



Hewlett Packard
Enterprise

Codar

Software version: 1.70.0002

For Microsoft Windows® and Linux operating systems

Patch Read Me

Document release date: December 2016

Software release date: December 2016

Contents

Introduction	3
Fixed issues	3
Known issues	4
Patch installation	9
Check preinstallation requirements	9
Install the patch	10
Verify the patch installation.....	10
Patch removal - Linux	11
Before uninstalling the patch	11
Uninstall the patch on standalone and cluster Codar servers.....	11
Patch removal - Windows	11
Before uninstalling the patch	11
Uninstalling the patch on standalone and clustered environments.....	12
Patch removal verification	12
Codar modified files	13
Send documentation feedback	14
Legal notices	14

Introduction

This readme describes the fixed issues and known issues in this patch and provides instructions for installing and configuring the patch on a Linux or Windows HPE Codar server. The cumulative patch updates the Codar server to 1.70.0002.

In this document, <CSA_HOME> refers to the directory in which HPE Codar is installed.

Note: All the fixed and known issues listed in this document pertain to systems with CSA and CSA+Codar installations only.

Fixed issues

The following table describes the issues that are fixed in this patch.

Issue	Description
QCCR1D227441	The LDAP user is unable to login to CSA or Marketplace Portal immediately after access control configuration in the organization due to IdM - Async Roster API causing delay in the LDAP group and CSA sync.
QCCR1D227500	IdM - After creating an organization and configuring LDAP, the user should be able to login instead it takes around 10 mins to allow user to login.
QCCR1D228864	Exponential degradation in MPP Submit request (Order new subscription API) under load after 40 hours of load test.
QCCR1D228865	Exponential degradation in SMC Clone SO (Save as) under load after 40 hours of load test.
QCCR1D228866	Exponential degradation in SMC Clone SD (Save as) under load after 40 hours of load test.
QCCR1D229839	CSA/Propel: Transfer Subscription Failed.
QCCR1D230349	Unable to transfer ownership for service subscription from a user to an organization admin.
QCCR1D230418	IdM - Named Group Approver is not working when SAML is enabled on the Consumer Organization.
QCCR1D230521	When existing users are removed from catalogs and then added back in access control, 503 service unavailable error is displayed.
QCCR1D230556	Unable to transfer ownership of subscriptions from CSA/Propel.
QCCR1D230601	When consumer organization admin tries to add group approval policy in MPP, an error is displayed and gets logged out of MPP.
QCCR1D232011	When the user is on SMC dashboard, IdM - Session timeout error is displayed.
QCCR1D230273	When a lifecycle action fails due to an exception, the ActionProcessCallBackHandler is not handling error conditions by lifecycle actions. As a result, failed service instance/subscription get stuck in "Deploying" and "Pending" state instead of going to "Failed" and "Terminated".
QCCR1D230777	When a flow is moved to a new location and an action is recreated pointing to that flow, the underlying process definition is not updated with the new location of the flow.
QCCR1D232562	CSA 4.7 Organization UI and MPP do not come up if host name has underscore.

Known issues

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

Issues	Description
QCCR1D233897	<p>Problem : On logging in to an organization through CSA REST API, after the DN to which the user belongs to is added in access control, the system requires a minimum delay of 10 minutes for the first time login.</p> <p>Workaround : No workaround available.</p>
QCCR1D233719	<p>Problem : MPP organization fails to load with invalid tenant when the created organization has '\$' symbol in Organization Name.</p> <p>Workaround : No workaround available.</p>
QCCR1D229855	<p>Problem : CSANG Adapter Recipient need to be the Subscription Owner Not the Submitter.</p> <p>Workaround : Steps:</p> <ol style="list-style-type: none"> 1. Login to propel provider UI. 2. Go to "Content Management". 3. Locate CSA request to fulfillment and download it. 4. Unpack the archive and navigate to <i>csa-ng-r2flsx\templates</i>. 5. Edit the createReqUrl.ftl. 6. Locate line starting with <i>/api/consumption/v2....</i> and Change line content to: <i>/api/consumption/v2/request/?onBehalf=\${message.inputEntity.summary.recipient}&onBehalfOrg=\${instanceConfig.sxInfo.organization}</i>. 7. Pack the content. 8. Upload modified content pack back to Propel.
QCCR1D217764	<p>Problem : Cannot launch the show performance page using SSO from MPP.</p> <p>Cause : Upload modified content pack back to Propel</p> <p>Workaround : No workaround available.</p>
QCCR1D230291	<p>Problem : Not able to bring up the MPP Login page in Cluster environment.</p> <p>Cause : This happens because of the double encryption of the <i>idm.encryptedSigningKey</i> in the standalone instance.</p> <p>Workaround : No workaround available.</p>
QCCR1D228633	<p>Problem : Login to Provider organization with LDAP is not working when SAML is enabled in 4.7 upgrade setup.</p> <p>Cause : When SAML is configured, LDAP representation with absolute DN is expected for successful login, but relative DN is available in upgrade setup.</p> <p>Workaround : Update the existing DN in access control of provider organization.</p>
QCCR1D227922	<p>Problem : Organization LDAP Configuration - Invalid Hostname or Port shows wrong error message.</p> <p>Workaround : Hewlett Packard Enterprise (HPE) has been unable to reproduce this issue. If the same behavior still exists and you can reproduce it, please contact Hewlett Packard Enterprise Software Support referencing this document. Be prepared to provide the exact steps to reproduce and/or demonstrate the steps and environment details to Software Support. The current Change Request will remain in HPE's database for future reference.</p>
QCCR1D230356	<p>Problem : Cannot launch the show performance page using SSO from MPP.</p> <p>Cause : Cannot launch the show performance page using SSO from MPP.</p>

Issues	Description
	Workaround : User can login to Cloud Optimizer manually by entering username and password.
QCCR1D230507	<p>Problem : Kafka service is not starting/stopping.</p> <p>Cause : Introduced new commands to enable/disable Kafka service in Cloud Optimizer.</p> <p>Workaround : To check Status/Enable/Disable kafka, please find below commands:</p> <p><u>To check kafka status:</u></p> <pre># OVC hpcsrvd HPCS Server AGENT,OA (1213) Running hpekafka HPE Kafka Service CORE,SERVER (1364) Running hpezookeeper HPE Zookeeper Service CORE,SERVER (989) Running ovbbccb OV Communication Broker CORE (1187) Running ovcd OV Control CORE (1115) Running ovtomcatB OV Tomcat(B) Servlet Container WEB,SERVER (1858) Running pvcd PV Core PV (6127) Running</pre> <p><u>To Enable kafka:</u></p> <pre># /opt/OV/bin/msgbus.sh -enable ===== Current Messagebus Configuration ===== HPEKafka and HPEZookeeper are disabled. ===== Enabling Msgbus Registering HPEKafka and HPEZookeeper Starting HPEZookeeper and HPEKafka ===== ===== To Disable kafka: # /opt/OV/bin/msgbus.sh -disable ===== Disabling Msgbus Stopping HPEZookeeper and HPEKafka Unregistering HPEKafka and HPEZookeeper ===== New Messagebus Configuration ===== HPEKafka and HPEZookeeper are disabled. ===== =====</pre>
QCCR1D218883	<p>Problem : Custom changes in Elasticsearch configuration may be discarded during an HA upgrade installation.</p> <p>Cause : Product defect.</p> <p>Workaround : Custom changes from upgraded installation are stored in a backup folder in /elasticsearch/config/. Transfer custom changes from the older installation file into the upgraded file.</p>

Issues	Description
QCCR1D219172	<p>Problem : Logging to MPP using a personal identity verification (PIV) card fails after upgrading from CSA 4.5 to CSA 4.6. This issue is seen only in Linux environments.</p> <p>Cause : The default HPE SSO value is incorrect in the CSA 4.5 environment prior to the upgrade. The upgrade process does not properly update the idm.war file, resulting in HP SSO not functioning correctly after the upgrade.</p> <p>Workaround : Edit the idm.war/WEB-INF/web.xml file. Find the section below:</p> <pre><listener> <listener-class>com.hp.hpssso.HpSsoContextListener</listener- class> </listener> <context-param> <param- name>com.hp.sw.bto.ast.security.lwssso.conf.fileLocation</param- name> <param-value>/usr/local/hp/csa/jboss- as/standalone/deployments/idm-service.war/WEB- INF/web.xml</param-value> </context-param>.</pre> <p>Now change - web.xml To hpsssoConfig.xml. and then restart the CSA service</p>
QCCR1D222070 (225115)	<p>Problem : Providers not defined in a resource environment are used during provisioning when internal actions for building and selecting from a resource provider list are not used.</p> <p>Cause : Filtering is not done when internal actions are not used to identify providers that can be used during provisioning. This is a product limitation.</p> <p>Workaround : No workaround available.</p>
QCCR1D224553	<p>Problem : When creating or editing a string property on a component type or component template in the Designs / Sequenced / Components areas of the Cloud Service Management Console, the Property Value input may not be visible.</p> <p>Cause : Product defect.</p> <p>Workaround : Close the dialog and refresh the current page. Re-open the dialog again.</p>
QCCR1D225958	<p>Problem : Missing data points when VM is powered Off or Suspended.</p> <p>Cause : Unable to plot the graph for missing data points.</p> <p>Workaround : No workaround available.</p>
QCCR1D226184	<p>Problem : In Operation Console for Service Instance upgrade:</p> <ul style="list-style-type: none"> Existing actions display name get changed after upgrade. Source column shows original Resource Offering display name for upgrading actions instead of its own Resource Offering display name. <p>Cause : If the Resource Offering for upgrade was created by doing save as from the original Resource Offering and Initializing, Reserving, and Deploying lifecycle actions are kept as is, but display name is being modified for them. In that case all the existing actions would get new display name from new Resource Offering.</p> <p>Workaround : No workaround available.</p>
QCCR1D226494	<p>Problem : The Featured Category list is empty for a newly created organization.</p>

Issues	Description
	<p>Cause : The organization data synchronization is not complete after a new organization is created in IDM tables.</p> <p>Workaround : After the synchronization is completed, the catalogs and featured category list will appear. (~30 seconds).</p>
QCCR1D227598	<p>Problem : SAML authorization does not work if the access control is configured with the LDAP sub tree.</p> <p>Cause : CSA does not support the LDAP sub tree for Access Control (ACL) when SAML is enabled.</p> <p>Workaround : No workaround available.</p>
QCCR1D227675	<p>Problem : Infrastructure monitoring health status information is not available for infrastructure servers in Market place portal and Server Management Console even after configuring the Cloud Optimizer provider.</p> <p>Cause : This feature cannot be enabled with the current version of Cloud Optimizer.</p> <p>Workaround : If you are subscribed for email notifications of CSA 4.7 documentation updates, you will be notified when the CSA 4.7 Support Matrix is updated with information about the supported version of Cloud Optimizer.</p>
QCCR1D228220	<p>Problem : Health status is not updated for servers deployed on Helion Openstack (HOS) provider.</p> <p>Cause : CSA is unable to retrieve the health status since Cloud Optimizer (CO) is not supporting HOS 3.0.</p> <p>Workaround : It is a product limitation. No workaround available.</p>
QCCR1D228293	<p>Problem : Unable to launch MPP Organization created with special character-2894.</p> <p>Cause : Customers with already existing special character organization names will not be able to access MPP after upgrading to 4.7.</p> <p>Workaround : Change the organization name and ensure not to have any special characters in the name.</p>
QCCR1D228421	<p>Problem : When SSO is enabled, Operation Orchestration (OO) does not prompt for login after CSA tokenGlobaltimeout is elapsed.</p> <p>Cause : SSO configuration differs in CSA and OO and settings is not fully compatible.</p> <p>Workaround : Steps:</p> <ol style="list-style-type: none"> 1. SSO in CSA is configured in CSA\jboss-as\standalone\deployments\idm-service.war\WEB-INF\hpsssoConfig.xml, <ul style="list-style-type: none"> • See tokenGlobalTimeout and tokenIdleTimeout parameters. 2. SSO in OO is configured in OO\central\tomcat\webapps\oo\WEB-INF\classes\lwssofmconf.xml, <ul style="list-style-type: none"> • See expirationPeriod parameter, which corresponds to tokenIdleTimeout in CSA. 3. Check if both values are in sync. <p>Note: However, there is no counterpart for tokenGlobalTimeout in OO.</p>
QCCR1D228600	<p>Problem : Cannot use groups in Service Management Console that were created through Artifact API with name containing characters other than alphanumeric and hyphen (-).</p> <p>Cause : There is no group name validation in Artifact API.</p>

Issues	Description
	<p>Workaround : Use only alphanumeric characters or '-' for group name when creating group through Artifact API.</p>
QCCR1D228619	<p>Problem : Global search from MPP portal does not work in a Linux CSA installation.</p> <p>Cause : CSA Search service fails to update the Elastic search indices as a result of which Global search from MPP returns nothing.</p> <p>Workaround : After CSA installation is complete, or after restarting CSA, stop the CSA Search service and restart it manually by following the steps below: If CSA was installed in a location other than /usr/local/hp/csa, adjust the path accordingly.</p>
QCCR1D228672	<p>Problem : Cannot launch the show performance page using SSO from MPP.</p> <p>Cause : SSO token is not passed correctly.</p> <p>Workaround : User can login to Cloud Optimizer manually by entering username and password.</p>
QCCR1D228716	<p>Problem : Transfer ownership operation fails even after the ownership is successfully transferred. It happens only when the user has different name and display name.</p> <p>Cause : It is caused by implementation of checkTransferOwnershipResponse.ftl * input message contains user's full name (User15), but user's name (user15) - comparison fails (upper case vs lower case), so request is marked as failed. Input message : <pre>"flatFields" : [{ "id" : "transferTo", "value" : "User15", "type" : "DROPDOWN_LIST" }],</pre> </p> <p>Workaround : This is not a functional problem. Only the message about the result of the ownership transfer is wrong but the transfer is successful. Therefore workaround is either ignoring the "failed status" of the transfer ownership or avoiding usage of users with different name and display name.</p>
QCCR1D228726	<p>Problem : Launching help content for adding upgrade path in offerings throws page not found error.</p> <p>Cause : No topic ID is defined for the help icon on that dialog box.</p> <p>Workaround : Open the help and navigate to Deploy > Offerings > Upgradability for a topic on upgradability.</p>
QCCR1D229537	<p>Problem : Cannot upgrade to CSA 4.7 when Base DN in LDAP tab in the Organization detail is empty (Oracle only).</p> <p>Cause : Software defect.</p> <p>Workaround : If upgrade has already started and stopped with an error, update the Base DN directly in the Database. Set the base_dn column in the csa_ldap_access_point table for each record that is present in the table. The Base DN is last part of the LDAP Full DN. It can be "dn=company,dn=com" if full dn of some group is "cn=group1,dn=company,dn=com". It depends on the LDAP settings.</p>

Issues	Description
	Stop CSA and install upgrade again.
QCCR1D220470	<p>Problem : After applying the patch, custom changes related to cluster are not retained.</p> <p>Cause : Cluster environment fails after installation of patch if CSA is configured in high-availability mode.</p> <p>Workaround : From %CSA_HOME%/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext.xml</p> <p>Replace this:</p> <pre data-bbox="570 468 1450 579"> <!--START HA Mode Configuration--> <!-- <jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/> <!--END HA Mode Configuration--> </pre> <p>With this:</p> <pre data-bbox="570 642 1414 753"> <!--START HA Mode Configuration--> <jee:jndi-lookup id="channelGroup" jndi-name="java:jboss/clustering/group/server" expected-type="org.wildfly.clustering.group.Group"/> <!--END HA Mode Configuration--> </pre> <p>Restart the services of CSA after all the above changes made.</p>

Patch installation

This section describes how to install the patch.

Check preinstallation requirements

Make sure you fulfill these prerequisites before installing:

1. Check minimum hardware requirements:
 - CPU: 4 CPU, 3.0 GHz
 - RAM: 8 GB
 - Hard Drive: 20 GB
2. Check the [Codar 1.70 Support Matrix](#) to verify operating-system requirements.
3. Check minimum software requirements:

Codar version 1.70.0000

4. Set the CSA_HOME environment variable:

In case of remote MPP installation, please ensure that CSA_HOME environment variable is set.

- **Windows:** Set the CSA_HOME environment variable to point to the Codar installed location.
Example: C:\Program Files\HPE\Codar
- **Linux:** Set the CSA_HOME environment variable to point to the Codar installed location.
Example: /usr/local/hpe/codar

5. Back up your Codar environment.
6. Stop the following Codar services: HPE Codar, HPE Marketplace Portal, HPE Search Service and Elasticsearch 1.6.1(elasticsearch-service-x64).

Important: You must stop these services on each node in a cluster.

Note: If you do not stop these services manually, the following folders will not be cleared and will cause UI issues after installing the patch:

Windows: <CSA_HOME>\jboss-as\standalone\tmp

Linux: /usr/local/hpe/codar/jboss-as/standalone/tmp

Install the patch

Use the following procedure to install the patch in a standalone configuration or on *each* node of a cluster:

1. Download the Codar patch file:

Linux:

https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CODAR_00013

Windows:

https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/CODAR_00014

2. **Linux:**

Note: For clusters, perform all steps on each node in a cluster.

- a. Extract the downloaded file: HPE_Codar_Patch_01.70.0002.bin file from the patch file.
- b. Make sure that the `codaruser` user is the owner of the file and has full privileges.
- c. Log in as `codaruser` and run `HPE_CODAR_Patch_01.70.0002.bin` to open the Codar patch installer console mode.
- d. Enter `./HPE_CODAR_Patch_01.70.0002.bin` to run the patch installer.
- e. Select **Enter** in the introduction, warnings, and prerequisites screens.
- f. In the environment dialog screen, select **Standalone** or **Cluster** environment, then click **Enter**.
- g. Click **Enter**.
- h. In the pre-installation summary dialog screen, click **Enter**.

The patch installer begins the installation.

3. When prompted, click **Enter** to exit the installation.

4. **Windows:**

- a. Extract the `HPE_CODAR_Patch_01.70.0002.exe` file from the patch zip file.
- b. Run `HPE_CODAR_Patch_01.70.0002.exe` to launch the installation wizard.
- c. Click **Next** to open the Codar Environment Selection wizard.
- d. Select **Standalone** or **Cluster** environment, then click **Next**.
- e. Click **Install** to run the patch installation.
- f. When prompted, click **Done** to exit the installation.

Verify the patch 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 for errors in the log files:

Windows: <CSA_HOME>_Codar_1_70_2_installation\Logs

Linux: \$CSA_HOME/_Codar_1_70_2_installation/Logs

Log files include `codar_install.log` and `codar_InstallPatch.log`.

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

2. Clear the browser cache.
3. Make sure the Codar, HPE Search, and Elasticsearch services 1.6.1 (elasticsearch-service-x64) are running:

Windows: Installer automatically starts these services.

Linux: Start the services manually. In a cluster environment, manually start the services on all nodes.

4. Launch the Codar Console, log in, and check for the updated version.

Patch removal - Linux

This section provides the steps to uninstall the patch on a Linux server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

Before uninstalling the patch

Complete the following preparation steps before you uninstall the patch:

1. Back up the Codar environment.

Warning: If you do not stop creation and modification, the uninstallation might fail and Codar might be left in an unstable state.

2. Sign out of all open instances of the Codar Provider Console.
3. Stop the following Codar services: HPE Codar, HPE Marketplace Portal, HPE Search Service, and Elasticsearch 1.6.1(elasticsearch-service-x64)

Important: You must stop these services on each node in a cluster.

Uninstall the patch on standalone and cluster Codar servers

To uninstall the patch:

1. Navigate to `$CSA_HOME/_Codar_1_70_2_installation/Uninstaller`.
2. Run `./Uninstall HPE Codar Patch` to start the uninstaller console mode.
3. Click **Enter** for the introductory and warning screens.
4. Click **Enter** to run the patch uninstaller.
5. When the patch uninstallation is complete, click **Enter** to exit the uninstallation process.

Patch removal - Windows

This section provides the steps to uninstall the patch on a Windows server in both standalone and clustered environments.

Note: Uninstallation of the patch will not revert the database-indexing changes made during patch installation.

Before uninstalling the patch

Complete the following preparation steps before you uninstall the patch:

1. Backup the Codar environment.
2. Stop new subscription creation and subscription modification.

Warning: If you do not stop creation and modification, the uninstallation might fail and Codar might be left in an unstable state.

3. Sign out of all open instances of the Codar Provider Console and Marketplace Portal.
4. Stop the following Codar services: HPE Codar, HPE Marketplace Portal, HPE Search Service and Elasticsearch 1.6.1(elasticsearch-service-x64).

Important: You must stop these services on each node in a cluster.

Uninstalling the patch on standalone and clustered environments

You can uninstall the patch using either of the following methods:

- Using the Control Panel
- Using the Uninstall Codar Patch wizard

Note: For clustered environments, perform the steps on each node of the cluster after stopping the services on all nodes.

To uninstall the patch using the Control Panel:

1. In the Control Panel, choose **Uninstall a program**.
2. Select **Codar Patch** and click **Uninstall**.
3. Follow the instructions on the uninstall wizard to uninstall the patch.

To uninstall the patch using the Uninstall Codar Patch wizard:

1. Navigate to `<CSA_HOME>_CODAR_1_70_2_installation\Uninstaller`.
2. Execute `Uninstall HPE Codar Patch.exe` to open the Uninstall Codar Patch wizard.
3. Click **Uninstall** to uninstall the patch.
4. Click **Done** to exit the uninstall wizard.

Patch removal verification

After uninstalling the patch, perform the following steps to verify the patch was removed. These verification steps apply to both standalone and clustered environments.

Note: For clustered environments, complete these steps on each node.

1. Check for errors in the log files:

Windows: `<CSA_HOME>_Codar_1_70_2_installation\Logs`

Linux: `$CSA_HOME/_Codar_1_70_2_installation/Logs`

Log files include `codar_uninstall.log`, and `codar_unInstallPatch.log`.

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

2. Clear the browser cache.
3. Make sure the Codar, HPE Search, and Elasticsearch 1.6.1 services are running:

Windows: The installer automatically starts these services.

Linux: Start the services manually. In a cluster environment, manually start the services on all nodes.

Codar modified files

```
<CSA_HOME>/jboss-as/standalone/deployments/csa.war/*  
<CSA_HOME>/jboss-as/standalone/deployments/csa.war/idm-service.war/*  
<CSA_HOME>/portal/*
```

```
CSA_HOME/CSAKit-1.7/Lib/service manager/HPSM_CSA_Integration_file.unl  
CSA_HOME/Tools
```

Send documentation feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

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

© Copyright 2016 Hewlett Packard Enterprise Development LP

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® 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.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register:

<https://softwaresupport.hpe.com>.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

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

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at <https://softwaresupport.hpe.com>.