HP Service Manager

for supported Windows® and UNIX® operating systems

Release Notes

Software version: 9.30.116 Patch 2 / October 3, 2011

This document provides an overview of the changes made to HP Service Manager for 9.30.116, patch 2. It contains important information not included in the manuals or in online help.

Documentation Updates

The first page of this release notes document contains the following identifying information:

- Version number, which indicates the software version.
- Publish date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL: **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.

Note: To view files in PDF format (`*.pdf`), Adobe Acrobat Reader must be installed on your system. To download Adobe Acrobat Reader, go to the following web site:
http://www.adobe.com/.

In This Version

Service Manager Version 9.30, build 116, patch 2 (SM 9.30p2) includes several customer requested software enhancements and fixes. Refer to the sections below for information about the defects, enhancements, and known issues included in this release.

- Enhancements
- Server Updates
- Web Client Updates
- Windows Client Updates
- Known Issues

This patch is cumulative. It includes the enhancements and fixes from all earlier patches to Service Manager 9.30. For information about previous patches, refer to the release documentation (included with this release) for each patch.

Enhancements

The following enhancements are included with this software release.

Global ID	Problem	Solution
QCCR1E64278 QCCR1E64285 QCCR1E64290	Service Manager does not enable you to block executable files from being submitted as attachments.	To prevent potentially dangerous executable files from being submitted as attachments, Service Manager now provides support for blocking certain types of attachments submitted through the Windows and web clients, as well as through web services, based on a pre-defined list of blocked file extensions. At startup, the web tier and the Windows client retrieve the list of blocked file extensions, which is stored in the extensionstate table in the database; if no list is available, the clients use a default list of blocked file types. To take advantage of this enhancement, you must install all of the following: • The Windows client update for this release (QCCR1E64285) • The Web Client update for this release (QCCR1E64278) • The server update for this release (QCCR1E64290), including the supporting application unload file, QCCR1E67610_SM930P2.unl. For more information see Additions to the documentation.
QCCR1E67030	The Service Manager documentation should describe if setting protected domains is necessary for configuring LW-SSO.	Provided information on protecting domains when configuring LW-SSO. For more information see Additions to the documentation.

QCCR1E67744	The Service Manager documentation does not state that when integrating other applications with Service Manager through web services, array data should be broken into multi elements by separator "\r". Failure to do so could cause problems. For example, even if a configuration item (CI) is not changed, Service Manager always updates a change request, since the CI is stored in the Service Manager database as utf-8 while in UCMDB it is encoded as base64.	Provided information on how to prepare array data when integrating other applications with Service Manager through web services. For more information see Additions to the documentation.
QCCR1E67825	We need a way to decompress zip files in JavaScript.	Added a new JavaScript global method, uncompressFile, to provide this capability. This method expands a .zip file into a specified location, using the following syntax: `uncompressFile(file name, target directory);` For more information see Additions to the documentation.
QCCR1E68229	In Process Designer, provide support to directly open rule sets, approvals, and alerts from the workflow editor.	Improved the usability of Process Designer by adding the View icon in the Rule Sets, Approvals, and Alerts tabs of the workflow editor. This gives the Implementer the ability to open rule sets, approvals, or alerts that are defined in a workflow phase without having to exit the workflow editor and doing a search.
QCCR1E68230	In Process Designer, provide the ability to specify localized values for transitions.	Added the Localize Command Label icon to view the scmessage record for a transition. To view the scmessage record of a transition, click a transition of a workflow and click the Localize Command Label icon in the Command Name text box. Add an scmessage record for a new transition, or view the scmessage record of an existing transition.
QCCR1E68231	Provide support for a graphical interface to create, edit, and delete tasks for a Change Model.	Added a new widget to Forms Designer. This widget gives the ability to add the Task Editor graphical interface to add, edit, and delete tasks for a Change Model. Features include pan, zoom, auto layout of tasks, and outline the graph of tasks to view and navigate. **Note:** This functionality will not be available until an upcoming Process Designer Content pack is applied. Complete documentation on the feature will be made available at that time.

Server updates

The following updates are included with this software release.

Global ID	Problem	Solution
QCCR1E32397	During table creation, specified tablespace parameters are not honored.	During table creation, specified tablespace parameters will now be honored.
QCCR1E58163	Service Manager (SM) processes fail during startup if the log parameter refers to an absolute path.	SM processes accept the absolute path for the log parameter and the processes start without any errors.
QCCR1E58648	When Service Manager acts as a web service client, the doSoapRequest method may timeout and generate error messages that are not easily understood by administrators in the server log file (sm.log).	Error or informational messages that are generated in the log as the result of a timeout when performing a doSoapRequest method should now indicate that a timeout has occurred.
QCCR1E59527	In environments deploying a case-sensitive RDBMS in combination with a case-insensitive LDAP server for authentication, users can log in to Service Manager (SM) successfully using a lowercase, uppercase or mixed-case user name. However, if the case of the login name (for example, Susan) does not match the operator name in the LDAP (for example, susan), after login, the System Navigator displays an empty tree and the Todo list displays with no additional queues, which results in an inability to use SM.	Users can use SM properly after logging in successfully with a lowercase, uppercase or mixed-case user name if the LDAP is used for authentication. Without LDAP authentication, the case-sensitivity of login depends on the case-sensitivity setting of the RDBMS. **Note:** To take advantage of this fix, users must also update their client to 9.30p2 or later.
QCCR1E60543	Trying to update a column in a table of the type RAW(255) to any larger size fails with the following error message : • An error occurred while attempting to update a record (record.update,start) • File:(dbdict) key:(name=slo) (record.update,start) • Changing SQL data type from 'RAW(255)' to 'RAW(500)' for column 'CONDITION' in table 'SLOM1' is not supported. Update cancelled. (record.update,start)	For Oracle RDBMS, added support for widening the RAW data type to the maximum size (2000).
QCCR1E63178	The ORA-30556 error occurred when attempting to alert the UPGRECONCILIATION table, which blocked the load transfer on case-insensitive Oracle.	No errors occur when attempting to alter a table on case-insensitive Oracle or case-sensitive Oracle.
QCCR1E65361	Fields in the generated "make-up" dbdict for ADHOC SQL sometimes have an identical index number.	The index numbers are different.
QCCR1E65999	The sm transient process crashes while executing sm -version:999.	The sm transient process will continue while executing sm -version:999.

QCCR1E66003	When the Service Manager Server generates a huge XML document, it may run out of memory and does not catch this exception.	The Service Manager Server now will catch the OutOfMemoryException, write the exception to the server log, and terminate the current client session. **Note:** Memory monitor thread must be disabled (by setting memorypollinterval:0 in the sm.ini file) for this fix to work.
QCCR1E66747	JavaScript system.functions._null causes memory leak in Service Manager.	Initialized the members of LocalRootAddScope with the passed in parameter, so that JavaScript system.functions do not leak memory.
QCCR1E66852	In Linux and Solaris, signal 11 and core dumps might occur at start-up if the system resources were exhausted.	In Linux and Solaris, if the system resources were exhausted, Service Manager process will not run into a signal 11.
QCCR1E66855	RAD function fduplicate sometimes will return an invalid return value, even if it executes successfully when being called in JavaScript.	Changed the behavior so that the RAD function fduplicate will not return an invalid return value when it executes successfully while being called in JavaScript.
QCCR1E66886	A Javacore error occurs when uCMDB pushes data into Service Manager in multi-thread mode.	Changed the default value of the initial Java heap size to 192M. Service Manager will log a warning when the user provides JVMOption heap size min or max greater than 512M.
QCCR1E67101	Service Manager displays a stack trace after the "sm -version" command is run.	Only the version information is displayed when the "sm -version" command is run.
QCCR1E67121	When trying to modify the unique key of a table, the following error occurs, and the indexes are not updated. Error: SQL State: 42S22-1911 Message: [Microsoft][ODBC SQL Server Driver][SQL Server]Column name 'RECORD_KEY' does not exist in the target table.	In this case, a full-table-copy will be performed.
QCCR1E67233	If the backend RDBMS is not started or the wrong ODBC driver is used when executing the command sm -sqlverifyconnection, the console freezes and connection 'retry' information prints infinitely in the server log file (sm.log).	After trying the connection three times and failing to connect to the RDBMS, the failure information will print in the log and the connection command will terminate.
QCCR1E67300	In some horizontal scaling scenarios, new TRClient threads are launched while the parent process is being shut down.	Service Manager processes now shut down cleanly. It no longer creates more TRClient threads while shutting down.

QCCR1E67416	Using a JavaScript call in a conditional RAD expression on a decision panel causes an error message: "Assignment operator found while evaluating a condition!", even when the JavaScript call works properly.	Using a JavaScript call in a conditional RAD expression on a decision panel will no longer cause an error message when the JavaScript call works properly.
QCCR1E68200	The displayed data List is incorrect after using Customize Current View when adding a field.	The displayed data List will be correct when using the Customize Current View whether adding a field, or otherwise.

Web tier updates

The following updates are included with this software release.

Global ID	Problem	Solution
QCCR1E54269	Web client hover form has a scroll bar, but it cannot be used because the hover form moves away from the mouse.	The web client hover form will remain fixed and visible so that the scroll bar can be used.
QCCR1E62847	When viewing a form within the Service Catalog 'Order from Catalog,' a multi-line text box does not align correctly on the Web Tier.	The multi-line text box spans two columns if the label is empty, while keeping a 50/50 split for the text box with a label.
QCCR1E63395	The "Quick Close" and "Submit" buttons are not displayed when a user opens an Employee Self Service (ESS) interaction for the first time with category RFA.	The "Quick Close" and "Submit" buttons are now displayed, as expected, when a user opens an Employee Self Service (ESS) interaction for the first time with category RFA.
QCCR1E63974	Web Tier page display leaves the mouse pointer in a loading state (hour glass or spinning wheel, depending on the browser) until the mouse is moved. This causes users to think the list is still loading when it is not.	The mouse pointer returns to the normal arrow, when the record set or page data is done loading.
QCCR1E64121	Closing the Print window causes the web client to hang.	Closing print window in the web client now returns the user to record as expected.
QCCR1E64480	Pressing the left arrow key returns the cursor to the last position of the field.	Pressing the arrow key now moves the cursor to the expected position.
QCCR1E64621	Two Service Manager tabs can show the [x] close button at the same time.	The ID of the tab element has been fixed so that only one Service Manager tab at a time will have the [x] close button when a tab is being loaded.

QCCR1E64720	The web client does not always prevent a user from performing a Fill against a Read-Only field. If the cursor defaults to a Read-Only field when rendering or displaying a record, the web client will allow a Fill if it is the first action performed on the screen.	Fixed a problem in the web client that enabled users to fill read-only fields in some circumstances.
QCCR1E65123	When performing routine tasks in the web client, the user can be unexpectedly logged out.	The web client has been corrected to protect necessary session information to ensure the session is not terminated unexpectedly.
QCCR1E65890	When performing "Search CIs" from the web client, Service Manager returns the configuration item (CI) list, but the CI details panel remains blank and Service Manager displays the following error: "Java heap space." In addition, Tomcat throws an OutOfMemory error into the log.	The web client no longer experiences a memory error when attempting to display a subview that does not have the "Display Using Table" property correctly configured. Instead, it displays the subview as a separate table.
QCCR1E66005	MySM page receives the following message, "The page cannot be displayed," in every small window using SSL configuration via Cisco ACE NLB.	Changed the way MySM URLs are constructed to maintain protocol/host/port of the original request. This enables the pages to be displayed when using SSL configuration via Cisco ACE NLB.
QCCR1E66150	The cursor does not show the correct position once the web page is refreshed. For example, once the web client prompts an error to a field, the expected result is that the cursor should focus on that field. The focus should be set to the target field after the web page is loaded.	The focus position will be reset after the current web page is refreshed.
QCCR1E66419	Web client appends hard-coded help directory to any help URL.	Added a new parameter (helpServerContext) to solve this issue. For more information see Additions to the documentation.
QCCR1E66683	It is not possible to select a catalog line item by clicking on the group value when the group value is missing.	Empty columns are rendered properly in the table so users can select rows by clicking on an empty column.
QCCR1E66809	In the Workflow Editor, if there is a status message, it overlaps on the workflow canvas and obscures the top of the workflow.	The status message is never shown on the workflow canvas. This is similar to other Service Manager (SM) screens, such as MySM, that never show the status message. **Note:** The messages are still available via the Messages and Alerts button in the toolbar.

QCCR1E67006	The Web Tier infinitely sends the getLanguages SOAP request to the Service Manager server after the session is timed out in a particular environment, which causes the Service Manager server to stop responding.	The user will be re-directed to the log-in page if the session times out. In some environments, this may re-direct to the log-out page instead.
QCCR1E67055	If a status message was present on top of the Workflow Editor canvas and the Condition Editor was opened, the layout of the Condition Editor becomes garbled with the main buttons out-of-place.	The status message no longer appears on the workflow canvas, so the Condition Editor will lay out properly.
QCCR1E67295	If you negate an entire expression by using the Condition Editor, Process Designer does not display the correct user-friendly representation. The outermost “NOT” is missing from the user-friendly representation of the condition. The back-end representation is fine. **Note:** This is only a display problem before saving and reloading, and only affects the outermost expression. Negation displays fine for internal expressions.	The expression “NOT” is correctly appended to the outermost group of the user-friendly representation.
QCCR1E67433	The Spell Checker of HTML Editor widget does not open when you click the "Check Spelling" button.	The Spell Checker of Html Editor now opens when you click the button.
QCCR1E67795	The record list sometimes fails to display in List Detail mode.	The record list always displays in List Detail mode.
QCCR1E68516	JavaScript files remain cached in user's browser, even when the user updates the web application.	Changed the default max-age value of 'Cache-Control' property of 'cacheFilter' bean from 1296000 seconds to 28800 seconds to avoid some cache-caused issues. **Important:** Web user's browser cache will not automatically get refreshed after this value is changed and the web application server is restarted. For this reason, web users may have to manually clear their browser cache before logging in to the updated web client, as the user's cache may contain outdated web resources that are not expired based on the old max-age value.

Windows client updates

The following updates are included with this software release.

Global ID	Problem	Solution
QCCR1E49051	The HTML Editor spell check replaces back slash with a square when correcting misspelled words.	The HTML Editor spell check will now handle the backslash character correctly, and not remove backslashes from the text.
QCCR1E57474	Dynamic view dependency (DVD) does not work when the source is on a tab that comes after an invisible tab in a notebook.	DVD conditions now work properly on a notebook tab that comes after an invisible tab.
QCCR1E60369	The Windows client crashes with error "JVM terminated. Exit code=1073807364." This was caused by a memory leak.	The memory will be released, which will alleviate the errors that caused the crash.
QCCR1E62584	In the Windows client on an Arabic operating system, Arabic strings are displayed from the left side of a field when and after they are entered in the field.	This is a known issue in 9.30p1, which can be solved using the workarounds provided. See also Knowledgebase document #KM223618. In 9.30p2, Arabic strings now display from right to left except when they appear in fields that use the Rich Text Editor. A future patch release may address the issue that occurs with Rich Text Editor fields.
QCCR1E65410	In the Arabic environment, when a user drags a component from left to right by mouse, the component goes to the opposite side. **Note:** The same issue occurs when moving the component using the left/right arrow keys.	Recalculated the component position and size so that mouse movement and use of the left/right arrow keys positions them correctly in the Arabic environment.

Known problems, limitations, and workarounds

This software release has the following known issues.

Global ID	Known Issue	Workaround
QCCR1E28000	If the Equal sign (=) is the first character in an array field, it will be truncated.	No workaround is available at this time.
QCCR1E68803	The help topic "Hardware load balancers" refers to functionality not available in the 9.30 release.	This topic should be removed from the 9.30 help. The functionality may become available in a future release.

Installation Notes

The Arabic language pack requires either the Windows client 9.30P2 or greater (on a supported Windows operating system other than Windows XP) or the Service Manager Web client and Internet Explorer 8.

Web tier installation

The Web Tier update consists of a compressed file, `sm9.30.116-P2_Web_Tier.zip`. The specific upgrade process depends on your particular Web application server, but follows the same steps as deploying a new installation.

The Service Manager Web Tier contains a J2EE-compliant web application that runs on your web application server. Each web application server has its own method of deploying web applications. See your web application server documentation for specific instructions on deploying a web application.

The upgrade does not automatically save your Web Tier customizations. To keep your changes, you must save your customized files and replace the new version of these files with your customized version. For more information, refer to the *Service Manager Interactive Installation Guide*.

Note: For an updated example of deploying the web tier, see Deploying the Service Manager Web Tier on WebSphere Application Server 7, included in this document.

Note: Arabic language support requires Internet Explorer 8.

1. Back up your `web.xml` file, splash screen, style sheets, and any other customizations you made, including your `webtier-9.30.war` (`webtier-ear-9.30.ear`) file.
2. Delete or uninstall the existing `webtier-9.30.war` or `webtier-ear-9.30.ear` file.

   The "Update Application" function in WebSphere application server allows you to redeploy using a new copy of `webtier-9.30.war` (Webtier.ear-9.30.ear). First, update the `web.xml` in the `webtier-9.30.war` (`.ear`) file, and then redo the shared library configuration. For more information, see the IBM WebSphere documentation.
3. Deploy the new `webtier-9.30.war` (`.ear`) file by following the instructions in the Service Manager Installation Guide.

   Note: HP recommends that you deploy with a unique context root, for example /webtier-9.30.116.
4. Replace the new versions of any files you customized with your customized versions.
5. Make any new customizations necessary for your deployment.
6. Restart the Application server.
   Note: Before accessing the new Web Tier, HP recommends that all users empty their browser cache.

Windows client installation

The Windows client update consists of a compressed file, `sm9.30.116-P2_Windows_Client.zip`, which contains the executable installation files.

To install the Windows client update:

1. Stop the Service Manager Windows client.
2. Uninstall the Service Manager Windows client. (Your connection and personalized settings are retained.)

3 Run `setup.exe` and install the client by following the instructions in the Service Manager Installation guide and Release Notes for your version.

4 Check the version in **Help > About Service Manager Client**.
The client should be Release: 9.30.116.

Server installation

The server update for your operating system (OS) consists of a compressed file, `sm9.30.116-P2_<OS>.zip` (or `.tar`), which contains the Service Manager server files. These files add to or replace the files in the `[SM Root]\` (`[SM Root]/`) `RUN`, `irlang`, `legacyintegration`, and `platform_unloads` directories.

To install the Server update:

1 Stop all Service Manager clients.

2 Stop the Service Manager server.

3 Make a backup of the RUN directory.

4 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`.

5 For UNIX servers, set the file permissions for all Service Manager files to 755.

6 Restart the Service Manager server.

7 Restart the Service Manager clients.

8 Check the version in **Help > About Service Manager Server**.
The server should be Release: 9.30.116.

Application unload installation

The application consists of the unload files that come with the server update. When you extract `sm9.30.116-P2_<OS>.zip` (or `.tar`), it will add the new files to your `[SM Root]\platform_unloads` (`[SM Root]/platform_unloads`) directory.

To install the new applications load the following unload file, `QCCR1E67610_SM930P2.unl`, which enables you to block potentially dangerous attachments.

To load an unload file:

1 Select either client or server-side unload, depending on the location of the unload files.

  a From the Windows client, go to **Window > Preference > HP Service Manager**.

  b Flag **Client-Side Load/Unload** if the files are on the client machine, and clear the flag if they are on the server.

  c Restart the Windows client if you changed the setting.

2 Open **Tailoring > Database Manager**.

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

4 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.

Note: You can view the contents of an unload file before importing it by clicking **List Contents**.

5. Click **Load FG**.

Additions to the Documentation

The following information supports updates included in this patch.

- Setting protected domains when configuring LW-SSO
- Blocking attachments with certain file extensions
- Deploying the Service Manager web tier on WebSphere Application Server 7
- Help connection parameters
- Preparing array data when integrating other applications with Service Manager through web services
- JavaScript global method: uncompressFile

Setting protected domains when configuring LW-SSO

The following documentation explains how to set protected domains when configuring LW-SSO.

Note: For related information, such as using LW-SSO with integrations, see the online Help.

Configure LW-SSO in the Service Manager web tier

User role: System Administrator

If Lightweight Single Sign-On (LW-SSO) is enabled in the Service Manager Web tier, integrations from other HP products will bypass Service Manager authentication when launching the Service Manager Web client, provided that the HP product user is already authenticated and a proper token is used.

To enable users to launch the Web client from another HP product using LW-SSO, you must also enable LW-SSO in the Service Manager server.

Once you have enabled LW-SSO in the web tier, web client users should use the web tier server's fully-qualified domain name (FQDN) in the login URL:
`http://<myWebtierHostName>.<myDomain>:<port>/webtier-9.30/index.do.`

The following procedure example, assumes that the Service Manager Web tier is deployed on Tomcat.

To configure LW-SSO in the Service Manager Web tier:

1. Open the `<Tomcat>\webapps\< Service Manager Web tier>\WEB-INF\web.xml` file in a text editor.
2. Modify the `web.xml` file as follows:
   a. Set the <serverHost> parameter to the fully-qualified domain name of the Service Manager server.

      Note: This is required to enable LW-SSO from the web tier to the server.

   b. Set the <serverPort> parameter to the communications port of the Service Manager server.
   c. Set the <secureLogin> and <sslPort> parameters. For example, set the secureLogin parameter to true (default) and sslPort to the SSL port of the web application server.

      To use secure login, you must enable SSL on your web application server. For details, refer to your web application server documentation.

      Note: HP recommends that you do not disable secure login. For more information, refer to the online help for the “Web parameter: secureLogin" and "Web parameter: sslPort”.

   d. Change the value of context parameter “isCustomAuthenticationUsed” to false.

e Remove the comment tags (**`<!-- and -->`**) enclosing the following elements to enable LW-SSO authentication.

```
<!--
  <filter>
    <filter-name>LWSSO</filter-name>
    <filter-class>com.hp.sw.bto.ast.security.lwsso.LWSSOFilter</filter-class>
  </filter>
-->
......
<!--
  <filter-mapping>
    <filter-name>LWSSO</filter-name>
    <url-pattern>/*</url-pattern>
  </filter-mapping>
-->
```

f Save the `web.xml` file.

3 Open the `<Tomcat>\webapps\<Service Manager Web tier>\WEB-INF\classes\lwssofmconf.xml` file in a text editor.

4 Modify the lwssofmconf.xml file as follows:

a Set the value of “enableLWSSOFramework” to true (default is false).

b Set the <domain> parameter to the domain name of the server where you deploy your Service Manager Web tier. For example, if your Web tier's fully qualified domain name is mywebtier.domain.hp.com, then the domain portion is domain.hp.com.

c Set the <initString> value to the password used to connect HP applications through LW-SSO (minimum length: 12 characters). For example, smintegrationlwsso. Make sure that other HP applications (for example, Release Control) connecting to Service Manager through LW-SSO share the same password in their LW-SSO configurations.

d In the <multiDomain> element, set the trusted hosts connecting through LW-SSO. If the Service Manager web tier server and other application servers connecting through LW-SSO are in the same domain, you can ignore the <multiDomain> element ; If the servers are in multiple domains, for each server, you must set the correct DNSDomain (domain name), NetBiosName (server name), IP (IP address), and FQDN (fully-qualified domain name) values. The following is an example.

```
<DNSDomain>example.com</DNSDomain>
<NetBiosName>myserver</NetBiosName>
<IP>1.23.456.789</IP>
<FQDN>myserver.example.com</FQDN>
```

Note: Service Manager 9.30p2 uses <multiDomain> instead of <protectedDomains>, used in earlier versions. The multi-domain functionality is relevant only for UI LW-SSO (not for web services LW-SSO). This functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL in a browser window, except when both applications are in the same domain.

Example lwssofmconf.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwsso/2.0">
  <enableLWSSO
    enableLWSSOFramework="true"
    enableCookieCreation="true"
    cookieCreationType="LWSSO"/>
  <webui>
        <validation>
          <in-ui-lwsso>
        <lwssoValidation id="ID000001">
```

```
         <domain>example.com</domain>
          <crypto cipherType="symmetricBlockCipher"
            engineName="AES" paddingModeName="CBC" keySize="256"
            encodingMode="Base64Url"
            initString="This is a shared secret passphrase"/>
        </lwssoValidation>
          </in-ui-lwsso>
          <validationPoint
        enabled="false"
        refid="ID000001"
        authenicationPointServer="http://server1.example.com:8080/bsf"/>
        </validation>
        <creation>
          <lwssoCreationRef>
        <lwssoValidationRef refid="ID000001"/>
        <expirationPeriod>50</expirationPeriod>
          </lwssoCreationRef>
        </creation>
        <logoutURLs>
          <url>.*/goodbye.jsp.*</url>
        </logoutURLs>
        <nonsecureURLs>
          <url>.*/sso_timeout.jsp.*</url>
        </nonsecureURLs>
        <multiDomain>
          <trustedHosts>
         <DNSDomain>example.com</DNSDomain>
         <DNSDomain>example1.com</DNSDomain>
         <NetBiosName>myserver</NetBiosName>
         <NetBiosName>myserver1</NetBiosName>
         <IP>102.102.102.102</IP>
         <IP>102.102.102.102</IP>
         <FQDN>myserver.example.com</FQDN>
         <FQDN>myserver1.example1.com</FQDN>
          </trustedHosts>
       </multiDomain>
  </webui>
      <lwsso-plugin type="Acegi">
        <roleIntegration
          rolePrefix="ROLE_"
          fromLWSSO2Plugin="external"
          fromPlugin2LWSSO="enabled"
          caseConversion="upperCase"/>
        <groupIntegration
          groupPrefix=""
          fromLWSSO2Plugin="external"
          fromPlugin2LWSSO="enabled"
          caseConversion="upperCase"/>
      </lwsso-plugin>
</lwsso-config>
```

e Save the lwssofmconf.xml file.

5 Open the `<Tomcat>\webapps\<Service Manager Web tier>\WEB-INF\classes\application-context.xml` in a text editor.

6 Modify the `application-context.xml` as follows:

a Add lwSsoFilter to filterChainProxy:

```
/**=httpSessionContextIntegrationFilter,lwSsoFilter,anonymousProcessingFilter
```

Note: If you need to enable web tier LW-SSO for integrations and also enable trusted sign-on for your web client users, add lwSsoFilter followed by preAuthenticationFilter, as shown in the following:

```
/**=httpSessionContextIntegrationFilter,lwSsoFilter,preAuthenticationFilter,anonymousProcessingFil
    ter
```

For information about how to enable trusted sign-on in Service Manager, see Example: Enabling trusted sign-on.

b Uncomment bean lwSsoFilter:

```
<bean id="lwSsoFilter" class="com.hp.ov.sm.client.webtier.lwsso.LwSsoPreAuthenticationFilter">
```

c Save the application-context.xml file.

7 Repack the updated Service Manager web tier files and replace the old web tier .war file deployed in the <Tomcat>\webapps folder.

8 Restart Tomcat so that the configuration takes effect.

Blocking attachments with certain file extensions

To prevent potentially dangerous executable files from being submitted as attachments, Service Manager now provides support for blocking certain types of attachments submitted through the Windows and web clients, as well as through web services, based on a pre-defined list of blocked file extensions. At startup, the Windows and web clients retrieve the list of blocked file extensions, which is stored in the `extensionstate` table in the database. If no list is available, the clients use a default list. (For more information, see Default list of blocked file extensions.)

To take advantage of this enhancement, you must install all of the following:

- The Windows client update for this release (QCCR1E64285)
- The Web Client update for this release (QCCR1E64278)
- The server update for this release (QCCR1E64290), including the supporting application unload file, QCCR1E67610_SM930P2.unl.

System Administrators can add, delete, and update records in the `extensionstate` table to customize the list of blocked file extensions. (For more information, see Customize the list of blocked file extensions.)

If a search engine is installed and connected to the system, System Administrators must also update the sclib knowledgebase records, to include .unsafe to the list of file extensions that should be skipped for indexing. (For more information, see Add .unsafe to the list of file extensions to skip for knowledgebase indexing.)

Note: When your customization is complete, you must restart the web tier's web application server (for example, Tomcat, WebSphere) or restart the Windows client for the changes to take effect.

With these enhancements, Service Manager blocks the attachments in the following ways:

- When users attempt to attach a file whose extension is in the list of blocked file extensions to a record, the clients disallow attaching the file and display the following error message: "File type: <filetype>, is not allowed as an attachment."
- If the clients retrieve an existing attachment whose extension is included in the list of blocked file extensions, the clients append ".UNSAFE" to the file name to prevent the file from being automatically 'run' on the user's machine.
- During web services processing, if a transaction submits or retrieves a file as an attachment whose extension is included in the list of blocked file extensions, the server appends ".UNSAFE" to the submitted or retrieved file name.

Customize the list of blocked file extensions

User Role: System Administrator

You can add or remove files from the list of blocked file extensions based on the needs of your company.

To view and customize the list of blocked file extensions:

1. Open **System Administration > Base System Configuration > Miscellaneous > File Extensions**.
2. Click **Search**.
   A list of file extension records displays.
3. To add a new record:
   a. Open an existing record.
   b. Update the fields as follows:
      - **File Extension:** Type an extension without the dot character (.) For example, type "`bat`" rather than ".bat".
      - **Unsafe:** Check this box to block attachments with this file extension or uncheck this box to unblock them.
      - **File Type:** Type a description of this file type.

   c. Click **Add**.
      The new file extension is added to the list.
4. To update an existing record:
   a. Select the record from the list.
   b. Check or uncheck the **Unsafe** check box.
   c. Click **Save** to save the record.
5. To delete a record:
   a. Select the record from the list.
   b. Click **Delete**.
   c. Click **Yes** to confirm the deletion.
      The record is removed from the list.
6. Do the following for the changes to take effect:
   - **Windows client:** Log out and exit the client and then restart it.
   - **Web client:** Restart the web application server.

Add .unsafe to the list of file extensions to skip for knowledgebase indexing

User Role: System Administrator

To prevent Service Manager from indexing unsafe attachments for knowledgebase searches, add **`.unsafe`** to the list of file extensions that should not be indexed or extracted. To do this, updating the following sclib type knowledgebases: Incident_Library, Interaction_Library, Knowledge_Library, Knownerror_Library, and Problem_Library.

Note: This task requires that you have a search engine installed and correctly configured.

To update the knowledgebases:

1. Open **Knowledge Management > Configuration > Knowledgebases**.
2. Click **Search**.

A list of records displays: Incident_Library, Interaction_Library, Knowledge_Library, Knownerror_Library, and Problem_Library.

3 Select a record in the list, and open the **Type information** tab.

4 In the **Skip these extensions** field, add .unsafe to the existing file extension list, using a semi-colon as the separator. For example, type: `jpg;bmp;gif;exe;unl;unsafe.`

5 Click **Save**.

6 For the other records in the record list, repeat steps 3 through 5.

After you complete this, the files you indicated will be blocked from being submitted as attachments.

Default list of block file extensions

Service Manager blocks attachments whose file name extensions are included in a list of files retrieved from the database. If such a list is not available from the database, Service Manager blocks attachments with the file name extensions listed in the following table.

File Name Extension	Description
.ade	Access Project Extension (Microsoft)
.adp	Access Project (Microsoft)
.app	Executable Application
.asp	Active Server Page
.bas	Active Server Page
.bat	Batch Processing
.cer	Internet Security Certificate File
.chm	Compiled HTML Help
.cmd	DOS CP/M Command File, Command File for Windows NT
.com	Command
.cpl	Windows Control Panel Extension (Microsoft)
.crt	Certificate File
.csh	csh Script
.der	DER Encoded X509 Certificate File
.exe	Executable File
.fxp	FoxPro Compiled Source (Microsoft)
.gadget	Windows Vista gadget
.hlp	Windows Help File
.hta	Hypertext Application
.inf	Hypertext Application
.ins	IIS Internet Communications Settings (Microsoft)
.isp	IIS Internet Service Provider Settings (Microsoft)

.its	Internet Document Set, Internet Translation
.js	JavaScript Source Code
.jse	JScript Encoded Script File
.ksh	UNIX Shell Script
.lnk	Windows Shortcut File
.mad	Access Module Shortcut (Microsoft)
.maf	Access (Microsoft)
.mag	Access Diagram Shortcut (Microsoft)
.mam	Access Macro Shortcut (Microsoft)
.maq	Access Query Shortcut (Microsoft)
.mar	Access Report Shortcut (Microsoft)
.mas	Access Stored Procedures (Microsoft)
.mat	Access Table Shortcut (Microsoft)
.mau	Media Attachment Unit
.mav	Access View Shortcut (Microsoft)
.maw	Access Data Access Page (Microsoft)
.mda	Access Add-in (Microsoft), MDA Access 2 Workgroup (Microsoft)
.mdb	Access Application (Microsoft), MDB Access Database (Microsoft)
.mde	Access MDE Database File (Microsoft)
.mdt	Access Add-in Data (Microsoft)
.mdw	Access Workgroup Information (Microsoft)
.mdz	Access Wizard Template (Microsoft)
.msc	Microsoft Management Console Snap-in Control File (Microsoft)
.msh	Microsoft Shell
.msh1	Microsoft Shell
.msh2	Microsoft Shell
.mshxml	Microsoft Shell
.msh1xml	Microsoft Shell
.msh2xml	Microsoft Shell
.msi	Windows Installer File (Microsoft)
.msp	Windows Installer Update
.mst	Windows SDK Setup Transform Script
.ops	Office Profile Settings File
.pcd	Visual Test (Microsoft)

.pif	Windows Program Information File (Microsoft)
.plg	Developer Studio Build Log
.prf	Windows System File
.prg	Program File
.pst	MS Exchange Address Book File, Outlook Personal Folder File (Microsoft)
.reg	Registration Information/Key for W95/98, Registry Data File
.scf	Windows Explorer Command
.scr	Windows Screen Saver
.sct	Windows Script Component, Foxpro Screen (Microsoft)
.shb	Windows Shortcut into a Document
.shs	Shell Scrap Object File
.ps1	Windows PowerShell
.ps1xml	Windows PowerShell
.ps2	Windows PowerShell
.ps2xml	Windows PowerShell
.psc1	Windows PowerShell
.psc2	Windows PowerShell
.tmp	Temporary File/Folder
.url	Internet Location
.vb	VBScript File or Any VisualBasic Source
.vbe	VBScript Script File, Visual Basic for Applications Script
.vbs	VBScript Script File, Visual Basic for Applications Script
.vsmacros	Visual Studio .NET Binary-based Macro Project (Microsoft)
.vsw	Visio Workspace File (Microsoft)
.ws	Windows Script File
.wsc	Windows Script Component
.wsf	Windows Script File
.wsh	Windows Script Host Settings File
.xnk	Exchange Public Folder Shortcut

Deploying the Service Manager web tier on WebSphere Application Server 7

HP recommends that you deploy with a unique context root, for example /webtier-<version>.<buildNumber>

Example deployment on WebSphere application server:

1 Log in to the server as a user with local administrator privileges.

2 Insert the Service Manager installation DVD into the appropriate drive of the server.

3 Access the .ear file, by navigating to the \Webtier directory on the installation media.

4 Copy or save the `webtier-ear-9.30.ear` file onto your local system.

5 The `webtier-ear-9.30.ear` file contains `webtier-9.30.war`. Inside of that is the `web.xml` file. Extract `web.xml` and edit it to add your server connection information.

The settings you define in `web.xml` determine the client preferences for all web clients. View the Service Manager online help for a complete list and more detailed explanation of each parameter.

a Set the required parameters: serverHost, serverPort secureLogin, and sslPort.

Parameter	**Default value**	**Description**
serverHost	localhost	Specifies the name of the Service Manager host server.
serverPort	13080	Specifies the communications port number to which the Service Manager server listens.
secureLogin	true	Controls the encryption of network communication between the web application server and the web browser. Set it to false if you do not use Secure Sockets Layer (SSL) connections to the web server. Note: To use secure login, you must enable SSL on your web application server. For details, refer to your web application server documentation. Note: HP recommends that you use secure login.
sslPort	8443	This parameter is needed only when secureLogin is set to true. Set it to the SSL port of the web application server.

b Set other parameters as desired. The table below lists the commonly set parameters and their default values.

Parameter	**Default value**	**Description**
cacerts	WEB-INF	Lists the path to the CA certificates required for SSL support.
compress_soap	false	Specifies if you want to use data compression between web clients and the web tier.
helpServerHost	localhost	Specifies the name of the Help Server.
helpServerPort	80	Specifies the communications port number to which the Help Server listens.

helpServerContext	help	This parameter defines the context path when deploying the Service Manager help on a web server (for example, Apache). The context path refers to the virtual directory name where the Service Manager help is installed. For more information, see Web Client Parameter: helpServerContext.
refreshMessages	false	Determines whether the browser checks for new messages from the application server.
refreshMessagesInterval	15000	Determines how often (in milliseconds) the browser checks for new messages from the application server.
ssl	false	Enables the web client to encrypt communications using the server's demonstration certificate.
viewactivenotes	false	Determines whether you see a pop-up message when the server sends a message.

c Save, close and re-archive the files.

Note: Keep the original filenames and folder structure when re-archiving.

6 Start the WebSphere application server.

7 Set the web application server heap size. The web application server heap size determines how many connections each web application server can handle. Most application servers require a heap size of at least 256 MB for optimal performance. If you experience poor performance from your web client connections, increase the web application server heap size. See your web application server documentation for instructions.

8 Log on to the WebSphere administrative console with system administrator privileges.

9 Install the `webtier-ear-9.30.ear` file.

a Open **Applications > New Application > New Enterprise Application**.

b Select "**Local file system**", and browse to the `webtier-ear-9.30.ear` file.

c Click **Next**. The file uploading starts. This may take quite a while.

10 Click **Next** on each screen to accept the default settings until you reach "Step 4: Summary", and then click **Finish**. The installation of the web tier ear file begins.

11 When the installation is successfully completed, click **Save** to save your local configuration changes to the master configuration.

12 Configure the Application's properties.

a Open **Applications > Application Types > WebSphere enterprise applications**.

b Click **HP Service Manager 9.30 Web** and click **Start**. When the application has started, its state changes to green.

c Under **Detail Properties**, click **Class loading and update detection**, and make the following selections:

— **Class loader order**: Classes loaded with local class loader first (parent last)

— **WAR class loader policy**: Single class loader for application

d Click **Apply**.

13 Configure the HP Service Manager module.

a Open **Applications > Application Types > WebSphere enterprise applications > HP Service Manager 9.30 Web > Manage Modules**.

b Click the **HP Service Manager** module and make the following selection:

Class loader order: `Classes loaded with parent class loader first`

Note: Keep the other default settings.

c Click **Apply**.

14 Configure the default http transport port of the WebSphere application server. You will use this port when launching the Service Manager web client.

a Go to **WebSphere application servers > server 1**.

b In the **Communications > Ports** section, make note of the **WC_defaulthost** port number (for example, 9082).

Note: You can change this port number to another one that is not in use. This port number is automatically synchronized to the port number used in **Application servers > server1 > Web container transport chains > HttpQueueInboundDefault**.

c Open **Environments > Virtual Hosts > default_host > Host Aliases**, and make sure that the **WC_defaulthost** port number is in the Host Aliases list. If it is not, do the following to add the port number to the list.

1. Click **New**.
2. Type the following port information:
   Host Name:*
   Port:xxxx (for example, 9085)
3. Click **Apply**, and then click **OK**. The port number is added to the Host Aliases list of default_host.

d Click **Save** to save the changes to the master configuration.

e Restart the WebSphere application server. Now the server will start binding to the new port.

Note: If you didn't change the port number, you do not need to restart the server.

15 Go to **Applications > Applications Type > WebSphere enterprise applications**, select **HP Service Manager 9.30 Web**, and click **Start**.
When the application is successfully started, its state changes to green.

16 Launch the Service Manager web client using a URL like this one:
`http://<WAS application server name>:<Port>/webtier-9.30/index.do`, where <Port> is the WC_defaulthost port number you configured previously.

Example: `http://abc.def.hp.net:9085/webtier-9.30/index.do`.

Note: Before accessing the new Web Tier, HP recommends that all users empty their browser cache.

Help connection parameters

The following parameters enable you to connect to the help from the Service Manager client.

Web Client Parameter: helpServerContext

To connect the help from the Web client:

1. Open the Web tier configuration file (`web.xml`) in a text editor.
2. Specify the following parameters:
   helpServerHost: The host name of the Help Server
   helpServerPort: The communications port of the Help Server
3. If your Help Server is not deployed in the default "/help" folder (for example: C:/Apache/2.2/htdocs/help), specify the Help Server context path (either empty or not) by adding the helpServerContext parameter in the `web.xml`. The following are two examples:

   ```
   <init-param>
   <param-name>helpServerContext</param-name>
   <param-value/>
   </init-param/>
   ```

   Or

   ```
   <init-param>
   <param-name>helpServerContext</param-name>
   <param-value>sm/9.30_help</param-value>
   </init-param>
   ```
4. In the `web.xml` file, make sure that the **showHelp** parameter value is set to true.
5. Restart the web application server.
6. Click the Help (question mark) button in the web client tooltray to launch the Help Server. Service Manager will automatically launch the Help Server URL:
   `http://<helpServerHost>:<helpServerPort>/<helpServerContext>`

Preparing array data when integrating applications with Service Manager through web services

When integrating other applications with Service Manager, array data should be broken into multi elements by separator "\r". This is because Service Manager uses "\r" as the separator between array elements. When a string that contains "\r" is retrieved from the Service Manager system, it is decoded as an array with multi elements separated by "\r". For this reason, when integrating other applications (for example, UCMDB) with Service Manager through web services, array data should be broken into multi elements by separator "\r" before the data is encoded and sent to the Service Manage system.

For example, if an array contains elements "aabb" and "ccdd", it should be sent to Service Manager as the following:

```
<ns:Comments type=\"Array\">
  <ns:Comments mandatory=\"\" readonly=\"\">aabb</ns:Comments>
  <ns:Comments mandatory=\"\" readonly=\"\">ccdd</ns:Comments>
</ns:Comments>
```

JavaScript global method: uncompressFile

This method expands a .zip file into a specified location.

Syntax

uncompressFile(file name, target directory);

Parameters

The following arguments are valid for this function:

Argument	**Data Type**	**Required**	**Description**
file name	String	Yes	This argument specifies the name of the file to uncompress.
target directory	String	No	This argument specifies the target directory. If not specified, the default is to use the location of the compressed file.

Return values

True indicates that the file uncompressed successfully, any other return value indicates failure.

Example

This example unzips the file upgtest.zip to c:/test.

```
var rc = uncompressFile("c:/test/upgtest.zip");
if( rc == true )
{
  print("uncompress file with one file successfully");
 // this will unzip the file to C:/test/test
  rc = uncompressFile("c:/test/upgtest.zip", "c:/test/test");
}
else
{
  print("Failed to uncompress file.");
}

if(rc == true)
{
  print("All tasks are finished.");
}
```

Verified Environments

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

To access the 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.

Local Language Support

UTF-8 is part of the Unicode standard, which enables you to encode text in practically any script and language. Service Manager 9.30 supports UTF-8 as an encoding method for new or existing data. It can support multiple languages that adhere to the Unicode standard on the same server.

Support

You can visit the HP Software support web site at:
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 software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support 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 an active support contract. To find more information about support access levels, go to the following URL: **http://h20230.www2.hp.com/new_access_levels.jsp**.

To register for an HP Passport ID, go to the following URL:
http://h20229.www2.hp.com/passport-registration.html.

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.
- Java is a registered trademark of Oracle and/or its affiliates.
- Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.
- UNIX® is a registered trademark of The Open Group.

For a complete list of open source and third party acknowledgements, visit the HP Software Support Online web site and search for the product manual called HP Service Manager Open Source and Third Party License Agreements.