HP Service Manager

For the supported Windows and Unix systems

Software Version: 9.32

Patch 1 Release Notes

Document Release Date: October 2013

Software Release Date: October 2013

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

What's New in This Release

This section describes important changes in this release.

Enabling LDAP over SSL without setting any certificate on the SM server side

Before Service Manager 9.32 Patch 1, when you enable LDAP over SSL in Service Manager, the root certificate of the CA that issued the LDAP server's certificate need be set on the SM server side. This requirement is unnecessary and causes inconvenience to customers who wish to enable LDAP over SSL, or to deploy LDAP over SSL in a more flexible way.

In fact, the client side verification on LDAP server's certification is not mandatory to implement LDAP over SSL. In this solution, a new parameter `ldapsslallownocert` is added. When you set this parameter to `1`, RTE will no longer check that issuer CA's root certification, in fact customers can skip providing any LDAP server cert.

The following steps describe how to configure it:

1. Log in to the Windows client as an administrator, click **System administration** > **Ongoing Maintenance** > **LDAP Mapping**.
2. Set the **LDAP Server** and **LDAP Base Directory** fields, select the **LDAP SSL** check box. Leave the **LDAP SSL DB Path** field blank.

   Note: You can set the **LDAP SSL DB Path** field, but the certificate file will never be verified during the login. Before this patch, this field must be set to the path of the certificate file.
3. Click **Set File/Field level mapping**, enter `operator` in the **Name** field, then map the **Name** field to `sAMAccountName` (for AD server).
4. Set `ldapsslallownocert:1` in `sm.ini`.

If you wish to authenticate SM users that belong to different domains or sub domains, you can deploy multiple LDAP servers that belong to the corresponding domains, and then set up a horizontal scaled (HS) cluster. By proper configuration, users belong to Domain 1 can directly connect to server node 1 and get authenticated by LDAP server 1, users belong to Domain 2 can directly connect to server node 2 and get authenticated by LDAP server 2. Hence, they can share the same database while at the same time get authenticated by different domain's LDAP servers over SSL without any certificate being provided.

The following steps describe how to configure it:

1. Leave everything on the **LDAP Mapping** page empty; only map the **Name** field of operator file to `sAMAccountName` (for AD server).

2. In sm.ini, add a parameter: ldapserver1:IP%636%DN Search Base, where IP is the IP address of the LDAP server. Different LDAP servers' IP should be set on different SM APP server nodes.

3. Set ldapsslallownocert:1 in sm.ini.

Note: In both cases above, you still need to set the ldapbinddn and ldapbindpass parameters in sm.ini.

Please note the following when you configure the ldapserver parameter, which is used to set 1~99 backup LDAP servers:

- The old separator "," is replaced with "%", because Domain Name (DN) search base should have "," in it.

  Now the format of this parameter is:

  ldapserver<XX>:<host>%<port>%<DN Search Base>%<Server CA's root cert path>.

- If the LDAP SSL port number is not 636, then the <Server CA's root cert path> part of the ldapserver parameter must *not* be empty, you can set it to any character string (it still will not be used when ldapallownocert is turned on), we suggest to set it to SSL. In this case, the parameter looks like:

  ldapserver1:16.183.93.217%1234%cn=users,dc=swsm,dc=ind,dc=lab%SSL

- If the <DN search base> part of the parameter is not set, RTE will use the one set in the **LDAP Mapping** page.

  If both are set, the one set in the ldapserver parameter will be used during LDAP search.

  If both are empty, a warning will be logged in the sm.ini file.

Service Manager verifies the Oracle DB version during start-up

Prior to this release, Service Manager does not check the version of Oracle DB during start-up. In this release, after Service Manager is connected to the Oracle DB and prints out the "Connection to dbtype" message, Service Manager checks the Oracle Server and Client versions.

- If the DB version is unsupported, for example, Oracle Server/Client version 10:
  - Service Manager will disconnect the DB server if the allowunsupporteddbversion parameter is configured to 0 in sm.ini.

  - Service Manager will connect the DB server if the `allowunsupportteddbversion` parameter is configured to `1` in `sm.ini`.

- If the Oracle Client version is 11.2.0.1 or 11.2.0.2, the `allowsupportteddbversion` parameter does not work and customer needs to upgrade the Oracle Client version to 11.2.0.3 or above according to Service Manager 9.32 support matrix:

  http://support.openview.hp.com/selfsolve/document/KM00491737

For more information about the `allowunsupporteddbversion` parameter, see "Startup parameter: allowunsupporteddbversion" below.

Viewing Patch Level Information

Before this release, when you run the `sm -version` command, you can see the version and build number of your Service Manager, but you cannot determine the patch level that you have applied to your system.

As of this release, you can view the patch level information when you run the `sm -version` command.

For example, now if you run the `sm -version` command after you apply this patch, you will see the following:

```
----HP Service Manager Version/Environment Details-----
  Executable name: sm
          Version: 9.32.1001
      Patch Level: P1
```

For more information, see "QCCR1E97612" on page 13.

New Parameters

This release introduces the following new parameters.

Startup parameter: allowunsupporteddbversion

Parameter

allowunsupporteddbversion

Description

This parameter specifies whether the unsupported Oracle DB versions are allowed or not when Service Manager connects to the DB server. After Service Manager is connected to Oracle DB and prints out the "Connection to dbtype" message, Service Manager checks the Oracle server and client versions. If the DB version is unsupported and the parameter allowunsupporteddbversion is configured to 0, Service Manager will disconnect the DB server.

See also "QCCR1E98628" on page 14.

Valid if set from

Server's OS command prompt

Initialization file (`sm.ini`)

Requires restart of Service Manager server?

Yes

Default value

0

Possible values

0: Do not allow unsupported Oracle DB versions.

1: Allow unsupported Oracle DB versions.

Example usage

Command line: `sm -allowunsupporteddbversion:0`

Initialization file: `allowunsupporteddbversion:0`

Startup parameter: ldapsslallownocert

For information on how to use this parameter, see "Enabling LDAP over SSL without setting any certificate on the SM server side" on page 7

Startup parameter: maxmemoryperthread

Parameter

maxmemoryperthread

Description

This parameter specifies the maximum memory allowed for a session (in MB). After the limit is reached, the session is terminated. By default, this parameter is disabled (set to 0), which means there is no memory limit for each session and therefore each session can use the maximum memory available to the server's operating system.

See also QCCR1E72835.

Valid if set from

Server's OS command prompt

Initialization file (`sm.ini`)

Requires restart of Service Manager server?

Yes

Default value

0 (Disabled)

Possible values

0 (Disabled): No limit, and the server's OS memory limit is used instead.

100 or greater: Use the specified value (in MB) as the maximum memory allowed for a session. After the limit is reached, the session is terminated. If a value less than 100 is specified, Service Manager will display a warning message.

Example usage

Command line: `sm -httpPort:13080 -maxmemoryperthread:500`

Initialization file: `maxmemoryperthread:500`

Fixed Defects

This release fixes the following defects.

Server

CR	Problem	Solution
QCCR1E56264	When you enable LDAP over SSL in Service Manager, the root certificate of the CA that issued the LDAP server's certificate need be set on the SM server side. This requirement is unnecessary and causes inconvenience to customers who wish to enable LDAP over SSL, or to deploy LDAP over SSL in a more flexible way.	In fact, the client side verification on LDAP server's certification is not mandatory to implement LDAP over SSL. In this solution, a new parameter `ldapsslallownocert` is added. When you set this parameter to `1`, RTE will no longer check that issuer CA's root certification, in fact customers can skip providing any LDAP server cert. For more information, see "Enabling LDAP over SSL without setting any certificate on the SM server side" on page 7.
QCCR1E63154	When users perform a search that includes only stop words, they get the following message: "No incidents found." This message can confuse users, because they do not know the hundreds of stop words and the system does not tell them that it ignored every word of their search string so nothing was searched.	Now when all of the input search text are stop words, RTE will return an extra message, which says "The search text entered contains only excluded words".

CR	Problem	Solution
QCCR1E72835	An Administrator cannot limit the amount of memory consumed by individual threads in SM. An Administrator may want to do this when a poorly created view causes servlets to consume too much CPU and memory and then terminates the servlets.	The new `maxmemoryperthread` parameter has been added. This parameter specifies the maximum memory allowed for a session (in MB). After the limit is reached, the session is terminated. **Note:** The minimum is 100 MB, and the maximum is as permitted by the server OS (Set the parameter to 0 to use the OS limit).
QCCR1E96811	Attachments cannot be transferred to SM using external web service. There is no error message in the Web service call, attachments not transferred to staging table.	Even the placeholder key is provided in the CREATE web service request, the sent attachments are stored in table and associated with the key of the created record.
QCCR1E97612	Users have no way to identify the patch or hotfix information from the RTE log or the RTE command "sm -version". From the RTE command "sm -version", you can only see the version string and build number, but you cannot determine which patch or hotfix has been applied.	Now when you run the RTE command "sm -version", you can see the exact patch level information such as P2HF2.
QCCR1E97620	The following message is written to the log over 4,000 times over a few days: `RTE D Login: Could not find field user.login.count in operator file.`	When a field in operator record is null, the system initializes the field instead of writing out the error message.
QCCR1E97999	SM server runs with application version lower than 9.32 when primary key mode is enabled.	Now primary key mode can only be enabled when running with application version 9.32 or higher.

CR	Problem	Solution
QCCR1E98059	Memory leaks when exception is thrown in handling request to doc engine	No memory leak occurs when exception is thrown in handling request to doc engine.
QCCR1E98628	When Service Manager is running on an unsupported version of Oracle, Service manager should refuse to start rather than potentially corrupting data.	After RTE is connected to Oracle DB and prints out the "Connection to dbtype" message, RTE will check the Oracle server and client versions. If the DB version is unsupported, and the new parameter `allowunsupporteddbversion` is configured to `0` (do not allow unsupported versions), RTE will disconnect the DB server. For more information, see "Startup parameter: allowunsupporteddbversion" on page 9.
QCCR1E98809	When the primary key mode is enabled, the JS function doSave() fails if you save the same record twice.	When the primary key mode is enabled, the JS function doSave() can run successfully even if you save the same record twice.
QCCR1E99117	when you run a cross table query and in the where clause if a field is mapped to BLOB/Clob/Image, client shows a duplicate error message: `Queries on Blob/Clob/Text/Image field is not supported in cross table query. Queries on Blob/Clob/Text/Image field is not supported in cross table query.`	Remove the duplicate error message, and specify the field name that is not qualified.
QCCR1E99331	The RTE call "tagquery" cannot generate the query from tag when the primary is enabled.	The RTE call "tagquery" can generate the query correctly.
QCCR1E99296	SM 9.32 does not run on SUSE Linux 10.1, it fails with floating point exception.	SM 9.32 can run on SUSE Linux 10.1.

Web Client

CR	Problem	Solution
QCCR1E98637	If you enter texts in a dropdown list and then click the expand icon, the matched item does not scroll into view.	Now , if you enter texts in a dropdown list and then click the expand icon, the matched item can scroll into view.
QCCR1E99699	You create an external link (for example, http://www.google.de) in MySM. When you attempt to open the link, your attempt fails with `HTTP 404 / Page Not Found`.	You create an external link in MySM. When you attempt to open the link, the web page can be opened. **Limitation:** If your web tier works in an SSL environment (https mode), the external link cannot be opened due to the browser security settings.
QCCR1E98705	The uploaded image is not displayed when editing Service Catalog items.	The uploaded image is displayed correctly.
QCCR1E98708	The image file spacer.gif is "Not Found" in a 404 error page.	The whitespace image can be shown in 404 page now.

Known Problems, Limitations, and Workarounds

This software release has the following known issues and limitations. This is a cumulative list of known issues and limitations in Service Manager 9.32, including those that are already documented in previous release notes (Service Manager 9.31 and patches).

Issues in SM9.31 and Patches

Global ID	Problem	Workaround
QCCR1E63663	The Service Manager (SM) client loses connectivity during JavaScript execution of the file.list RAD application.	No workaround available. Created a knowledge article (KM1166532), which states that Service Manager does not currently support calls from JavaScript on RAD applications that use the rio/fdisp panels.

Global ID	Problem	Workaround
QCCR1E57385	When Service Manager is running on Unix, the legacy listener may log intermittent signal 11 upon CIT initial connectivity test if exec-shield is not set properly.	Use one of the following solutions to solve this issue on Unix. **Solution 1**: Connect Connect-It to the Web Services connector instead of the Legacy Listener connector. **Solution 2**: Before connecting Connect-It to the Legacy Listener connector, do the following: 1. Add usethreading:0 in the sc.ini file, which is located in <Service Manager server installation path>\LegacyIntegration\RUN. **Note**: For 64-bit RedHat Linux servers only, you can alternatively run the following shell commands as root: # sysctl -w kernel.exec-shield=0 # sysctl -w kernel.randomize_va_space=0 2. Start the legacy listener.

Global ID	Problem	Workaround
QCCR1E67491	When the collation of the db instance is Chinese_PRC_BIN, Web service clients fail to connect to Service Manager (SM). Only ASCII operator names are supported, so only ASCII operator names can be used.	**Note**: This issue only exists in Web service integrations. Therefore, the SM clients do not have this problem. When SM is handling an incoming SOAP request, the authorization string is decoded by BASE64Decoder. SM uses the decoded string value to construct a UTF-8 string that is used in the RTE. However, the authorization string is in the header and SM does not know the charset or encoding of the underling string value, which is BASE64 encoded. Therefore, if the underlying string value is not UTF-8, this problem will occur. In SM, when fetching an operator record from the database, no matter what collation the database uses, the operator record finally will get a UTF-8 operator value. However, even if users put the same value in the authorization header, the operator name may differ because of the charset/encoding issue. Because of this, the operator will fail to log on. This is a limitation of SM. Do not use non-ASCII characters in operator names. Created a knowledge article (KM1442479) to document this limitation.

Global ID	Problem	Workaround
QCCR1E75182	HTML email truncates the body of the message and sends the HTML code without translating it.	When the content of an HTML email template exceeds 8192 bytes in size, the content will be truncated and displayed as HTML code. Make sure your HTML email templates do not exceed this size limit.
QCCR1E89890	Grouped Views are not correctly updated after logging a new Incident.	When you log a new incident, to keep consistency with actual incidents, the group number is not updated. You need to click the "Refresh" button to update grouped Views.
QCCR1E72835	Add the ability to limit the memory consumed by individual threads in SM as specified by an Administrator.	The requested change is not implemented to avoid performance degrade. No workaround is currently available.
QCCR1E77563	Signal 11 error is received when calling the toXMLString() routine of the Users object.	No workaround is currently available.

Global ID	Problem	Workaround
QCCR1E88222	An unload file that is exported from an Oracle to an SQL Server database fails to import when the unload file already contains a RECORD_KEY field and the length of first unique key exceeds the db limitation.	This request is caused by the product running in an unsupported configuration. Change to a documented and supported configuration. If the problem still exists in a supported environment, contact HP Support. To work around this issue, do not use "RECORD_KEY" as a SQL Name for a field in dbdict. This field name is reserved by SM. To do this, follow these steps: 1. Enter `dbdict` in the SM command line box. 2. Enter "esdquestions" in to the search field, and then click the Search button. 3. Select the "record.key" field, and then change the SQL Name from "RECORD_KEY" to anything else.
QCCR1E74808	After clicking the **Cancel** button in the Condition Editor from the Workflow Editor, the current tab sometimes becomes a blank screen and the tab cannot be closed.	No workaround is currently available.

Issues in SM9.32 and Patches

Service Manager Issues

Global ID	Problem	Workaround
QCCR1E64377	In the web client, when a Configuration Item (CI) record is opened, the CI label does not show (or only shows for the first time) in the CI Visualization (Relationship Graph). This issue occurs only when JRE 6 is used.	As Oracle has fixed this Applet issue, JRE 6 customers need to upgrade their JRE to the latest JRE6 or JRE7 on the machine that runs Internet Explorer or Firefox in order for CI Visualization to display CI labels correctly.
QCCR1E95418	CI Relationship Graph is not immediately refreshed after changing CI Relationships.	No workaround is currently available.
QCCR1E95725	Due to a known issue in JDK (bug id:7196513), CI icons are not displayed correctly in Firefox when Httponly cookies are enabled in the web application server.	When Httponly cookies are enabled, users can only use Internet Explorer 7 or higher for CI icons to display correctly. As Oracle has fixed the Httponly cookie issue as of JDK 7u6, users need to install the latest 32-bit JRE (7u6 or above) on the machine that runs Internet Explorer 7 or higher.
QCCR1E95963	An error occurs when loading a dbdict twice in an unload file. The two dbdict records have the same name, but different key types: the first one has unique key, while the second's key type is primary key.	Do not export to an unload file a dbdict record whose key type has changed.

Global ID	Problem	Workaround
QCCR1E97260	When SSL is enabled between the web application server and Firefox, a ClassNot found Exception error displays in the workflow section of the Change form. This issue does not occur in IE or in Firefox without SSL enabled.	There are two workarounds: • Use Internet Explorer instead of Firefox. • If using Firefox, import the client certificate into the Java console on the end user's machine. Here are the steps for Windows 7: a. Open Control Panel, and i n the Control Panel Search box enter "`Java Control Panel`". b. Double-click the Java console icon to open the Java console. c. On the **Security** tab, click **Manage Certificates ...**. d. On the Certificates window, select certificate type: **Client Authentication**, and click **Import**. e. Follow the wizard and import the client user's certificate.
QCCR1E97492	Clicking the **Back** button on the CI Visualization page (which opens when you click **More** > **Expand CI Visualization** in a CI record) causes a Firefox crash.	No workaround is currently available.

Global ID	Problem	Workaround
QCCR1E97539	If JRE 7 (update 21 or greater) is used in the web browser, when the user opens a configuration item the browser displays a security warning: `Block potentially unsafe components from being run?` The reason why this warning occurs is that as of Java SE 7 update 21, JavaScript code that calls code within a privileged applet is treated as mixed code and warning dialogs are raised if the signed JAR files are not tagged with the Trusted-Library attribute.	This warning does not indicate the Service Manager product is unsafe. Ignore this warning and select **Don't Block** in the warning dialog to continue.
QCCR1E97603	If a format that contains a button with Enable condition is created or modified by using a SM9.31 patch 1 server, when using it in SM 9.31 GA or earlier, the client crashes. However, formats created by using the SM9.31 GA or earlier server work fine.	Upgrade both of the SM server and client to the same patch level: SM 9.31 patch 1 or later.
QCCR1E94657	When PDCP4 is applied, the first group on the form is not shown in the Jump Address drop down list.	Move the scroll bar to the top-most position and then you will see the first group.
QCCR1E97856	In a single-line text field, some special characters whose HTML code is `&#x...;` (where ... stands for a hex number) are not represented as their original format. Instead, they display as `&#x...;`. However, such characters are represented as the original format in other widgets (textarea, label, message panel, and so on).	No workaround is currently available.

Global ID	Problem	Workaround
QCCR1E98343	When you try to remove a group from the permission list of a Knowledge Category record, if you select the group by clicking on the white space in either cell and then click the "Remove" button, the group is still there.	Before clicking the "Remove" button to remove the group, try making the selection by clicking on the text in either cell.
QCCR1E98705	The image uploaded for a service catalog item displays as broken (a cross-mark).	Go ahead to save the current record. When you retrieve this record again, the image will display correctly.
QCCR1E93604	The HTTP Response Code is 200 instead of 400 when a RESTful request uses an invalid sort field separator (for example, a plus symbol).	Use a valid sort field separator.
QCCR1E94204	Because of the incorrect status, the operation could not proceed after merging a record.	Reset the status of this record (for example, reopen the closed record) and perform the last operation again.
QCCR1E94206	The last operation could not be repeated after merging a record because the button for the last operation disappears.	Reset the condition for the button in this record, for example, Reopen the closed record, and perform the last operation again.
QCCR1E96353	RESTful API: An incident record is successfully resolved when posting an incident resolve action with a blank "ClosureCode" and "Solution".	Validation is not performed for the fields. To work around this issue, validate them at the RESTful client side, or manually add validation for the fields to the format control.
QCCR1E96391	Restful API: Results are in the wrong order when sorted by an array field. This issue occurs because the SM RTE does not support sorting by array fields. A list is returned without any error message.	No workaround is currently available.

Global ID	Problem	Workaround
QCCR1E97898	Restful API: A 400 Bad Request error occurs when a RESTful API request is a cross-table join query.	The RESTful API framework supports simple queries and SM native queries. Currently RESTful API framework does not support cross-table SQL queries.
QCCR1E98320	When a record is removed after being read, the Merge function still allows the user to merge the record and the user's input is lost.	No workaround is currently available.
QCCR1E98227	In Approval Delegation wizard, go to another page (do not change the delegation module) after choose the operator to delegate in "Select Approval Groups" page, then back to "Select Approval Groups" page again. You will find a blank line is displayed in the right table, instead of the operator record.	This is only a display issue, and will not impact the functionality. If you need to remove the operator from the delegation list, choose the blank line, and then click the remove icon; otherwise the operator will be successfully delegated once you save the update.
QCCR1E98576	when there are conflicted updates on system fields, the system displays the message "The conflicted fields cannot be merged. Reload the record.", whereas the Merge button is available. Actually, the merge function should not be available in such case.	Ignore the Merge button. Reload the latest record to edit this record again.
QCCR1E98398	When you are updating a record and adding attachments to this record, if your updates conflict with another users' updates or the updates of a background process, the attachments will be lost after either automatic or manual merge.	After automatic or manual merge, add the attachments again before saving the merged result of the record.

Global ID	Problem	Workaround
QCCR1E98411	SRC failed to retrieve service catalog items from SM on upgrade from SM 7.11 to SM 9.32.	In the svcCatalog dbdict, the id.attach field is character type, which should be number type. The id.attach field is an alias of the id field in the svcCatalog table. To fix the issue, change the field type using the Dbdict Utility.
QCCR1E98606	When purging all duplicated records for upgrade, the following error message occurs: `No display screen named "kmgroup.save" found`	No workaround is currently available.
QCCR1E98618	Subcategory data on the Incident form is not available after upgrading from ServiceCenter 6.2 to Service Manager 9.32. Subcategory data is not upgraded.	If necessary, manually add the subcategory data. 1. Enter `db` in the SM command line box. 2. In the Table field, enter `subcategory`, and click **Search**. 3. For each Catagory in the dropdown list, add the following Areas (enter a value in the Area field and click **Add**): `access`, `data`, `failure`, `hardware`, `performance`, and `security`.

Global ID	Problem	Workaround
QCCR1E98713	After applying an upgrade, the following error message occurs: `Unable to open file <file path> for writing`	This error has no impact on the upgrade, and can be ignored. To prevent this message from occurring, do the following before applying an upgrade: 1. In Database Manager, search for table `help`. 2. Double-click **help.detail**. 3. Enter the following values, and click **Search**: File Name: `formatctrl` Format: `formatctrl.maint.seq.b` Term: `Format Control maintenance - Sequentially Numbered fields` 4. Click **Delete** to delete the record.
QCCR1E98298	Survey Integration: If you use an invalid parameter name when you configure a survey with an API-based connector, the parameter is replaced with an empty value incorrectly.	Do not use invalid parameter names.
QCCR1E98299	Survey Integration: When you use the Mass Update utility to update multiple survey records, ruleset validation does not work.	No workaround is currently available.

Global ID	Problem	Workaround
QCCR1E98475	With Process Designer Content Pack 9.30.3 applied, the Merge functionality does not work when a user clicks **Save & New** in an interaction record opened through a search. 1. Open an interaction through a search. 2. Update the Title. 3. Another back-end process has updated the Title to another value. 4. Click **Save & New**. An error occurs: `This record has changed since you selected it.` You cannot perform Merge for the conflicted updates as expected.	If you encounter the error "This record has changed since you selected it." when clicking the **Save & New** button on an interaction opened through a search, to avoid abandoning your updates, do not use the **Save & New** button to save your updates; instead, first click the **Save** button to save your updates with the merged result, and then register a new interaction from the navigation menu.
QCCR1E99998	The following text string in the web tier is not localized: File: `<webtier-9.32.war>WEB-INF/lib/cwc-9.32..jar/com/hp/ov/cwc/web/login.properties` Text: `Logout.WarningMessage.CloseBrowser=Please close your browser window.`	Manually localize it using the `native2ascii` tool. For detailed steps, see the SM9.31p2 Release Notes.
QCCR1E99940	Customers who use Solaris 9 cannot upgrade Service Manager to SM9.31p2 and above patches because JRE7 does not support Solaris 9 and SM starts with a JRE validation, which constraints the JRE version below JRE7 up15.	Modify the `validjava.sh` file under the Service Manager `RUN/` folder, for details, see "Appendix. Workaround for QCCR1E99940" on page 51.

Service Request Catalog Issues

Global ID	Problem	Workaround
QCCR1E90074	When entering a search string in Service Request Catalog, auto-complete does not work if the browser's preferred language is set to an East Asian language (for example, Simplified Chinese).	No workaround is currently available.
QCCR1E98339	Custom fields do not load the DEFAULT company value when the checkout panel is empty for one of the three checkout panels of your company.	After upgrade, you should manually add the same structure configuration of the DEFAULT company for the empty checkout panel of your company. For example, before upgrade, you, as an SRC administrator, only defined custom fields for the Service Catalog checkout panel for your company. After upgrade to SM932, if you want to use the support checkout panel and generic support checkout panel in SRC correctly, you need to manually add OOB configurations for the Support Catalog and Generic Support checkout panels, which you can copy from those panels of the DEFAULT company.

Backup and Backout Instructions

In case you need to restore your Service Manager system to its original state after installing the component patches in this release, make necessary backups before each patch installation. If a rollback is needed, follow the backout instructions.

Server

Backup

Before applying the server patch, make a backup of the server installation folder. For example, `C:\Program Files\HP\Service Manager` 9.30`\Server`.

> **Note:** If you have a horizontally scaled system, be sure to back up the server installation folder for each server instance.

Backout

Service Manager 9.32 supports FIPS mode. To run SM in FIPS mode, you must upgrade your database to the 256-bit AES encryption algorithm. Once you change all of the encrypted fields to use the new 32 character encryption you cannot roll back the RTE and still read the encrypted data.

After installing the patch, do the following to backout:

1. Stop the Service Manager server.
2. Remove the existing server installation folder.
3. Copy the backup folder back.

   > **Note:** Make sure that the embedded Tomcat is also replaced with the backup, because the version of the embedded Tomcat may have dependency on a specific server version.

   > **Note:** If you have a horizontally scaled system, make sure that every server instance is replaced with its backup.

4. If you have also loaded platform unload files required for your server changes, you must also roll back the application changes made by the unload files. See "Applications" on page 32.
5. For Unix-based platforms other than Linux, make a backup of your JRE if you have not yet upgraded to JRE 1.7.
6. Restart the Service Manager server.

Web Tier

Backup

Before deploying the new web tier, make a backup of the following items:

- web.xml file
- application-context.xml
- log4j.properties
- splash screen
- style sheets
- any other customizations you made, including your webtier-<version>.war (webtier-ear-<version>.ear) file.

Backout

To roll back to the old web tier:

1. Delete or uninstall the existing web tier.
2. Clear the cache of your web application server (for example, Tomcat).
3. Redeploy the old web tier.
4. Restore your old customizations.

Windows Client

Backup

1. Make a backup of your Windows client home folder, for example, `C:\Users\<username>\ServiceManager`. Your connections and personalized settings are stored in this folder.

   Note: This is the out-of-the-box home directory, and could differ from yours if you made changes to `<Client>\configuration\config.ini` file. If so, back up the files from the location specified in that file.

2. Make a backup of your certificate configuration files if any (**Window** > **Preferences** > **HP Service Manager** > **Security**). For example, your CA certificates file and client keystore file.

Backout

1. Uninstall the new Windows client.
2. Reinstall the previous Windows client.
3. Restore your old Windows connections and configurations.

Applications

If you plan to upgrade your applications to this release level, make a backup of your database before the upgrade, in case you need to restore your database after the upgrade. Creating a backup of the entire database and restoring the database if needed is a better approach for a full applications upgrade.

If you plan to load individual unload files in this release, follow the backup and backout instructions below.

Backup

> **Tip:** If your application version is 7.11 ap3, 9.21 ap3, 9.30 ap3, 9.31 or later, you are recommended to use Unload Manager to make a backup of the files to be modified by an unload file, because Unload Manager can create a backup of your old data during the installation of the unload; if your application version is other than any of these, Unload Manager is not available and you can use Database Manager instead.

To use Unload Manager to make a backup:

1. Go to **System Administration** > **Ongoing Maintenance** > **Unload Manager**.
2. Double-click **Apply Unload**. A wizard opens.
3. Select the unload file you want to apply, also specify a backup file, and then click **Next**. Details of the unload file appear.
4. Double-click a conflicting object in the table to open the merge tool:
   a. Merge the object, and then select the **Reconciled** check box.
   b. Click **Save** to go back to the wizard.
5. Click **Next** after all the conflicting objects are reconciled.
6. Click **Yes** on the confirmation window to apply the unload.
7. Click **Finish**.

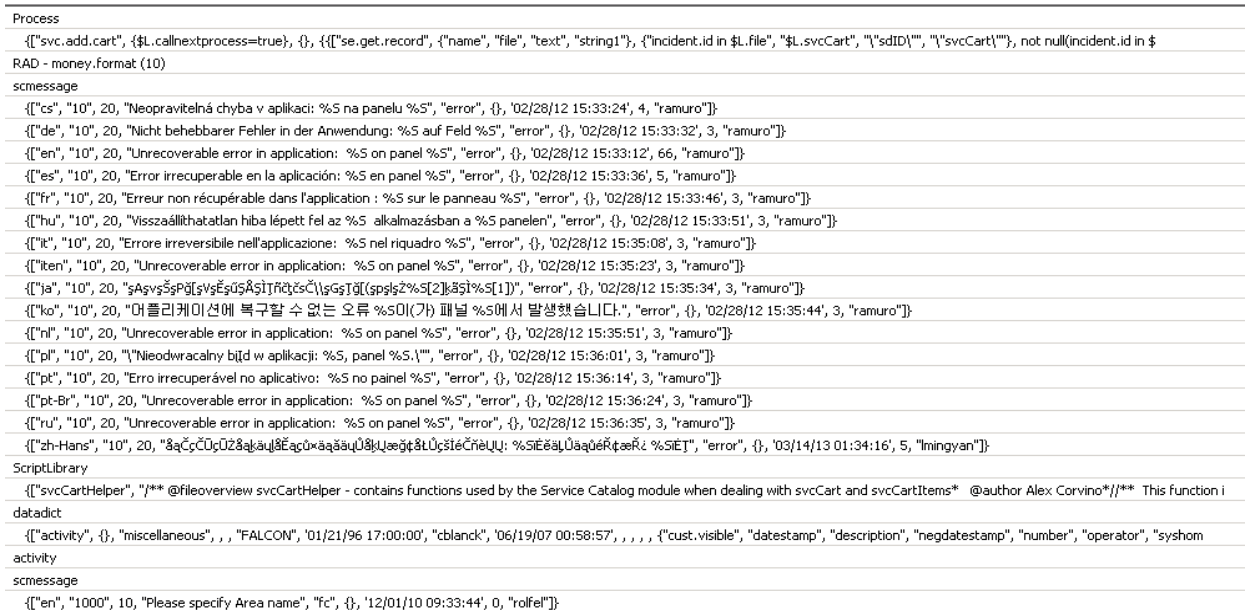
   Now, the unload has been applied and at the same time your old data backed up.

To use Database Manager to make a backup:

1. Go to Database Manager, select **Import/Load** from **More** or the More Actions menu, and browse to the unload file.
2. Click **List Contents** on the menu bar, to view a list of files that have been updated in this

unload.

See the following figure for an example.



This figure shows the contents of an unload file that contains changes to the following files:

File	Record
Process	svc.add.cart
application	money.format **Note**: The `scmessage` records listed under each RAD application are messages used in this RAD application; no backup is needed for them.
ScriptLibrary	svcCartHelper
datadict	activity
dbdict	activity **Note:** The “activity” file with no records actually represents the dbdict record of the activity file.
scmessage	The record whose message class is “fc” and message number is 1000.

3. Go to Database Manager, in the Table field enter a file name you got in step 2, and click the Search button.

4. If the format selection page shows, select the proper format by double-clicking it (for example, select the `device` format for the `device` file), and then search for the file record.
5. Click **More** (or the More Actions menu) > **Export/Unload** after the file record displays.

   Note: If **Export/Unload** is not available, check the **Administration Mode** check box in Database Manager and try again.

6. In the pop-up window, specify your backup upload file path/name, and click **Unload Appl**.

   Caution: Make sure that **Append to file** is selected.

7. Repeat steps 3 through 6 to back up the rest of the files you got in step 2.

Backout

Tip: You can use Unload Manager (recommended) or Database Manager (if Unload Manager is not available in your application version) to roll back to your old data, as described in the following.

To roll back to your old data using Unload Manager:

1. Go to **System Administration** > **Ongoing Maintenance** > **Unload Manager**.
2. Double-click **Apply Unload**. A wizard opens.
3. Select the unload file generated in the backup process, specify a backup file, and then click **Next**. Details of the unload file display.
4. Double-click a conflicting object in the table to open the merge tool:
   a. Merge the object, and then select the **Reconciled** check box.
   b. Click **Save** to return to the wizard.
5. Click **Next** after all the conflicting objects are reconciled.
6. Click **Yes** on the confirmation window to apply the backup unload.
7. Click **Finish**.

To roll back to your old data using Database Manager:

1. Go to Database Manager, click **More** > **Import/Load**.
2. Browse to the backup unload file you created.
3. Click **Load FG**.

Knowledge Management Search Engine

To backout your Knowledge Management (KM) search engine changes, make a backup before your KM patch installation.

Note: Keep in mind that you also need to roll back KM-related server side and application side changes. For details, see the Server and Application backup and backout Instructions.

Backup

Before applying the KM patch and upgrading the JDK and KM embedded Tomcat, do the following:

1. Make a backup of the search engine installation folder. For example, `C:\Program Files\HP\Service Manager 9.30\Search Engine Backup`
2. Make a backup of the files to be modified by the unload files in the KM patch.
3. Make a backup of your `schemastub.xml` file under directory `<SM server>/RUN/km/styles/`.

Backout

After installing the patch, do the following to backout:

1. Stop your KM search engine.
2. Remove the existing search engine installation folder.
3. Copy the backup folder back.
4. Rollback the previous JDK installation and change the `JAVA_HOME` environment variable back.
5. Be sure to roll back KM related changes on the SM server and application sides, including the `kmsolr unloads` files and the server's `schemastub` file.
6. Restart your KM search engine.
7. Perform a full re-indexing on all of your knowledgebases.

Installation Notes

This section provides instructions on installing each component in this patch release.

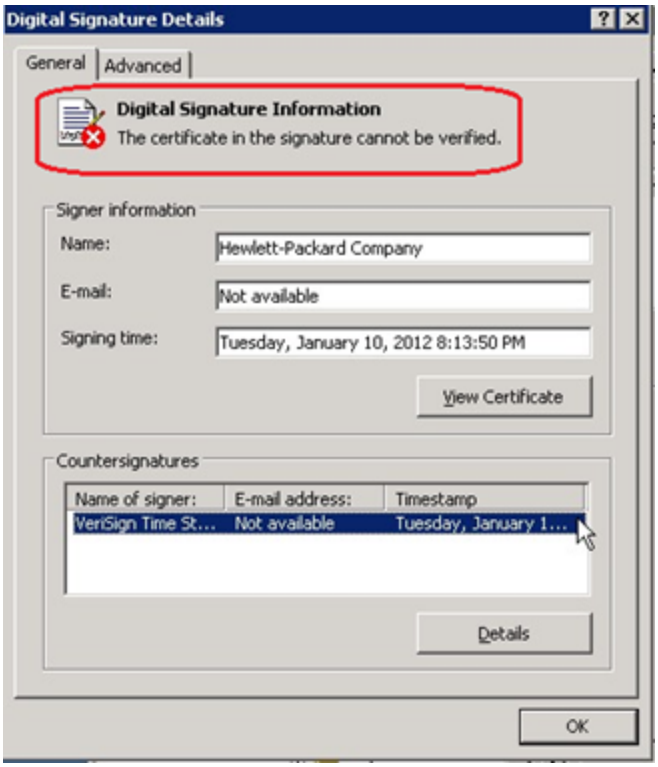
Before you proceed, HP recommends that you consult the latest *Service Manager 9.32 Support Matrix* and the *Compatibility Matrix for Service Manager Applications Content* at:

http://support.openview.hp.com/sc/support_matrices.jsp

For more information, see "Service Manager Support Matrix and Applications Content Compatibility Matrix" on page 50.

Digital Signature Notice

HP signs Windows executable files with a digital signature. Since January 2012, this process has been updated to use a new VeriSign root certificate. On a Windows system that does not have the new VeriSign root or intermediate certificate installed, when the user right-clicks the file and then goes to **Properties** > **Digital Signatures** > **Details**, a verification error will display: “The certificate in this signature cannot be verified.”



To resolve this issue, either enable Windows Update or download and install the G5 Root certificate as documented at: **https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&actp=CROSSLINK&id=SO19140**

Server Update Installation

The server update for your operating system (OS) consists of a compressed file, `sm9.32.1001-P1_<OS>.zip` (or `.tar`), which contains updated files of the Service Manager server. These files add to or replace the files in the `[SM Server Root]\([SM Server Root]/)RUN, irlang, bin, legacyintegration`, and `platform_unloads` directories.

Note: If using an Oracle RDBMS, be aware that Oracle Call Interface (OCI) 11.2.0.3 is required for SM9.30p5, SM9.31, SM9.32 and later. See the latest *Service Manager 9.32 Support Matrix* at http://support.openview.hp.com/sc/support_matrices.jsp.

Built-In Troubleshooting Tool (SM Doctor)

Additionally, this server patch includes an installation of the HP Service Manager Doctor (SM Doctor) tool. The server patch will install the tool in the `[SM Server Root]\([SM Server Root]/)smdoctor` directory. For information on how to use this tool, see the *Guides and reference* > *Troubleshooting* > *HP Service Manager Doctor* section in the online help.

Upgrade Paths

This server patch must be applied on top of one of the following versions/patch levels of the SM server:

- SM9.30 GA
- SM9.30 Patch/Hotfix
- SM9.31
- SM 9.31 Patch/Hotfix
- SM 9.32

The following server upgrade paths are recommended:

- New customers: Install the SM9.30 GA server, and then directly apply this server patch;
- Existing SC6.2, SM7.11, and 9.21 customers: Uninstall the old server, install the SM9.30 GA server, and then apply this server patch;
- Existing SM9.30, 9.31, and 9.32 customers: Apply this server patch.

For installation instructions of the SM9.30 GA server, see the *Service Manager 9.30 Interactive Installation Guide*, which is available from the HP Software Manuals Site: **http://support.openview.hp.com/selfsolve/document/KM1195794**

For installation instructions of the server patch, see "Server Patch Installation Steps" on the facing page.

Compatibility Mode for Installation on Windows Server 2012

As of this release, Windows Server 2012 is supported. Be aware that compatibility mode is required for installing the SM9.30 GA server on Windows Server 2012 (not required for Windows Server 2008). To run your server installation in compatibility mode, do the following:

1. Right–click the server's `setupwin32.exe` file icon.
2. Click **Properties** > **Compatibility**.
3. Click **Run this program in compatibility mode for** and select **Windows Vista (Service Pack 2)**.
4. Click **Apply** and **OK**.
5. Run the `setupwin32.exe` file to complete the installation.

When uninstalling your server on Windows Server 2012, you should also use compatibility mode. To do so, set your Windows server uninstaller file (`_uninst\uninstaller.exe`) to compatibility mode as described above and then uninstall the server using the uninstaller or from your Control Panel.

Server Patch Installation Steps

Caution:

- The server patch will upgrade your embedded Tomcat to version 6.0.36, and therefore requires additional steps.
- The server patch will upgrade your JGroups (in the `RUN/lib` directory) to version 3.2.
- Starting with SM9.31p2, the SM server requires JRE 1.7. For Windows and Linux, the embedded JRE has already upgraded to version 1.7; for other Unix-based platforms, you need to manually perform this JRE upgrade.

  The JRE upgrade will cause external web service calls over SSL to fail if the remote endpoint does not support Server Name Indication (SNI), which is by default activated in JRE 1.7. Once Service Manager is upgraded to use JRE 1.7, it starts to use SNI extensions during the SSL handshake. If the remote endpoint does not support SNI, the web service call will fail with an error message. To solve this issue, do either of the following:

  - Activate SNI at the remote end point (recommended)
  - If the remote endpoint does not support SNI extensions, and SNI cannot be activated, add the following JVMOption<n> parameter either to the `sm.ini` file, or to the start command of the servlet(s) in the `sm.cfg` file:

    ```
    JVMOption2:-Djsse.enableSNIExtension=false
    ```

Note: If you have a horizontally scaled system, you must upgrade all of your server instances.

1. Stop all Service Manager clients.
2. Stop the Service Manager server.
3. Make a backup of the Server installation directory. See also "Backup and Backout Instructions" on page 30.
4. Delete the `RUN/tomcat` directory. Tomcat in this directory will be upgraded to version 6.0.36 when you extract the server files later.
5. Delete the `RUN/lib` directory.
6. For Windows and Linux platforms, delete the `RUN/jre` directory.

   Note: This step is required only when you are upgrading from a server version earlier than 9.31p2. This is to avoid conflicts between the old 1.6-based JRE and new 1.7-based JRE.

7. Extract the compressed files for your operating system into the main Service Manager directory on the server. The default path is: `C:\Program Files\HP\Service Manager 9.30\Server`.
8. For UNIX servers, set the file permissions for all Service Manager files to 755.
9. For the following Unix servers, manually upgrade to JRE1.7 if you have not already done so.
   a. Install either JDK1.7 or JRE1.7 for your specific platform.

Solaris	JRE1.7 (update 15 or greater)
HP-UX	JRE1.7 (JRE_7.0.04 or greater)
AIX	JRE1.7 (SR4 or greater)

   b. Set your JAVA_HOME environment variable to point to JDK1.7 (if you have JDK1.7 installed) or JRE1.7 (if you have only JRE1.7 installed).
   c. Execute `\RUN\removeLinks.sh` to remove the old symbolic links and then execute `\RUN\setupLinks.sh` to create new symbolic links.
   d. Run the following command to check that the JRE version is 1.7:

   ```
   RUN\jre\bin\java –version
   ```

10. If you have made any customizations/changes to the original `RUN/tomcat` folder, restore them in the new `RUN/tomcat` folder.
11. Your old `schemastub.xml` file (in the `<SM_Server_Home>\RUN\km\styles\` directory) has been updated to a newer version. Either keep your old file by copying it back or keep the updated

version (a KM knowledgebase full reindexing is then required).

12. Run the `sm -unlockdatabase` command.

    Note: This step is required the first time you upgrade to 9.30p4 or later; it is also required whenever you change the server's IP address after your upgrade to 9.30p4 or later. The purpose of this step is to prevent stale license information from being kept in the system. In a scaling implementation, you can run this command from any one of your servers.

13. Restart the Service Manager server.
14. Restart the Service Manager clients.
15. Check the version in **Help** > **About Service Manager Server**.

    The server should be Release: **9.32.1001**.

Web Tier Installation

The web tier update consists of a compressed file, sm9.32.1001-P1_Web_Tier.zip, which contains the installation files (both the .war and .ear files) for installing the SM9.32 web tier. Installing the new web tier will upgrade your web client to this release level.

The installation steps are the same as installing the SM9.30 web tier. The specific installation process depends on your particular web application server. For detailed steps, see the *Service Manager 9.30 Interactive Installation Guide*, which is available from the HP Software Manuals Site: **http://support.openview.hp.com/selfsolve/document/KM1195794**

New Customers

You only need to install the new web tier using the .war or .ear file from the sm9.32.1001-P1_Web_Tier.zip file in this release. For installation instructions, see the *Service Manager 9.30 Interactive Installation Guide*.

Existing Customers

To upgrade your web tier to this patch level, you need to back up and uninstall your old web tier and then install the new web tier. The upgrade does not automatically save your web tier customizations. To keep your changes, you must back up your customized files and restore your customizations in the new deployment.

Note on Tomcat 7.0: If you plan to deploy the web tier on Tomcat 7.0 using the Tomcat Manager, be sure to set the `max-file-size` and `max-request-size` parameters (default: 52428800) in the `<Tomcat 7.0_Home>webapps\manager\WEB-INF\web.xml` to an appropriate value greater than the web tier .war file size; otherwise the deployment request will be rejected because the web tier .war file exceeds the default maximum values. This restriction does not exist in Tomcat 6.0.

To install the new web tier:

1. Make necessary backups. For details, see "Backup and Backout Instructions" on page 30.
2. Delete or uninstall the existing web tier .war (or the .ear) file.
3. Clear the cache of your web application server.
4. Deploy the new webtier-9.32.war (or the .ear) file following the instructions in the *Service Manager 9.30 Interactive Installation Guide*.

   Note: It is best practice to deploy with a unique context root. For example: /webtier-9.32.1001
5. Use a diff utility to compare the new web tier's `web.xml` file against your backed-up version to ensure that any new parameters are properly merged into the files used in your final deployment. Do this for `application-context.xml` as well as any other files you may have customized (such as style sheets and splash screens).
6. Make any new customizations necessary for your deployment.
7. Restart the web application server.
8. Check the version by clicking the HP logo (About HP Service Manager) icon.

   The web tier version should be: **9.32.1001**.

Windows Client Installation

This release does not contain any Windows Client update.The latest Windows Client package has been shipped with the SM9.32 release.

You can download this package from
http://support.openview.hp.com/selfsolve/document/KM00495872

For installation instructions, see the Service Manager 9.32 Release Notes.

Windows Client Configuration Utility Installation

This release does not contain any update for the Windows Client Configuration Utility. The latest Windows Client Configuration Utility package has been shipped with the SM9.32 release.

You can download this package from
http://support.openview.hp.com/selfsolve/document/KM00495874

For installation instructions, see the Service Manager 9.32 Release Notes.

Applications Update Installation

The latest Applications package has been shipped with the SM9.32 release.

You can download this package from
http://support.openview.hp.com/selfsolve/document/KM00495886

For installation instructions, see the Service Manager 9.32 Release Notes.

Application Unload Installation

Note: All unload files in the server's platform_unloads directory in this release have been already merged into the Service Manager 9.32 applications. These files are provided just in case you do not plan to upgrade to applications 9.32 while still want to take advantage of the relevant new features/fixes.

If a platform fix (in most cases, a server fix) also requires an applications change to resolve the relevant issue, an unload file is provided. Unload files introduced in earlier patches are also included in this cumulative release. If you have not already applied them for a previous patch, you should also apply the unload files that are intended for your applications version. For more details about these applications updates, see the Release Notes for those patches.

This patch release includes the unload files that come with the server update. When you extract sm9.32.1001_<OS>.zip (or .tar), it will add the files to the following directory:

`[SM Server Root]\platform_unloads ([SM Server Root]/platform_unloads)`

Note: Unload files should be installed in their patch order. That is, those introduced in patch 1 should be applied first, then those introduced in patch 2, and so on. However, unload files introduced in the same patch can be installed in a random order, unless otherwise specified.

Unload File Naming Convention

The unload files use the following naming convention: <CR_ID>_SMxxxPxx_SMxxx.unl, where:

- <CR_ID>: The identification number of the applications defect that the unload file fixes. For example, QCCR1E12345.
- SMxxxPxx: The minimum Service Manager patch level that requires the unload file. For example, SM921P2, which means the unload file comes with the server updates in Service Manager 9.21 patch 2 and should be used for patch 2 or higher.

  Note: Sometimes this portion contains an additional hot fix number, for example, SM711P16HF8. This example means the unload file is intended for Service Manager 7.11 patch 16 Hot Fix 8 or higher.
- SMxxx: The Service Manager applications version that requires the unload file. For example, SM711, which means the unload file is intended only for Service Manager applications version 7.11.

  Note: If the applications version suffix is omitted, the unload file is then intended for all applications versions compatible with the server version, unless otherwise specified. For example, QCCR1Exxxx_SM930P4.unl is normally intended for applications versions 7.11,

9.20, and 9.30 (which are compatible with Service Manager server 9.30), unless otherwise specified in the unload file description. For information on the applicable applications versions for each unload file included in the current patch, see Unload Files Included in the Current Patch.

Unload Files Included in the Current Patch

The following are unload files included in the current patch release.

Unload file	Introduced in 9.3x patch	Used for apps version (s)	Description
QCCR1E31324_SM932.unl	9.32	7.11, 9.21, 9.30 and 9.31	Fixes this issue : With Syslog audit turned on, only a syslog record showing login is created; no record for logoff is recorded if the user does not log out "normally." **Associated server fix**: QCCR1E31324
QCCR1E96802_SM931P3.unl	9.31p3	7.11, 9.21, 9.30 and 9.31	Changes the behavior when handling web service request user passwords. See the SM9.31p3 Release Notes. **Associated server fix**: QCCR1E96802
QCCR1E52767_SM931P3_SM930.unl	9.31p3	9.30	Fixes the issue that users cannot add data policy definitions on joined tables. **Note**: You do not need to load this unload if you are running on SM9.31, 9.21, or 7.11 applications. **Associated server fix**: QCCR1E52767
QCCR1E76724_SM931P2_SM930.unl	9.31p2	9.30 and 9.31	Fixes the issue that after deleting the unique key of cm3r, a signal 11 happened while doing an IR regeneration. **Associated server fix**: QCCR1E76724
QCCR1E76227_SM930P6_SM930.unl	9.31	9.30	Contains the code changes to support localization of incident/change priority and urgency strings for the 9.31 Mobility Client. **Note:** Not needed for the SM9.32 or later Mobility client.

Unload file	Introduced in 9.3x patch	Used for apps version (s)	Description
QCCR1E78794_SM930P6_SM930.unl	9.31	9.30	Removes incident.assignee when a Web Service call specifies the assignee as 'NULL' through the SM9.31 Mobility Client. **Note:** Not needed for the SM9.32 or later Mobility client.
QCCR1E76796_SM930P6_SM930.unl	9.31	9.30	Provides the ability to turn on debugging dynamically for user sessions or schedulers. **Note:** This unload requires the SM9.31 server.
QCCR1E71099_SM930P5_SM711.unl	9.30p5	7.11	Displays Value Lists instead of the data directly retrieved from the database in a QBE list when adding a field by using Modify Columns. **Associated server fix**: QCCR1E71099
QCCR1E71099_SM930P5_SM920.unl	9.30p5	9.20	Displays Value Lists instead of the data directly retrieved from the database in a QBE list when adding a field by using Modify Columns. **Associated server fix**: QCCR1E71099
QCCR1E71099_SM930P5_SM930.unl	9.30p5	9.30	Displays Value Lists instead of the data directly retrieved from the database in a QBE list when adding a field by using Modify Columns. **Associated server fix**: QCCR1E71099
QCCR1E71139_SM930P5_SM930.unl	9.30p5	9.30	Works with server fix QCCR1E71139 to solve this issue: When Service Manager is configured to use LDAP as the authentication data source, the user is still forced to change the password if the user is expired in the local database.

Unload file	Introduced in 9.3x patch	Used for apps version (s)	Description
QCCR1E31941_SM930P4_SM930.unl	9.30P4	9.30	Enables users to use a pre-configured decimal symbol when completing numeric fields. **Note:** This enhancement requires a 9.30p4 or later server; however if you are using RTE version 9.30 with applications version 7.11 or 9.20, do not load this unload file; you can safely upgrade your server to 9.30p4 or later without applying this applications change. **Associated server fix**: QCCR1E31941.
QCCR1E73452_SM930P4.unl	9.30P4	7.11 - 9.30	Enables Mandanten restricting queries to be updated correctly after a profile is edited. **Associated server fix**: QCCR1E71897
QCCR1E67072_SM930P4_SM930.unl	9.30P3	7.11 and 9.20	Enables users to take advantage of the new KMStatusListener background process. **Note:** This unload file is not needed for applications version 9.30 or later, which supports only the Solr Search Engine. **Associated server fix**: QCCR1E67071
QCCR1E70163_SM930P4_SM711.unl	9.30P3	7.11	Fixes the issue that the KMUpdate process terminates abnormally. **Associated server fix**: QCCR1E69687
QCCR1E70163_SM930P4_SM920.unl	9.30P3	9.20	Fixes the issue that the KMUpdate process terminates abnormally. **Associated server fix**: QCCR1E69687
QCCR1E70163_SM930P4_SM930.unl	9.30P3	9.30	Fixes the issue that the KMUpdate process terminates abnormally. **Associated server fix**: QCCR1E69687

Unload file	Introduced in 9.3x patch	Used for apps version (s)	Description
QCCR1E67647_SM930P3.unl	9.30P3	7.11 - 9.30	Updates the exception message that occurs in the request response when closing an interaction by calling CloseInteraction from a web service without specifying the localSolution field in the request. **Associated server fix**: QCCR1E54192
QCCR1E67610_SM930P2.unl	9.30P2	7.11 - 9.30	Enables you to block potentially dangerous attachments. **Associated server fix**: QCCR1E64290

Tip: If your application version is 7.11 ap3, 9.21 ap3, 9.30 ap3, 9.31 or later, you are recommended to use Unload Manager to load an unload file, because Unload Manager can help you create a backup of your old data and reconcile conflicts during the installation of the unload; if your application version is other than any of these, Unload Manager is not available and you can use Database Manager instead.

To load an unload file using Unload Manager:

1. Go to **System Administration** > **Ongoing Maintenance** > **Unload Manager**.
2. Double-click **Apply Unload**. A wizard opens.
3. Select the unload file you want to apply, also specify a backup file, and then click **Next**. Details of the unload file appear.
4. Double-click a conflicting object in the table to open the merge tool:
   a. Merge the object, and then select the **Reconciled** check box.
   b. Click **Save** to go back to the wizard.
5. Click **Next** after all the conflicting objects are reconciled.
6. Click **Yes** on the confirmation window to apply the unload.
7. Click **Finish**.

   Now, the unload has been applied and at the same time your old data backed up.

To load an unload file using Database Manager:

1. Make sure the Windows client is configured for server-side load/unload.
   a. From the Windows client, go to **Window** > **Preferences** > **HP Service Manager**.

   b. Unselect **Client Side Load/Unload** if is flagged.

   c. Restart the Windows client.

2. Open **Tailoring** > **Database Manager**.

3. Right-click the form or open the More Actions menu and select **Import/Load**.

4. Browse to the unload file, and view the contents of an unload file before importing it by clicking **List Contents**.

5. Make a backup copy of all files to be modified by this unload. For detailed steps, see "Backup and Backout Instructions" on page 30.

6. Fill in the following fields.

Field	Description
File Name	Type the name and path of the file to load.
Import Descriptor	Since unload files do not require an Import Descriptor record, leave this field blank.
File Type	Select the source operating system of the unload file.
Messages Option —	
All Messages	Select this option to see all messages that Service Manager generates loading the file.
Messages Option —	
Totals Only	Select this option to see only the total number of files Service Manager loads.
Messages Option — None	Select this option to hide all messages that Service Manager generates when loading the file.

7. Click **Load FG**.

Service Request Catalog (SRC) Installation

This release does not contain any SRC update. The latest SRC package has been shipped with the SM9.32 release.

You can download this package from
http://support.openview.hp.com/selfsolve/document/KM00495894

For installation instructions, see the Service Manager 9.32 Release Notes.

Mobile Applications Installation

This release does not contain any mobile application update. The latest Mobile Application package has been shipped with the SM9.32 release.

You can download this package from
http://support.openview.hp.com/selfsolve/document/KM00495880

For installation instructions, see the Service Manager 9.32 Release Notes.

Knowledge Management (KM) Update Installation

This release does not contain any KM update. The latest KM package has been shipped with the SM9.32 release, which you can download from:

http://support.openview.hp.com/selfsolve/document/KM00495878

For installation instructions, see the Service Manager 9.32 Release Notes.

ODBC Driver Update Installation

This release does not contain any ODBC Driver update. The latest ODBC Driver package has been shipped with the SM9.30p4, SM9.30p5, and SM9.31 releases.

You can download the package from:

http://support.openview.hp.com/selfsolve/document/KM00207925

The ODBC Driver package contains the following updated files:

- Scodbc32.dll
- sci18n.dll
- sccl32.dll

To install the ODBC Driver update:

1. Extract the files to your ODBC Driver installation folder, for example: C:\Program Files\Peregrine Systems\ServiceCenter 6.2\ODBC Driver.

2. When prompted, replace the three old DLL files with the new ones.

Language Pack Installation

This release does not contain any language pack update. The latest language pack packages have been shipped with the SM9.32 release.

Service Manager 9.32 includes language packs for the Service Manager server, for 15 supported languages other than English.

For more information, see the Service Manager 9.32 Release Notes.

Online Help Installation

This release does not contain an updated the version of the online help. The latest online help package has been shipped with the SM9.32 release.

You can download this package from:
http://support.openview.hp.com/selfsolve/document/KM00493466

To install the online help, follow the instructions in the Service Manager 9.30 Interactive Installation Guide, which you can download from:

http://support.openview.hp.com/selfsolve/document/KM1195794

Service Manager Support Matrix and Applications Content Compatibility Matrix

The Support Matrix lists supported versions of operating systems, browsers, HP Software products, and other compatibility and support information.

The Applications Content Compatibility Matrix (named *Compatibility Matrix for Service Manager Applications Content*) provides compatibility information for Service Manager applications content packs (for example, Process Designer Content Packs).

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.

To register for an HP Passport ID, go to HP Passport Registration.

To access the Support Matrix and Applications Content Compatibility Matrix:

1. Use a browser to navigate to the Software Support Online (SSO) web page:

   http://support.openview.hp.com/sc/support_matrices.jsp

2. Log on with your Customer ID and password or your HP Passport sign-in.

3. Navigate to the applicable information.

Appendix. Workaround for QCCR1E99940

Customers who use Solaris 9 cannot upgrade to SM9.31p2 and above patches because JRE7 does not support Solaris 9 and SM starts with a JRE validation, which constraints the JRE version below JRE7 up15.

To work around this issue, modify the `validjava.sh` file under the Service Manager `RUN/` folder as follows:

```
#!/bin/sh

# Command to check for the required Java version for HP Service Manager.
# Copyright 1994-2010 Hewlett-Packard Development Company, L.P.
# All rights reserved.

# Where is the server installed?
RTE_DIR=`dirname $0`
RTE_DIR=`(cd "${RTE_DIR}"; pwd)`

cd "${RTE_DIR}"

# What OS is this?
OS_NAME=`uname -s`

if [ ! -d "${RTE_DIR}/jre/bin" ] ; then
   echo "Java not found."
   echo "Please ensure that ${RTE_DIR}/jre is a link to a valid JRE"
   echo ""
   echo "Exiting..."
   echo ""
   exit 0
else
   JAVA_VERSION_SUPPORTED=0
   JAVA_UPDATE_VERSION_CHECK=0
   if [ ${OS_NAME} = "HP-UX" ]; then
      JAVA_UPDATE_VERSION_SUPPORTED=04
   else
      JAVA_UPDATE_VERSION_SUPPORTED=15     //Modify the number in red to 20
  fi
   JAVA_FULL_VERSION=`${RTE_DIR}/jre/bin/java -version 2>&1 | grep "java ver
sion"|awk '{ print $3 }'`
   JAVA_VERSION=`${RTE_DIR}/jre/bin/java -version 2>&1 | grep "java version"
|awk '{ print $3 }'| cut -c2-4`

   if [ "${JAVA_VERSION}" = "1.7" ]; then  //Modify the number in red to 1.6
      JAVA_VERSION_SUPPORTED=1
```

```
   fi

   if [ ${JAVA_VERSION_SUPPORTED} -eq 1 ]; then
     if [ ${OS_NAME} = "SunOS" -o ${OS_NAME} = "Linux" -o ${OS_NAME} = "HP-U
X" ]; then
       JAVA_UPDATE_VERSION_CHECK=1
       JAVA_UPDATE=`${RTE_DIR}/jre/bin/java -version  2>&1 | grep "java vers
ion"|awk '{ print $3 }'| cut -c8-9`
       if [ ${JAVA_UPDATE} -lt ${JAVA_UPDATE_VERSION_SUPPORTED} ]; then
         JAVA_VERSION_SUPPORTED=0
       fi
    fi
   fi

   if [ ${JAVA_VERSION_SUPPORTED} -eq 0 ]; then
     echo ""
     echo "!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!"
     echo "Unsupported Java version ${JAVA_FULL_VERSION}"
     echo "Please run ./removeLinks.sh to delete all the symbolic links!"
     echo "Install or setup Java 7 correctly and then run ./setupLinks.sh to
re-create the symbolic links."   //Modify the number in red to 6
     if [ ${JAVA_UPDATE_VERSION_CHECK} -eq 1 ]; then
        echo "Make sure you are running Java 7 Update ${JAVA_UPDATE_VERSION_
SUPPORTED} or later."
     fi
     echo "!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!"
     echo ""
     echo "Exiting..."
     echo ""
     exit 0
   fi
fi
exit 1
```


Java™
COMPATIBLE