Patch Readme - Linux

HP Cloud Service Automation

Software version: CSA 4.50.0001 Patch

Publication Date: August 2015

Introduction

This document provides patch installation instructions for HP Cloud Service Automation Server (CSA) 04.50.0001 on Linux environments and describes the changes that were made to CSA version 4.50 in this update. The cumulative patch will update HP Cloud Service Automation Server to 04.50.0001.

This software patch applies to CSA version 04.50.0000 and is intended to improve the overall performance of CSA 4.50.

Table of Contents

Fixed issues

The following table describes the fixed issues available in this patch.

Table 1. Fixed Issues

Change Request	Description of fixed issue
QCCR1D170695	**Symptom:** The internal action - 'Build Resource Provider and Pool List' fails to select a valid Resource Pool when used with multiple resource providers **Resolution:** The CSA 3.2 internal action 'Build Resource Provider and Pool List' should support multiple Providers and select a valid Resource Pool.
QCCR1D190452	**Symptom:** Service Offering with a wide Optionsets takes long time to load in the MPP **Resolution:** Service offering with wide Option models will load quicker.
QCCR1D194880	**Symptom:** In CSA 4.10, the selected background image for the "Dashboard Widgets" is ignored and the background remains white in MPP. **Resolution:** HP has reviewed this change request. After careful consideration regrettably HP has determined the requested change will not be addressed within the product.
QCCR1D194983	**Symptom:** If the Subscriber Option properties that are set to invisible in the Service Design they will reappear after the visibility of the overlaying option in the Service Offering changed. **Resolution:** The visibility of the options in the portal are made consistent with their settings in the Offering UI
QCCR1D208427	**Symptom:** User should be able to view the properties of a canceled subscription **Resolution:** The backend code was modified to show the properties when the subscription is in cancelled state as well. Now on the services page the component properties will be shown even if the subscription is cancelled.
QCCR1D208611	**Symptom:** After Old subscriptions are deleted from MPP and CSM and using db purge tool to cleanup db, still in MPP > Notifications there are still plenty of logs left from before **Resolution:** Corrected the behavior with the required code changes.
QCCR1D208830	**Symptom:** Subscriber Option values from dynamic JSP pages are not loading when propertyName string used **Resolution:** Code problem was fixed

Change Request	Description of fixed issue
QCCR1D209136	**Symptom:** When the customer executes the following API call, they get a subscription count 1: https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&requestor=pvrbican_m&returnRetired=true&creationStartDate=2015-03-11T23:59:59 After they add the creationEndDate parameter and execute the API call (and use the same startDateParameter) they get a subscription count 87 (also see attachment: https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&requestor=pvrbican_m&returnRetired=true&creationStartDate=2015-03-11T23:59:59&creationEndDate=2015-03-17T23:59:59 **Resolution:** Modified the HQL query to solve the issue
QCCR1D209782	**Symptom:** In CSA 3.2 The 'Cancel Subscription' button is still available to the end-user. If the user clicks 'Cancel Subscription' again (as they have been trained to do in this instance), CSA will continue with the next actions in the de-provisioning lifecycle. In CSA 4.2 this option is not availble. Customer is requesting this feature back and does not see this as an enhancement, customer states that this is a defect and is afecting their future upgrade scheduled for July 10th. **Resolution:** Cancel Subscription button should be enabled in MPP UI if a subscription cancellation fails.

Known issues

The following table describes the remaining known issues in this patch.

Table 2. Known Issues

Change Request	Description of known issue
QCCR1D210391	**SYMPTOM DESCRIPTION:** Elastic Search does not work after installing CSA 4.5 Patch 1 when CSA 4.5 is configured in a high availability mode. **RESOLUTION DESCRIPTION:** Manual configuration changes are necessary for making Elastic Search work after installing CSA 4.5 Patch 1. These are described below: **How to configure Global Search (Elasticsearch) in HA Cluster** In CSA 4.5 Global search is disabled by default. Please refer to CSA Configuration Guide Chapter 7: The Marketplace Portal for details on enabling global search. When turning on Global Search in HA cluster, there are additional steps required.

Change Request	Description of known issue
	In 4.5 MR, strictSSL is not supported for elasticsearch in standalone or HA cluster mode. In 4.5 Patch 1, strictSSL is supported for both standalone and HA mode as long as certs are properly configured. **Enabling global search in HA configuration for 4.5 Patch 1.** 1. Replace csa.properties csa.provider.msvc.hostname with local node FQDN 2. Replace csa-search-service/app.json ccue-basic-server.host with local node FQDN 3. Replace csa-search-service/app.json msvc-basic-search.searchEngineURL with local node FQDN *If the cluster setup is using default CSA (self-signed) certificates complete the following 2 steps. (These 2 steps are not required if the cluster runs valid certificates signed by a common CA)* 4. Change csa-search-service/app.json msvc-basic-search.strictSSL/rejectUnauthorized: false 5. Change elasticsearch/config/elasticsearch.yml searchguard.ssl.transport.http.enforce_clientauth: false *Verify the following HA configurations in csa-search-service/app.json are maintained after the installation of the patch.* 6. idmURL should point to the load balancer *example:* *"idmURL": "https://http-loadbalancer.csapcoe.hp.com:8443/idm-service"* *Port 8443 is the Load balancer port which was configured manually during CSA 4.5 MR installation.* 7. cert should point to the load balancer cert *example:* *"ca": "C:/Program Files/Hewlett-Packard/CSA/jboss-as/standalone/configuration/apache_csa.crt"* *Name of crt cannot remain as jboss.crt which is set as default.* *For more information on setting up certificates please refer to the following documents:* *FIPS 140-2 Compliance Configuration Guild* *CSA 4.5 Cluster Configuration for High Availability Using an Apache Web Server*
QCCR1D210453	**SYMPTOM DESCRIPTION:** Option Model property editor for Topology Designs would allow users to select token values for List type properties based on dynamic options JSP files. After selecting a token value, users are able to modify the token value in the value input field. Modifying token values in Option Model property editor causes problems when retrieving property values from Marketplace Portal during service creation. **WORKAROUND:** Do not edit token value after selecting a token from available list of token for List type properties in Option Model property editor.
QCCR1D210590	**SYMPTOM DESCRIPTION:** Various issues are seen when using Google Chrome version 44 to browse Service Management Console and Marketplace Portal when CSA is setup with self signed certificates.

Change Request	Description of known issue
	1. After browsing for about ten minutes, the browser is automatically redirected to a security page with title "Your connection is not private" where users usually trust self signed certificates. 2. After browsing for some time, blank pages are displayed when navigating from one page to another. 3. An error message such as "An error has occurred. Cannot connect to the server. Check your network connection please" is displayed after browsing for some time. **WORKAROUND:** Versions of Google Chrome prior to version 44 do not have these problems. Other browsers such as Internet Explorer and Mozilla Firefox also do not have these problems. On Google Chrome version 44, trusting the self signed certificate by adding the certificate to 'Trusted Root Certificate Authorities' also seems to be solving this issue.
QCCR1D210850	**SYMPTOM DESCRIPTION:** After installing CSA 4.5 patch, the patch uninstallation shortcut is not added to the start menu on Windows 2012. **WORKAROUND:** In order to uninstall just the patch, please use one of following two options: 1) In "Control Panel" and "Add or remove programs", use "HP Cloud Service Automation Patch" or "HP Codar Patch" to uninstall just the patch. 2) Use 'Uninstall HP Cloud Service Automation Patch.exe' uninstallation binary present in <CSA_INSTALL_DIR>_CSA_4_50_1_installation\Uninstaller\ folder.
QCCR1D211195	**SYMPTOM DESCRIPTION:** Service topology view of a service subscription from Marketplace Portal does not show the state of a service component when users hover upon the icon which displays state of the service component. This problem is only limited to Internet Explorer 11. **WORKAROUND:** This problem is only limited to Internet Explorer 11. State of a service component is visible when using Google Chrome or Mozilla Firefox browsers to view the service topology view of a service subscription by hovering on a service component state icon.
QCCR1D211202	**SYMPTOM DESCRIPTION:** CSA ships a few out of the box OpenStack Service Designs. These Service Designs utilize dynamic option JSP files in Option Model. Opening a Service Offering based on these designs for the purpose of ordering a service from Marketplace Portal leads to the webpage being frozen. When this happens users are unable to order a service from this Service Offering. **WORKAROUND:** Logging out of Marketplace Portal and logging back in fixes this issue.

Enhancements

The following table describes the fixed issues available in this patch.

Table 3. Fixed Issues

Change Request	Description of fixed issue
QCCR1D188066	**Symptom:** Inability to read the catalog ID in the dynamic query JSPs, by adding the SVC_CATALOG_ID token to the list of available tokens in the dynamic query http body. **Resolution:** The catalog ID - *[PORTAL: CATALOG_ID] *should be available now for usage.
QCCR1D209730	**Symptom:** The logged in user id was not right when the group subscription was set up. It was always the user id of the one who created it. **Resolution:** More tokens have been added and also the user id shown will be the logged in user id.
QCCR1D208162	**Symptom:** Service Request does not track the completeness of the Subscription. **Resolution:** The state/status and completedOn timestamp of the service request was updated appropriately for various actions like order.modify,cancel action..
QCCR1D209226	**Symptom:** In the email confirming the rejection of a request towards an end user, the reason is not specified even though this is given in the portal. **Resolution:** An enhancement has been made to the product in 4.2 patch release to include the approver's comment for rejection.
QCCR1D210180	**Symptom:** Consumer admin is able to create service offerings from MPP and potentially set zero pricing **Resolution:** The ability to turn off 'Offering Management' widget from Marketplace Portal for Consumer Organization Administrators has been introduced. This will solve the problem where a Consumer Organization Administrator could create Service Offerings with zero pricing. When 'Offering Management' widget is turned off from Marketplace Portal, Consumer Organization Administrators will only be able to add service offerings created in Service Management Console through Marketplace Portal's 'Catalog Management' widget. Follow below steps to turn off 'Offering Management' widget from Marketplace Portal for Consumer Organization Administrators: To remove the Offering Management tile for the Tenant Admin: 1. Open {CSA_Installation_Folder} /portal/conf/dashboard.json in a text editor. 2. Find "MANAGE_OFFERINGS". 3. Remove the object that has the label "common.items.MANAGE_OFFERINGS". The whole object looks like:

Change Request	Description of fixed issue

	{
	"label": "common.items.MANAGE_OFFERINGS",
	"icon": {
	"className": "icon-services"
	},
	"className": "orange",
	"link": {
	"url" : "consumption/offerings/ ",
	"target": "_blank"}
	}
	4. Open {CSA_Installation_Folder}/portal/conf/mpp.json in a text editor.
	5. Find "enableOfferingAdministration".
	6. Set the consumption.enableOfferingAdministration property to false.
	7. Restart HP Marketplace Portal service

QCCR1D210054	**Symptom:** Need to ability to disable security warning banner **Resolution:** To change security warnings in the Marketplace Portal (MPP): 1.To change security warnings in the MPP: a.Open the MPP dashboard file in a text editor: CSA_HOME/portal/conf/dashboard.json b.Find the “header.securityWarning.enable” parameter and set to desired value (true or false). 2.To change security warnings for the MPP Tenant Admin: a.Open the MPP config file in a text editor: CSA_HOME/portal/node_modules/mpp consumption/dist/offerings/config.json b.Find the "enableSecurityWarning" parameter and set to desired value (true or false). 3.Documentation for changing security warnings in the Service Management Console: a.Open the Service Management Console config file in a text editor: CSA_HOME/jboss-as/standalone/deployments/csa.war/offerings/config.json b.Find the "enableSecurityWarning" parameter value and set to desired value (true or false).

Downloading and installing the patch

Pre-installation requirements

Before installing the patch…

1. Review all instructions in this document.
2. Review the Hewlett-Packard Support Line User Guide or your Hewlett-Packard support terms and conditions for precautions, scope of license, restrictions, and limitations of liability and warranties.
3. Make sure that your system meets the following minimum requirements:
    a. Minimum hardware:
        i. CPU: 4 CPU, 3.0 GHz
        ii. RAM: 8 GB
        iii. Hard Drive: 20 GB
    b. Operating system:

        For supported operating systems details, see HP CSA 4.50 Support Matrix available at: https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691511
    c. Software:

        Version 4.50.0000 of HP Cloud Service Automation
4. Back up the CSA environment.
5. Make sure that new subscriptions are not being created and that existing subscriptions are not being modified when this patch installer is being applied.

    Important: Failing to do this can leave CSA in an unstable state and the patch application can fail.
    a. Sign out of all open instances of the HP CSA Provider Console and HP Marketplace Portal.
    b. Stop the following CSA Services:
        i. HP Cloud Service Automation,
        ii. HP Marketplace Portal,
        iii. HP Search and
        iv. Elasticsearch 1.5.2 services.

    Important: For clustered CSA servers, stop the services on all nodes.

Installing the patch on standalone CSA servers

To install the patch in a standalone configuration:

1. Complete prerequisite steps described under Pre-installation requirements.
2. Download the CSA patch file.
3. Extract the `HP_CSA_Patch_04.50.0001.bin` file from the patch tar file.
4. Verify that `HP_CSA_Patch_04.50.0001.bin` is owned by the 'csauser' user and that csauser has full permissions to the file. If necessary, do the following:
    a. Log in as the root user and enter the following commands:

```
chown csauser:csagrp HP_CSA_Patch_04.50.0001.bin
chmod u+rwx HP_CSA_Patch_04.50.0001.bin
```

b. Log out as the root user.

5. Log in as csauser and run `HP_CSA_Patch_04.50.0001.bin` to open the console mode of the HP Cloud Service Automation Patch Installer.
6. Enter `./HP_CSA_Patch_04.50.0001.bin` to initiate the patch installer interview.
7. Acknowledge information screens and warnings:
   a. Read the introduction and click **Enter**.
   b. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites, click **Enter**.
8. Select **Standalone** as the HP CSA environment option, and click **Enter**.
9. Select the option that describes your set-up and click **Next**:
   a. Select **CSA and MPP are installed** if both the components are installed.
   b. Select **Only MPP is installed** if only MPP is installed.

   Note: If you selected **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
10. Review the pre-installation summary and click **Enter** to run the complete patch installation.
11. After the installation completes, click **Enter** to exit.
12. Verify the installation and restart services as instructed below under Verifying the installation.

Installing the patch on clustered CSA servers

To install the patch in a clustered environment, perform these steps on all nodes of the CSA cluster:

1. Complete prerequisite steps described under Pre-installation requirements.
2. Download the patch file.
3. Extract the `HP_CSA_Patch_04.50.0001.bin` file from the patch tar file.
4. Verify that `HP_CSA_Patch_04.50.0001.bin` is owned by the 'csauser' user and that csauser has full permissions to the file. If necessary, do the following:
   a. Log in as the root user and enter the following commands:

   ```
   chown csauser:csagrp HP_CSA_Patch_04.50.0001.bin chmod u+rwx
   HP_CSA_Patch_04.50.0001.bin
   ```

   b. Log out as the root user.
5. Log in as csauser and run `HP_CSA_Patch_04.50.0001.bin`. to open the console mode of the HP Cloud Service Automation Patch Installer.
6. Enter `./HP_CSA_Patch_04.50.0001.bin` to initiate the patch installer interview.
7. Acknowledge information screens and warnings:
   a. Read the introduction and click **Enter**.
   b. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites, click **Enter**.
8. Select **Cluster** as the HP CSA environment option, and click **Enter**.
9. Select the option that describes your set-up and click **Next**:
   a. Select **CSA and MPP are installed** if both the components are installed.
   b. Select **Only MPP is installed** if only MPP is installed.

   Note: If you selected **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.

10. Review the pre-installation summary and click **Enter** to run the complete patch installation.
11. After the installation completes, click **Enter** to exit.
12. Verify the installation and restart services as instructed below under Verifying the installation.

Verifying the installation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the installation on each node.

1. Check the logs for any errors under
   `$CSA_HOME/_CSA_4_50_1_installation/Logs`
   The log files include:
   - `csa_install.log`
   - `csa_InstallPatch.log`
   - `msvc_*.log`
   - `upgrade_idm.log`
   - `upgrade_search_service.log`
2. Ensure that the browser cache is cleared.
3. Start the following services if they are not already running:
   a. HP Cloud Service Automation
   b. HP Marketplace Portal
   c. HP Search
   d. Elasticsearch

   Note: For Linux, after the patch installation is complete, start the services manually.

   Important: In a clustered environment, make sure services are started on all nodes.
4. Launch the Cloud Service Management Console, log in, and then check for the updated version.

   Note: If there are errors in the log files, create a backup of the log files, restore the backup of the `CSA_HOME` directory, and contact HP Support.

Important: If the patch is installed in a cluster environment, Elasticsearch will be non-functional if it was enabled prior to the patch installation. In order to make global search functional, follow the steps defined in the "Configuring Elasticsearch in Cluster Environments."

Configuring Global Search in Cluster Environments

Manual configuration changes are necessary for making Elasticsearch work after installing CSA 4.50 Patch 1, as described below.

StrictSSL support for Elasticsearch:

- In 4.50 MR, strictSSL is not supported for Elasticsearch in standalone or HA cluster mode.
- In 4.50 Patch 1, strictSSL is supported for Elasticsearch for both standalone and HA mode as long as the certificates are properly configured.

How to configure Elasticsearch in a High Availability (HA) cluster

In CSA 4.5 Elasticsearch is disabled by default. For instructions on enabling Elasticsearch, see Chapter 7: The Marketplace Portal in the *CSA 4.50 Configuration Guide*.

After completing the steps described in the aforementioned configuration guide, the following additional steps are required when turning on Elasticsearch in an HA cluster environment.

1. Replace "`csa.properties csa.provider.msvc.hostname`" with local node FQDN.
2. Replace "`csa-search-service/app.json ccue-basic-server.host`" with local node FQDN.
3. Replace "`csa-search-service/app.json msvc-basic-search.searchEngineURL`" with local node FQDN.
4. Complete the certificate set-up appropriate steps for your environment:
    a. If the cluster setup is using the default CSA (self-signed) certificates change the following settings to "false."

    (**Note**: These 2 settings do not need to be modified if the cluster runs valid certificates signed by a common CA.)

    ```
    csa-search-service/app.json msvc-basic-search.strictSSL/rejectUnauthorized: false
    elasticsearch/config/elasticsearch.yml searchguard.ssl.transport.http.enforce_clientauth: false
    ```

    b. Verify the following HA configurations in `csa-search-service/app.json` are maintained after the installation of the patch:
        i. `idmURL` should point to the load balancer

        For example:

        ```
        "idmURL": "https://http-loadbalancer.csapcoe.hp.com:8443/idm-service"
        ```

        where `Port 8443` is the load balancer port that was configured manually during CSA 4.5 MR installation.

        ii. `cert` should point to the load balancer cert

        For example:

        ```
        "ca": "C:/Program Files/Hewlett-Packard/CSA/jboss-as/standalone/configuration/apache_csa.crt"
        ```

        The *.crt file name cannot remain as the default, "`jboss.crt`"

For more information on setting up certificates please refer to the following CSA 4.50 documents:

Document	Link to CSA 4.50 document on the SSO
FIPS 140-2 Compliance Statement	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691504
FIPS Compliance Configuration Guide	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702243
Configuring an HP CSA Linux Cluster for High Availability Using an Apache Web Server	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737522
Configuring an HP CSA Windows Cluster for High Availability Using an Apache Web Server	https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737523

Note: Please see the CSA 4.x Documentation Library on the HP Software Support Online (SSO) portal for links to all product documentation. (HP Passport is required.)

Uninstalling the patch

Preparing for uninstallation

1. Backup the CSA environment.
2. Make sure that new subscriptions are not being created and that existing subscriptions are not being modified when this patch installer is being applied.

   Important: Failing to do this can leave CSA in an unstable state and the patch application can fail.

   a. Sign out of all open instances of the HP CSA Provider Console and HP Marketplace Portal.
   b. Stop the following CSA Services:
      i. HP Cloud Service Automation,
      ii. HP Marketplace Portal,
      iii. HP Search and
      iv. Elasticsearch 1.5.2 services.

   Important: For clustered CSA servers, stop the services on all nodes.

Uninstalling the patch on standalone CSA servers

To uninstall the patch in a standalone configuration:

1. Complete prerequisite steps described under Preparing for uninstallation.
2. Navigate to the `$CSA_HOME/_CSA_4_50_1_installation/Uninstaller` folder.
3. Run `./Uninstall HP Cloud Service Automation Patch` to start the console mode of the patch uninstaller.
4. Read the introduction and click **Enter**.

5. Read warnings to stop services and comply with instructions before proceeding to the next step. Verify you have completed the required pre-requisites.
6. Click **Enter** to run the patch uninstaller.
7. After the uninstallation completes, click **Enter** to exit.
8. Verify the uninstallation and restart services as instructed under Verifying the uninstallation.

Uninstalling the patch on clustered CSA servers

To uninstall the patch in a clustered environment, perform these steps on all nodes of the CSA cluster:

1. Complete prerequisite steps described under Preparing for uninstallation.
2. Navigate to the `$CSA_HOME/_CSA_4_50_1_installation/Uninstaller` folder.
3. Run `./Uninstall HP Cloud Service Automation Patch` to start the console mode of the patch uninstaller.
4. Read the introduction and click **Enter**.
5. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites.
6. Click **Enter** to run the patch uninstaller.
7. After the uninstallation completes, click **Enter** to exit.
8. Verify the uninstallation and restart services as instructed under Verifying the uninstallation.

Verifying the uninstallation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the uninstallation on each node.

1. Verify the logs for any errors under
   `$CSA_HOME/_CSA_4_50_1_installation/Logs`
   The uninstall log files include:
   - `csa_install.log`
   - `csa_InstallPatch.log`
2. Ensure that the browser cache is cleared.
3. Start the following services if they are not already running:
   a. HP Cloud Service Automation
   b. HP Marketplace Portal
   c. HP Search
   d. Elasticsearch 1.5.2

   For Linux, after the patch installation is complete, start the services manually.

   Important: In a clustered environment, make sure services are started on all nodes.

CSA modified files

<CSA_HOME> refers to the location where CSA is installed

```
<CSA_HOME>\elasticsearch-1.5.2\config\*.*
<CSA_HOME>\jboss-as\standalone\deployments\idm-service.war\*.*
<CSA_HOME>\jboss-as\standalone\deployments\csa.war\*.*
<CSA_HOME>\CSAKit-4.5\OO Flow Content\9X\CSA-4_10-ContentInstaller.jar
<CSA_HOME>\CSAKit-4.5\OO Flow Content\10X\
            oo10-csa-cp-4.50.0000.jar
            oo10-csa-integrations-cp-4.50.0000.jar
<CSA_HOME>\portal\*.*
<CSA_HOME>\Tools\ComponentTool\*.*
<CSA_HOME>\Tools\ContentArchiveTool\
            CODAR_BP_EXISTING_WINDOWS_SERVER_COMPONENT_v1.50.00.zip
            content-archive-tool.jar
<CSA_HOME>\jboss-as\standalone\configuration
            standalone.xml
            standalone-full-ha.xml
<CSA_HOME>\Tools\DBPurgeTool\db-purge-tool.jar
<CSA_HOME>\Tools\PasswordUtil\passwordUtil-standalone.jar
<CSA_HOME>\Tools\ProcessDefinitionTool\process-defn-tool.jar
<CSA_HOME>\Tools\ProviderTool\provider-tool.jar
<CSA_HOME>\Tools\SchemaInstallationTool\*.*
<CSA_HOME>\Tools\SupportTool\support-tool.jar
<CSA_HOME>\csa-search-service\*.*
```

Additional information

HP Software Support

This web site provides contact information and details about the products, services, and support that HP Software offers. For more information, visit the HP Support web site at: HP Software Support Online.

HP Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business.

As a valued support customer, you can benefit by being able to:

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

To access the Self-Solve knowledge base, click Search. Use the filter panel to search for knowledge documents, product manuals, patches, or any kind of available documentation type.

Note: Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to: Access Levels. If you do not have an HP Passport, you will be given an opportunity to register for one from the login page.

To find documents on the HP Software Support portal:

1. Go to https://softwaresupport.hp.com/.
2. Log in using your HP Passport credentials.
3. Select **Dashboards > Manuals** to view all available documentation.
4. From the Self-Solve Knowledge Search results, use the search and filter functions to narrow the set of documents by Product, Version, Operating system, Document Type, Optional keyword(s) or phrases, and so on.
5. Select your document from the list.
6. From the document view, click the file link to download it or view it online, depending on your browser.

Note: For additional assistance on this portal, explore the options in the Website Assistance menu. To help us improve our documents, please send feedback to clouddocs@hp.com.

Legal notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft®, Windows®, and Windows® 7 are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

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

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