requiring all subscriptions to be term subscriptions. ◦ **Max Term Subscription Period (months)** - Select the maximum number of months (between 1 and 12) allowed for term subscriptions. When subscribers request a term subscription, they will not be able to specify an end date that is more than this number of months past the start date. For example, if the

Application Enhancements, continued

Item	Description
	subscriber selects a requested start date of June 15 2014, and **Max Term Subscription Period (months)** is set at its default value of 12, the requested end date cannot be later than June 14, 2015. This setting has no impact on recurring subscriptions.
History Details	Select the **Show Verbose Errors** box to display the status of the actions executed during the lifecycle of a service.

Themes

Item	Description
Theme	Select a theme or type the name of a customized theme for your organization's Marketplace Portal. Themes define colors, fonts and the general look-and-feel of the Marketplace Portal. The following themes are shipped out-of-the-box: ◦ Simplified ◦ Enterprise ◦ Playful ◦ Custom - Select **Custom**, and type a custom theme name in the text box. This name must match the name used to create the custom theme outlined in the guidelines for creating a custom theme. See the "Custom Themes" section in the *Customizing the Marketplace Portal* guide for specific information about configuring a custom theme.

Security Settings

Item	Description
Security Classification	Select from the following security banner options: ◦ **No Banner** - no banner displays in the Marketplace Portal. ◦ **Unclassified** - The banner is light green and contains no content. ◦ **Unclassified FOUO** - For official use only. The banner is light green and displays the text "FOUO." ◦ **Unclassified NOFORN** - Not releasable to foreign nationals. The banner is light green and displays the text "NOFORN." ◦ **Confidential** - The banner is light blue and displays the text

Security Settings, continued

Item	Description
	"CONFIDENTIAL." ◦ **Confidential FOUO** - The banner is light blue and displays the text "CONFIDENTIAL-FOUO." ◦ **Confidential NOFORN** - The banner is light blue and displays the text "CONFIDENTIAL-NOFORN." ◦ **Secret** - The banner is red and displays the text "SECRET. ◦ **Top Secret** - The banner is orange and displays the text "TOP SECRET."
Disclaimer	Type text for the disclaimer for your organization's Marketplace Portal. The disclaimer appears on the login page of the Marketplace Portal.

3. Click **Save**.

Dashboard Widgets

Create and edit custom tiles for your organization's Marketplace Portal dashboard. These tiles appear only in the **Discover More** section of the Marketplace Portal.

> **Note:** This section is not available to the provider organization.

To create or update dashboard widgets

1. In the organization's navigation frame, select **Dashboard Widgets**.
2. To create a widget, click a button listed in the following table. Or click **edit** for the item you want to update. The edit and disable buttons are only visible when you select or hover over the widget.
3. Provide or update the following information:

Button	Description
Add Link	Provide or change the following: • Name - The name associated with this link in the Cloud Service Management Console. • Title - The text that displays for the link in the Marketplace Portal.

Button	Description
	• URL - The URL that the link references in the Marketplace Portal. • Icon URL - The URL of an icon that displays near the center of the widget in the Marketplace Portal. • Background Image URL - The URL of an image that fills the background of the widget in the Marketplace Portal. • Target - The target attribute of the `<link>` element that appears in the Marketplace Portal and that controls the browser window in which the link will open. Valid values for the target attribute are defined in the HTML specification.

Add Mashup	Provide or change the following:
	• Name - The name associated with this widget in the Cloud Service Management Console.
	• Content - The HTML and JavaScript code for the mashup.
	When using iFRAME in a mashup widget, note the following:
	• iFrames that serve HTML pages that have the same URL structure as the Marketplace Portal will work properly. The same URL structure means that the pages are placed in the following directory:
	`%CSA_HOME%\portal\node_modules\mpp-ui\dist`
	For example, to correlate to the following URL structure:
	`https://server:8089/widgets/sample/index.html`
	You would place your pages in the following location:
	`%CSA_HOME%\portal\node_modules\mpp-ui\dist\widgets\sample\index.html`
	• iFrames that serve external NON-HTTPS content will be blocked by the browser. The specific error will vary based on client browser security.
	• iFrames that serve external HTTPS content that contains mixed HTTP and NON-HTTPS content will be blocked by the browser. The specific error will vary based on client browser security.
	• iFrames that serve external HTTPS content will work only if the following are true:

Button	Description
	◦ The remote site must not specify `x-frame-options DENY` in the response header. ◦ If the content is not of the same origin domain, and the remote site has not `specified x-frame-options SAMEORIGIN`, the content will display properly.
Add Featured Service	Adds a tile to the Marketplace Portal dashboard that contains a random service offering in the featured category configured for your organization. Provide or change the following: • Name - The name associated with this widget in the Cloud Service Management Console.

LDAP

LDAP (Lightweight Directory Access Protocol) used by CSA is configured in the Cloud Service Management Console.

LDAP is used to:

- Authenticate a user's login to the Cloud Service Management Console or Marketplace Portal
- Authenticate a user's access to information
- Authorize a user's access to information

To completely configure access to CSA, you must configure LDAP to authenticate a user's login, configure LDAP for an organization to authenticate a user's access to information, and configure access control for an organization to authorize a user's access to information.

From this page you can:

- Configure LDAP for authentication to log in to CSA.
- Configure LDAP to access information in CSA.

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 Cloud Service Management Console. And, when you configure LDAP for the consumer organization, you are configuring the set of users who can log in and be authenticated to perform actions in the Marketplace Portal.

To configure authorization to access information in CSA for organizations, see "Access control" on page 19.

For more information about organizations, see "Organizations"

To configure LDAP

> **Note:** If you are configuring CSA to be compliant with FIPS 140-2, configure CSA for FIPS 140-2 compliance before configuring this item. Refer to the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide* for more information.

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

> **Note**: The LDAP configuration fields are unavailable for editing when the `csa.ldapReadOnly` property is enabled. For information about the property, see the *Cloud Service Automation Configuration Guide*. For information about the LDAP Configuration Tool, used to configure the LDAP access point from the command line, see the *Cloud Service Automation LDAP Configuration Tool* guide.

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.
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 requre a User ID or password for authentication, this value can be omitted. Example: `uid=admin@xyz.com,ou=People,o=xyz.com`

Item	Description
Password	Password of the User ID. If the LDAP server does not requre 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, authentication, and approvals in CSA.

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 logged in user in the Marketplace Portal. If no avatar is specified, a default avatar will be used.

User Login Information

CSA uses a user search-based login method to authenticate access to information.

Item	Description
User Name Attribute	The name of the attribute of a user object that contains the username that will be used to log into the Cloud Service Management Console or Marketplace Portal. 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 to the Cloud Service Management Console or Marketplace Portal. 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 to the Cloud Service Management Console or Marketplace Portal, 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 the **Search Subtree** checkbox selected. If you want to restrict the search for a matching user to only the **User Search Base**, excluding any subtrees, unselect the **Search Subtree** checkbox.

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 Administration 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 CSA is configured in the Cloud Service 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 tile 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 *Cloud Service Automation Configuration Guide*.

For more information about organizations, see "Organizations"

Access control

Roles control what a user can access in CSA. For more information about available roles, see the *Welcome to Cloud Service Automation* topic in this help system. Adding a Distinguished Name (DN) to the roles authorizes members of the LDAP directory organizational units access to the Cloud Service Management Console or Marketplace Portal. If a user has access to the Cloud Service Management Console, a user may have access to one or more of the functional areas in the console. If a user has access to the Marketplace Portal, a user has access to all areas in the portal.

Access control allows you to add or remove directory service groups or organizational units (ou) to a CSA role by associating the ou's DN to the desired role. Authenticated LDAP users, who are members of a group or organizational unit that is assigned to a predefined role, can perform specific tasks and access specific parts of the Cloud Service Management Console or access the Marketplace Portal.

Only members of a group or organizational 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 organizational 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 to the Cloud Service Management Console and Marketplace Portal. Refer to "LDAP" on page 14 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 organizational unit DN) to add to the role. If there are no existing named DNs, this item is not selectable.

To add a new named DN:

Item	Description
Enter a name for the group or organizational unit DN	Enter a name to identify the DN.
Enter a group or organizational unit DN	Enter the group or organizational 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**.

Email notifications

An email notification is sent when there is a change to the subscription status, when a request needs to be approved or denied, or when a request has been approved or denied. The automatically-generated email message is sent to users who have been configured to receive notifications. The same email notification is also sent to the Marketplace Portal and can be viewed in the **Notifications** area of the Marketplace Portal. In order for these email notices to be sent, the SMTP Server Setting must be configured for the organization.

From the Email Notifications page, configure the SMTP server used to send email notifications. You can also configure the sender for the organization email notifications and text added to the beginning of the subject line of the notification.

To configure the mail server for CSA

> **Note:** If you are configuring CSA to be compliant with FIPS 140-2, configure CSA for FIPS 140-2 compliance before configuring this item. Refer to the *Cloud Service Automation FIPS 140-2 Compliance Configuration Guide* for more information.

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

SMTP Server Settings

Item	Description
Hostname	The fully-qualified domain name (server.domain.com) or IP address of the SMTP-compliant mail server that acts as the gateway for email notifications.
Port	The port used to connect to the mail server when sending email notifications. The default SMTP port number of 25 should be changed only if your email server has been specifically configured using a non-standard port.

Connection Security

Item	Description
SSL	If the mail server is configured to require https (http over SSL), select the **SSL** checkbox.
Requires	If the mail server requires you to log in before accessing it, select the **Requires**

Connection Security, continued

Item	Description
Authentication	**Authentication** checkbox and provide the following information: ◦ **User ID**: User whose account is used to email notifications from the mail server. ◦ **Password**: Password of the user account.

Email Source Settings

Item	Description
Sender Email Address	Email address to be used as the sender of the email notification.
Subject Prefix	Text added to the beginning of the subject line of the email notification.

Subscription Expiration Notification

Item	Description
Notification Before a Subscription Expires	From the drop-down list, select how far in advance a subscriber will be notified before a subscription expires.

3. Click **Save**.

Operations

The operations section allows you to configure operational settings and notifications for your organization.

> **Note:** This section is not available to the provider organization.

To configure operations settings for an organization

1. In the organization's navigation frame, select **Operations**.
2. Provide or update the following information and then click **Save**.

Item	Description
Provisioning Error Handling	Select one of the following: • **Fail Subscriptions On Provisioning Errors** - When an error occurs during provisioning, the configured Failure substate actions run, and the subscription is

Item	Description
	marked as Failed in both the Marketplace Portal and the Operations area of the Cloud Service Management Console. • **Pause Subscriptions On Provisioning Errors** - When an error occurs during provisioning, the provisioning process stops, and the subscription is marked as Pending in the Marketplace Portal and as Paused in the Operations area of the Cloud Service Management Console. You can troubleshoot the cause of the failure and then resume or cancel the paused subscription. For more information, see the topic "View Service Topology for a Subscription" in the Operations Help. > The resume behavior is different for subscriptions depending on how the underlying service design was created. • Most sequence based designs contain fine-grained lifecycle actions; therefore, the provisioning is able to resume from the specific lifecycle action that failed during deployment, and actions that have already succeeded are not repeated. • For topology designs, the behavior is always Fail Subscriptions on Provisioning Errors, regardless of the organization setting.
Paused Subscription Notifications	Select any of the following that apply: • **Notify Subscribers** - The first time a subscription is paused, subscribers receive an email message (as configured in "Email notifications" for the consumer organization), and a notification displays in the Marketplace Portal. • **Notify Operators** - Whenever a subscription is paused, operator users receive an email notification (as configured in "Email notifications" for the CSA-Provider organization).
Operator Users To Notify When Paused	This section lists the user names and email addresses of operator users who have been configured to be notified when a subscription is Paused. To add operator users to notify when a subscription is paused: 1. Click **Add Operator Users**, and do one of the following: ◦ Select one or more operator users, which are members of the Service Operations Manager role as configured for the CSA-Provider organization in "Access control". This list shows users who have logged into the Cloud Service Management Console at least one time, are LDAP users, and are members of the Service Operations Manager role as configured for the CSA-Provider organization in

Item	Description
	"Access control". Note that if a user has logged in and has been recently added to the role, it may take 30 minutes (based on the default LDAP cache configuration value in the `csa.properties` file) for the user to appear in the selection list. If the user you want to add has not yet logged in to the Cloud Service Management Console or is recently added to the Service Operations Manager role, you can manually add the user by typing a user name, as described below. ◦ Or, enter a user name manually by typing a user name in the text field. 2. Click **Save**.

Catalogs

View the catalogs that are associated with this organization. If you manage more than one organization, this view filters the catalogs you manage by organization. This is a read-only view.

The global catalog is visible to all organizations, including the provider organization.

Delete an organization

Only consumer organizations may be deleted. In order to successfully delete a consumer organization, its catalogs must not contain any published service offerings.

1. In the left navigation frame, select the organization to delete.
2. In the organization's navigation frame, select **General Information**.
3. Click **Delete**.
4. In the **Delete Organization?** dialog, click **Yes** to delete the organization.

Settings

Use the **Settings** tile in the Cloud Service Management Console to manage the Content Store settings for the ITOM Marketplace **Content Store** tile. The CSA Administrator is the only role that can access the Settings tile.

Tasks

You can perform the following task in this area:

- **Configure the Content Store** - in the left pane select **Content Store** to configure ITOM Marketplace in order to activate the Content Store tile. See "Configure Content Store settings" below.

Informational Icon

Icon	Description
*	Indicates the field is required, and you must enter information in order to successfully complete the configuration.

Configure 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 CSA Content Manager role can access the Content Store tile. See "Content Store" on page 27.

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,

HPE Passport Credentials, continued

Item	Description
	click here.
Password	The password for the HPE Passport account.

Connection to ITOM Marketplace

Item	Description
Service Access Point	The URL for connecting to the ITOM Marketplace service: https://marketplace.microfocus.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 tile 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 CSA product page on ITOM Marketplace.

4. Click **Save** when the configuration is validated to enable the Content Store tile. See "Content Store" on the next page.

Content Store

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

The content store has access to the latest CSA content offerings published on ITOM Marketplace and the extended community, the same way you access them externally. Refer to "Using Content Store with ITOM Marketplace" on page 31 for information on how to use Content Store with ITOM Marketplace.

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 CSA.

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 "Configure Content Store settings" on page 25
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`

> **Note**: A separate Truststore is created at the location `CSA_JRE_HOME/lib/security/capsuletrust` to validate the Capsule signatures. By default, the HPE-released capsule signature certificates are imported at this location. However, if you want to validate your capsules that you have signed using different certificate/s as "TRUSTED", you can use the Java™ `keytool` command and import the certificates to the Truststore location.

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 CSA from 4.70 to 4.80 version, the signature information of the capsules installed in 4.70 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 ITOM Marketplace. 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.

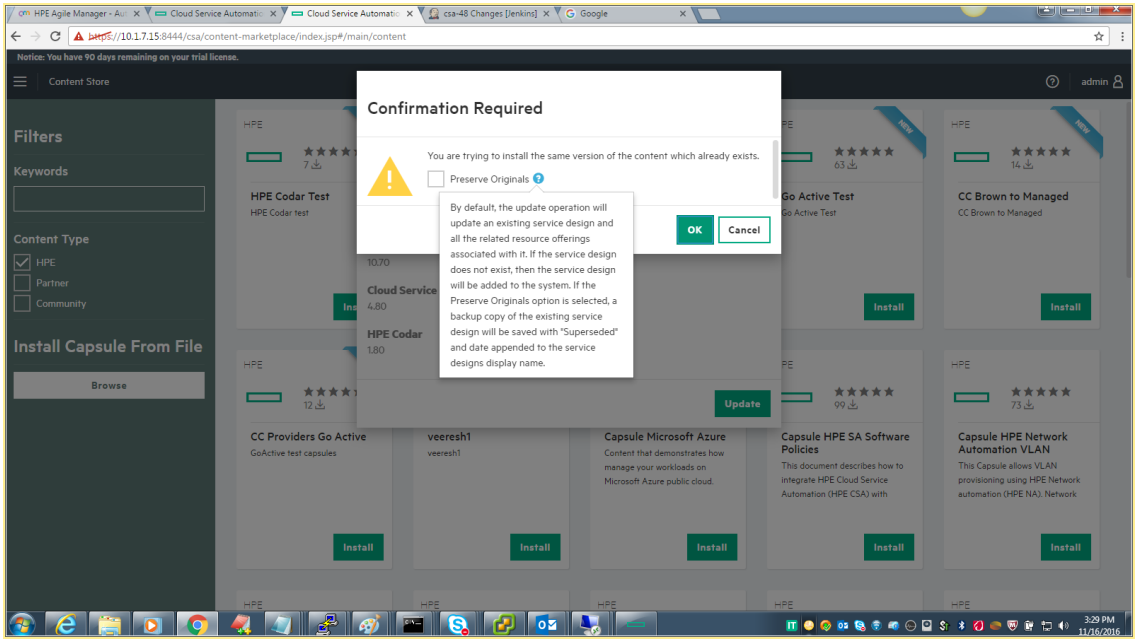
  To update to new version: Click **Update**, select the latest version from **Available versions** and click **Update**.

  > **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 4.7. You must select the same 4.7 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



- 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 4.80 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.

Capsule-specific Documentation

You can download the capsule-specific documentation right from the capsule install tile itself. All the capsule-related user manuals hosted through ITOM Marketplace will be listed under the **Documents** section in the capsule install tile. If no document is hosted for a capsule through ITOM Marketplace, the **Documents** section will not be visible.

Downloading capsule-specific documentation

To download any of the available capsule-specific documentation:

1. From the **Content Store** page, click the **Install** or **Update** button (as the case may be) of the capsule . The install tile appears.
2. In the install tile, from the **Available Versions** drop-down list, based on the documentation you need to download, select the respective capsule version. The **Documents** section now lists links of all the available user manuals, related to the selected capsule and capsule version.
3. Click the desired link.
   The document will be downloaded to your default 'Downloads' folder.

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`.

Using Content Store with ITOM Marketplace

Due to the unavailability of HPE Live Network, the Content Store too became nonfunctional. Now, the new ITOM Marketplace is in place which replaces the HPE Live Network.

Changes to be done in environments with earlier releases of CSA/Codar

To continue using Content Store with earlier releases of CSA/Codar, you need to make only one change in your CSA/Codar environment, which is trusting the new ITOM Marketplace's certificate.

Trusting the ITOM Marketplace involves the following two tasks:

- Exporting the ITOM Marketplace certificate
- Importing the ITOM Marketplace to CSA/Codar environment

Exporting ITOM Marketplace certificate

Refer to the documentation of your browser to know how to export a certificate. You need to export the entire certificate chain available in the **Certificate** dialog.

Importing ITOM Marketplace certificate

For a non-containerzied environment, complete the following steps to import the certificates

1. Copy the exported certificate archive to the CSA host server (any accessible location on the host).
2. Open a command prompt and change directories to CSA_HOME.
3. Run the following command:

   Windows:

   ```
   <CSA_JRE_HOME>\bin\keytool.exe -importcert -trustcacerts -alias <alias_name> -
   file <full_path_to_certificate_file> -keystore <CSA_JRE_
   HOME>\lib\security\cacerts -storepass <store_password>
   ```

   Non-Windows:

   ```
   <CSA_JRE_HOME>/bin/keytool -importcert -trustcacerts -alias <alias_name> -file
   <full_path_to_certificate_file> -keystore <CSA_JRE_HOME>/lib/security/cacerts -
   storepass <store_password>
   ```

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

For a containerized environment, complete the following steps to import the certificatse

1. Copy the exported certificates to `/etc/hcm/cacerts`directory.
2. Restart the CSA pod.

This completes the task of trusting ITOM Marketplace certificate.

Cloud Analytics

HPE IT Business Analytics automatically gathers metrics from CSA to build key performance indicators. It provides scorecards and dashboards so that Resource Supply Managers and Service Business Managers have insight into how to measure and optimize the cost, risk, quality and value of IT services and processes.

In CSA, the Administrator, Resource Supply Manager, and Service Business Manager roles have access to the Cloud Analytics tile in the dashboard. Clicking on the tile displays the next level of tiles, which are :

- **Resource Analytics tile** - Click this tile to launch a report that measures the cost and usage of resource providers in CSA. Administrators and Resource Supply Managers use this tile.
- **Service Analytics tile** - Click this tile to launch a report that measures the revenue, cost, and profit margin for business services in CSA. Administrators and Service Business Managers, use this tile
- **Showback Report tile** - Click this tile to view a showback report for an organization. Administrators and Service Business Managers use this tile.
- **Advanced Reporting tile** - Click this tile if you want to launch a standalone version of HPE IT Business Analytics in a separate window. Also, this tile allows you to perform more advanced operations, such as running custom reports and drilling down into additional details about information provided in the report. Administrators, Resource Supply Managers, and Service Business Managers use this tile.

Prerequisites

- You must have HPE IT Business Analytics installed and properly configured in your CSA environment. See *Cloud Service Automation Configuration Guide* for more information on how to enable HPE IT Business Analytics in your CSA environment.

Resource Analytics

Click this tile to launch a report that measures the cost and usage of resource providers in CSA.

Service Analytics

Click this tile to launch a report that measures the revenue, cost, and profit margin for business services in CSA.

Showback Report

Click this tile to view a showback report for an organization.

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 CSA, you can monitor the performance and analyze the capacity, usage, and forecast trends of the virtualized infrastructure.

In CSA, the Administrator, Service Designer, Service Business Manager, Resource Supply Manager, and Service Operations Manager roles have access to the Cloud Optimizer tile in the dashboard.

Prerequisites

- You must have Cloud Optimizer installed and properly configured in your CSA environment. See the *Cloud Service Automation Configuration Guide* for more information on how to enable Cloud Optimizer in your CSA 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 (Cloud Service Automation 4.90)

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!