HP Service Manager

For the supported Windows and Unix systems

Software Version: 7.11

Patch 20 Release Notes

Document Release Date: April 2013

Software Release Date: February 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.

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.

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

This document is an overview of the changes made to HP Service Manager 7.11 for patch 20. It contains important information that is not included in other documentation.

What's New in This Release

This section describes important changes in this release.

Server Embedded Tomcat Upgraded

The SM server's embedded Tomcat has been upgraded to the latest 6.x version (6.0.36) to take advantage of its security updates.

Notes:

After applying the server patch, if you need to roll back, be sure to restore your old embedded Tomcat. See "Backout Instructions" on page 46.

This upgrade requires additional steps when installing the server patch. For details, see "Server Update Installation" on page 49.

LW-SSO Update (Server and Web Tier)

Starting with this release, the SM 7.11 server supports LW-SSO. The lwssofmconf.xml configuration file has been added to the server's RUN folder, and the LW-SSO version is currently 2.5.

Starting with this release, the SM7.11 Web tier has been upgraded to LW-SSO version 2.5. The Web tier's lwssofmconf.xml file has introduced a new parameter, secureHTTPCookie. The default is "true". This parameter must be set in combination with the secureLogin parameter in the Web tier configuration file (web.xml) so that LW-SSO can work correctly:

- If secureHTTPCookie is set to true, secureLogin must also be set to true;
- If secureHTTPCookie is set to false, secureLogin can be set to true or false as needed (you are recommended to set both to true in a production environment).

For detailed LW-SSO configuration steps, see "Configure LW-SSO in the Service Manager server" below and "Configure LW-SSO in the Service Manager Web tier" on page 9.

Configure LW-SSO in the Service Manager server

Starting with SM7.11p20, the SM server supports Lightweight Single Sign-On (LW-SSO). A Service Manager integration can pass an authentication token to Service Manager and does not require re-authentication. This simplifies the configuration of Single Sign-On for HP solutions by removing the need to use Symphony Adapter (which proxies LW-SSO-based authentication with the Service Manager Trusted Sign-On solution).

Enabling LW-SSO in the Service Manager server enables web service integrations from other HP products (for example, Release Control) to bypass Service Manager authentication if the product user is already authenticated and a proper token is used; enabling LW-SSO in both the Service Manager server and web tier enables users to bypass the login prompts when launching the Service Manager web client from other HP applications.

Note: Existing integrations that use the Symphony Adapter and Trusted Sign-On rather than this new LW-SSO mechanism can continue to work.

To configure LW-SSO in the Service Manager server:

1. Go to the <Service Manager server installation path>/RUN folder, and open `lwssofmconf.xml` in a text editor.
2. Make sure that the `enableLWSSOFramework` attribute is set to `true` (default).
3. Change the domain value `example.com` to the domain name of your Service Manager server host.

   Note: To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application (for example, HP Enterprise Collaboration) to the web tier can log in but may be forcibly logged out after a while.
4. Set the `initString` value. This value MUST be the same with the LW-SSO setting of the other HP product you want to integrate with Service Manager.

Notes:

- LW-SSO version 2.5 is supported.
- Optionally, you can change attributes `paddingModeName`, `keySize`, `encodingMode`, `engineName`, and `cipherType`. However, you must make sure that they are same with the LW-SSO setting of the other HP product that you want to integrate with Service Manager.
- Do not change the other configurations, such as the content in tag `<restURLs>`, and the attribute of tag `<service>`.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config xmlns="http://www.hp.com/astsecurity/idmenablmentfw/lwss
o/2.0">
  <enableLWSSO enableLWSSOFramework="true"
   enableCookieCreation="true" cookieCreationType="LWSSO" />
    <web-service>
       <inbound>
         <restURLs>
               <url>.*7/ws.*</url>
               <url>.*sc62server/ws.*</url>
               <url>.*/ui.*</url>
         </restURLs>
         <service service-type="rest" >
           <in-lwsso>
               <lwssoValidation>
                 <domain>example.com</domain>
                <crypto cipherType="symmetricBlockCipher" engineName="AES"
```

```
                    paddingModeName="CBC" keySize="256" encodingMode="Base64Url"
                    initString="This is a shared secret passphrase"</crypto>
                </lwssoValidation>
            </in-lwsso>
          </service>
        </inbound>
        <outbound/>
    </web-service>
</lwsso-config>
```

Configure LW-SSO in the Service Manager Web tier

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.

Notes:

- 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-x.xx/index.do

The following procedure is provided as an example, assuming 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 Tomcat.

      Note: HP recommends that you not disable secure login.

   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.

      Note: To use LW-SSO, your Service Manager web tier and server must be deployed in the same domain; therefore you should use the same domain name for the web tier and server. If you fail to do so, users who log in from another application (for example, HP Enterprise Collaboration) to the web tier can log in but may be forcibly logged out after a while.
   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 now uses <multiDomain> instead of <protectedDomains>. 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.

e. Check the **secureHTTPCookie** value (default: true). If you set secureHTTPCookie to true (default), you must also set secureLogin in the web.xml file to true (default); if you set secureHTTPCookie to false, you can set secureLogin to either true or false. In a production environment, you are recommended to set both parameters to true.

Here is an example of `lwssofmconf.xml`:

```
<?xml version="1.0" encoding="UTF-8"?>
<lwsso-config xmlns="http://www.hp.com/astsecurity/idmenablmentf
w/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="25
6"
                    encodingMode="Base64Url"
                    initString="This is a shared secret passphrase"/>
                </lwssoValidation>
              </in-ui-lwsso>

              <validationPoint
                enabled="false"
                refid="ID000001"
                authenicationPointServer="http://server1.example.com:80
80/bsf"/>

            </validation>

            <creation>
              <lwssoCreationRef useHTTPOnly="true" secureHTTPCookie="tr
ue">
                <lwssoValidationRef refid="ID000001"/>
                <expirationPeriod>50</expirationPeriod>
              </lwssoCreationRef>
            </creation>

            <logoutURLs>
                <url>.*/goodbye.jsp.*</url>
                <url>.*/cwc/logoutcleanup.jsp.*</url>
            </logoutURLs>

            <nonsecureURLs>
```

```
                    <url>.*/images/.*</url>
                    <url>.*/js/.*</url>
                    <url>.*/css/.*</url>
                    <url>.*/cwc/tree/.*</url>
                    <url>.*/sso_timeout.jsp.*</url>
                </nonsecureURLs>

                <multiDomain>
                   <trustedHosts>
                      <DNSDomain>example.com</DNSDomain>
                      <DNSDomain>example1.com</DNSDomain>
                      <NetBiosName>myserver</NetBiosName>
                      <NetBiosName>myserver1</NetBiosName>

                      <IP>xxx.xxx.xxx.xxx</IP>
                      <IP>xxx.xxx.xxx.xxx</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>
```

f. 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,anonymousProcessingFilter
```

For information about how to enable trusted sign-on in Service Manager, see the online help.

b. Uncomment bean lwSsoFilter:

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

c. Save the application-context.xml file.

7. Redeploy the updated Service Manager web tier .war file in the <Tomcat>\webapps folder.
8. Restart Tomcat so that the configuration takes effect.

Special Configuration for WebSphere 7 on Solaris

This release adds support of IBM WebSphere Application Server 7 for the Web client. For Solaris, you are recommended to update to WAS 7.0.0.25，to avoid some issues. In addition, for WAS 7 running on Solaris, the following special configuration is required:

1. Add a JVM parameter.

   Navigate to **Application servers** > ***<server name>*** > **Process definition** > **Java Virtual Machine**, and enter the following line in the Generic JVM arguments field:

   ```
   -Dsun.lang.ClassLoader.allowArraySyntax=true
   ```

2. Change the class loader order & policy.

   Navigate to **Enterprise Applications** > **HP Service Manager 7.11.xxx Web** > **Class loader**, and select the following options:

   - **Single class loader for application**
   - **Classes loaded with local class loader first (parent last)**

Updating the Java Plug-in When Using Firefox 17

As of this release, the SM7.11 Web client supports Firefox 17; however, if you have the Java plugin, JRE versions below 1.6.0_31 or between 1.7.0 and 1.7.0_2 installed on your web client, you will need to click the Manage plug-in link to update the Java Platform Plugin to a newer version.

If you do not do so, problems might occur. For example, workflow graphics cannot display correctly.

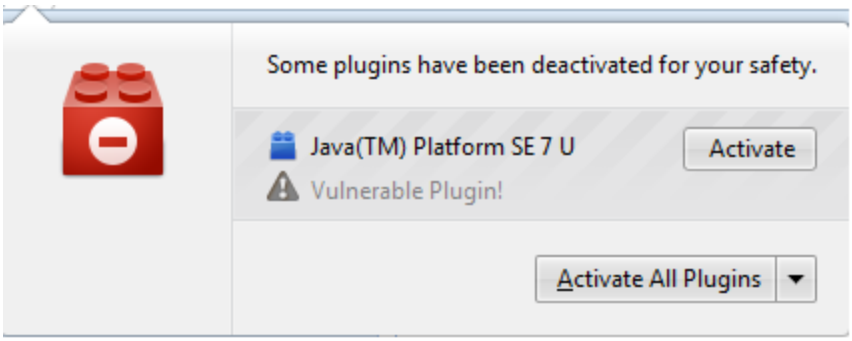
Activate your JRE7 plugin if blocked by Firefox

Due to a security enhancement in JRE 7, Firefox may deactivate your JRE7 plugin for your safety. When this happens, a red plugin icon appears in the address bar, next to your web client URL

string. For example, when you open the web client with `?telephonyuser=1` appended to its URL, Firefox deactivates the JRE 7 plugin; as a result, Service Manager cannot function properly (for example, cannot execute a telephony call). In this case, you need to activate your JRE7 plugin for your Service Manager web site as described here:

1. Click the red plugin icon in the address bar.

   A message window opens, as shown below.



2. Click **Activate All Plugins**.
3. Select **Always activate plugins for this site**.

   The red plugin icon now disappears from the address bar.

Deploying the Web Tier on JBoss 5.1

To deploy the web tier on JBoss 5.1:

1. Install JDK 1.5x from the Oracle web site.
2. Set the JAVA_HOME environment variable to the location of the JDK 1.5x version you installed in step 1.
3. Download the JBoss binary version from the JBoss web site.
4. Extract the JBoss package to a folder.
5. Add the JBOSS_HOME environment variable and set it to the location of the path above.
6. Before deploying the web tier .war file, extract the war file into a temporary folder.
7. Make necessary changes to the web.xml. For example, set the following parameters: secureLogin, sslPort, serverHost, and serverPort.
8. To prevent the JSF compatibility issue, add the following lines to the web.xml file:

```
<context-param>
    <param-name>org.jboss.jbossfaces.WAR_BUNDLES_JSF_IMPL</param-name>
    <param-value>true</param-value>
</context-param>
```

9. Zip the extracted .war file and rename it back to .war file.

10. Copy the modified .war file to: %JBOSS_HOME%\server\default\deploy.
11. To prevent the NullPointException when creating soap messages , modify "%JBOSS_HOME%\server\default\deploy\properties-service.xml" by adding the following lines:

```
<attribute name="Properties">
    javax.xml.soap.MessageFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl
    javax.xml.soap.SOAPFactory=com.sun.xml.messaging.saaj.soap.ver1_1.SOAPFactory1_1Impl
</attribute>
```

12. For Solaris only, to prevent the AttachmentStore issue, locate the following section in the profile.xml (%JBOSS_HOME%\server\default\conf\bootstrap\profile.xml), and change `<parameter class>` in this section to `<parameter class="java.io.File">`.

```
<bean name="AttachmentStore" class="org.jboss.system.server.profileservice.repository.AbstractAttachmentStore">
  <constructor>
  <parameter class>
      <inject bean="BootstrapProfileFactory" property="attachmentStoreRoot" />
    </parameter>
  </constructor>
  <property name="mainDeployer"><inject bean="MainDeployer" /></property>
  <property name="serializer"><inject bean="AttachmentsSerializer" /></property>
  <property name="persistenceFactory"><inject bean="PersistenceFactory" /></property>
</bean>
```

The updated section should look like this:

```
<bean name="AttachmentStore" class="org.jboss.system.server.profileservice.repository.AbstractAttachmentStore">
  <constructor>
  <parameter class="java.io.File">
      <inject bean="BootstrapProfileFactory" property="attachmentStoreRoot" />
    </parameter>
  </constructor>
```

```
  <property name="mainDeployer"><inject bean="MainDeployer" /></pro
perty>

  <property name="serializer"><inject bean="AttachmentsSerializer"
/></property>

  <property name="persistenceFactory"><inject bean="PersistenceFact
ory" /></property>

</bean>
```

13. Start JBoss manually if you did not set JBoss as a service from %JBOSS_HOME%\bin (by clicking run.bat).

    Note: To stop JBoss manually, navigate to the %JBOSS_HOME%\bin directory and issue the shutdown -S command.

14. Launch the web client URL to test the connection.

    Note: By default, JBoss listens on port 8080. If this port is already in use on your machine, change the HTTP Connector port in the JBoss server.xml file and restart the JBoss application server.

    Example: http://localhost:8080/webtier-7.11/index.do

New Parameters and RAD Functions

This release introduces the following new parameters and RAD functions.

Startup parameter: ldapnosizelimitmsg

Parameter
ldapnosizelimitmsg

Description
When limiting LDAP query with ldapmaxrecords:100 (for example), if LDAP query results are bigger than 100 records, users get the following message: `Message from LDAP server: Size limit exceeded`. This informational message may mislead users to think that something is not working correctly.

This parameter, when set to **1**, allows you to disable this informational message so that it will not display to and therefore not disturb end users.

See also QCCR1E31999.

Valid if set from

Server's OS command prompt
Initialization file (`sm.ini`)

Requires restart of Service Manager server?
No

Default value
0

Possible values
0 (Enable)
1 (Disable)

Example usage
Command line: `sm -httpPort:13080 -ldapserver1:ldapparent -ldapnosizelimitmsg:1`
Initialization file: `ldapnosizelimitmsg:1`

Startup parameter: maxgroupsperview

Parameter
maxgroupsperview

Description
This parameter defines the maximum number of groups that can be used in a view. When a user selects a view from the View list whose group count exceeds the limit, only the maximum allowed number of groups are displayed in the view, and the following message displays in the client UI:

"Maximum number of groups (xxxx) exceeded. Please modify the view definition to reduce the number of groups."

Note: This limit would be useful if a user runs a poorly created view that causes the servlets to consume too much CPU and memory and terminate the servlets.

See also QCCR1E72836.

Valid if set from
Server's OS command prompt
Initialization file (`sm.ini`)

Requires restart of Service Manager server?
Yes

Default value
5000 (groups)

Possible values
500 or greater. If a value less than 500 is specified, Service Manager will ignore the value and use 500 instead. A warning message will also occur in the sm.log file: "A maxgroupsperview value less than 500 specified and ignored. 500 is used."

Example usage
Command line: `sm -httpPort:13080 -maxgroupsperview:6000`
Initialization file: `maxgroupsperview:6000`

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. 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`

Startup parameter: maxhttpreqresponse

Parameter
maxhttpreqresponse

Description
This parameter defines the maximum response size (in bytes) for HTTP requests.
Note: A zero value disables the feature, which means there is no size limit.

Valid if set from
Server's OS command prompt
Initialization file (`sm.ini`)

Requires restart of Service Manager server?
Yes

Default value
20971520 (bytes)

Possible values
0: No size limit
Any size limit (in bytes)

Startup parameters: JavaScript access

Startup parameters change the behavior of the server.

Parameter
jsaccessfilereadregex
jsaccessfilewriteregex

Description

These parameters specify access restrictions from JavaScript code for file access. This is required for security reasons so that users with tailoring rights are not able to use the available SM JavaScript APIs to directly access the underlying host file system in an unauthorized way. These restrictions are described below:

- System administrator (sysadmin) users are allowed unrestricted access to the file system.
- Non-sysadmin users are allowed unrestricted access as well by default (none of these configuration parameters is present); if any of these parameters is present, access is restricted as follows:
  - `jsaccessfilereadregex:<regex>`: Files read using the readFile() JavaScript function must have an absolute path name that matches the regular expression <regex>.
  - `jsaccessfilewriteregex:<regex>`: Files written using the writeFile(), deleteFile(), writeAttachmentToFile() JavaScript functions must have an absolute path name that matches the regular expression <regex>.

Regular expressions must use proper syntax for Java-style regex (similar to Perl-style) (for example, '.' means any character and backslashes need to be doubled). File path names in `jsaccessfilereadregex` and `jsaccessfilewriteregex` must be absolute and use proper delimiters ('/' for UNIX, and '\' for Windows). They are case-sensitive for UNIX and case-insensitive for Windows.

File path names used as parameters to JavaScript functions can still be any legal OS-specific file path names. Absolute and relative path names are allowed as well as the usage of '.' and '..'. On Windows, delimiters can be either '/' or '\', while UNIX only allows '/'. However, path names from JavaScript commands are normalized first (relative paths are made absolute, the '.' and '..' are eliminated, and on Windows '/'s are transformed into '\'s) before they are pattern matched against their corresponding regular expression.

Valid if set from

Servers OS command promt
Initialization file (`sm.ini`)

Requires restart of server?

Yes

Default value

None (Unrestricted file access)

Possible values

Regular expressions

Example usage

- `jsaccessfilereadregex:C:\\Users\\joe\\Documents\\.+|C:\\SM-Install\\server-dist\\RUN\\(\w)+\.js`

  Read access is limited to any files under the C:\Users\joe\Documents directory and only for .js files under the C:\SM-Install\server-dist\RUN directory.

- `jsaccessfilewriteregex:^$`

  Only matches the empty string. This is used to deny all write access to the file system.

Parameter: fetchnotnullsystemp

Parameter
fetchnotnullsystemp

Description
Prior to SM7.11p20, records that have a non-NULL systemplate field were passed to the query condition filter before they merged the template, and were thus incorrectly filtered out. As of SM7.11p20, these records will merge the template record before they are passed to the query condition filter. You need to set it to "fetchnotnullsystemp:1" to fully enable the template merge functionality. However, it may cause performance issues if the table has more than 10K records whose systemplate field is not NULL.

See also QCCR1E32145.

Valid if set from
Server's OS command prompt
Initialization file (`sm.ini`)

Requires restart of Service Manager server?
No

Default value
0

Possible values
0 (Do not fully enable the template merge functionality)

1 (Fully enable the template merge functionality)

Example usage
Command line: `sm -fetchnotnullsystemp:1`
Initialization file: `fetchnotnullsystemp:1`

RAD function: datecmp

A RAD function that translates date/time fields to the correct SQL statement dialect. You can use this function in expert search of incidents, as well as in JavaScript programming.

See also QCCR1E52991.

Function
datecmp

Format
datecmp("DateTimeField1","LogicOperator","DateTimeField2","+/-", "TimeInterval")

Parameters
This function uses the following arguments.

Argument	Description	Example Value (s)
DateTimeField1	A date time field in a Service Manager table.	close.time

Argument	Description	Example Value (s)
LogicOperator	A logic operator.	>, >=, =, <=, <
DateTimeField2	Another date time field in the same Service Manager table.	open.time
+/-	Arithmetic operator: +or -.	+, -
TimeInterval	A string that represents the time interval to be added to or subtracted from the second date time field. The format of time interval can be: d, d hh:mm:ss, d h:m:s, hh:mm:ss, h:m:s, or hh:m:ss (1 digit mixed with 2 digits). Days can be omitted, or at most 9 digits. Hours, minutes, and seconds can be 1 or 2 digits (from 0 to 99), and hour:minute:second as a whole can be omitted if you enter only days.	10 02:03:04 (This string represents 10 days, 2 hours, 3 minutes and 4 seconds.)

Notes:

- All arguments must be enclosed in a pair of double quotes; otherwise the query parsing will fail.
- This function supports "AND"/"OR"/"NOT" to concatenate multiple datecmp() calls in one query.

  The following are two examples:

  datecmp("close.time", "<", "open.time","+", "1") or datecmp("close.time",">=", "open.time","+", "5:0:0")

  problem.status="Closed" and (not datecmp("close.time",">", "open.time", "+","31 04:02:30"))
- You can combine the result of this function with other query conditions to construct a complete query. For example, you can execute one of the following queries when performing an expert search of incidents:
  - problem.status="Closed" and datecmp("close.time","<","open.time","+","04:02:30") and datecmp("close.time",">=","open.time","+","02:02:30")
  - problem.status="Closed" and datecmp("open.time",">","close.time", "-", "04:02:30") and datecmp("close.time",">=","open.time","+","02:02:30")
  - problem.status="Closed" and datecmp("close.time",">", "open.time", "+","31 04:02:30")

  Note: The first two queries should return the same results, which are incidents whose closed time is between 2 hours and 4 hours from their open time; the third query should return incidents that were closed more than 31 days after their open time.

.

Example
An example of a JavaScript program that uses this function is as follows:

```
var f = new SCFile('probsummary', SCFILE_READONLY);

var query = 'problem.status="Closed" and datecmp("close.time", "<", "o
pen.time","+", "04:02:30") and datecmp("close.time",">=", "open.time",
"+", "02:02:30")';

if (RC_SUCCESS == f.doSelect(query))

{

do

{

print(f);

}

while (RC_SUCCESS == f.getNext());

};
```

Certifications

This release includes the following support matrix changes for the web client.

Added Support

- Internet Explorer 9
- WebSphere 7
- Firefox 17
- JBoss EAP 5.1
- JRE 7 (Update 11)

Dropped Support

- Firefox 3.x or earlier
- Tomcat 5.5 (**Note**: Tomcat 6.0.36 is recommended for enhanced security)
- JBoss 4.2

Enhancements

This release includes the following enhancements.

CR	Module	Problem	Solution
QCCR1E67279	Web Tier	The Service Manager Web Client does not support Internet Explorer 9.	The Web Client now works with Internet Explorer 9.
QCCR1E80261	Web Tier	Request that Service Manager 7.11 Web tier client be certified and supported with WebSphere 7.	Service Manager 7.11 supports WebSphere 7. However, special configuration is required to run Service Manager in WebSphere 7 on Solaris. See "Special Configuration for WebSphere 7 on Solaris" on page 13.
QCCR1E83966	Web Tier	As Java 6 is approaching its end of life, support for Java 7 on the Web client is required for all supported versions of Service Manager.	Java 7 on the Web client is now supported for Service Manager 7.11 Patch 20 or later. **Note**: Java 7 Update 10 and earlier versions of Java 7 contain a vulnerability that can allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system. For this reason, Java 7 Update 11 has been certified on Service Manager 7.11 Patch 20.
QCCR1E88961	Web Tier	JBOSS 5.1 is not certified on Service Manager 7.11.	JBOSS 5.1 has been certified on Service Manager 711 starting with patch 20.
QCCR1E88963	Web Tier	Firefox 17 is not supported for SM7.11.	Firefox 17 is now supported for SM7.11 patch 20 or later.

Fixed Defects

This release fixes the following defects.

Server

CR	Problem	Solution
QCCR1E18927	Operator records for users with an apostrophe in their last name usually have that in their email address, (vito.d'addabbo@abc.com). However, the apostrophe is treated as an escape character in UNIX.	Now, certain security sensitive characters are escaped, but email addresses are quoted.
QCCR1E31999	Users are receiving a confusing error message when LDAP query results exceed the maximum size (100 records, for example). The message should be available only in the log file for debugging purposes, rather than displaying in the Service Manager client window.	Added a new parameter (ldapnosizelimitmsg), which allows system administrators to disable the LDAP size limit message. See "Startup parameter: ldapnosizelimitmsg" on page 16.
QCCR1E32145	Search Results are inaccurate against the operator table if an operator's Template (systemplate) field has a value. The operator record will not display in a Search, even though the selection criteria says it should.	Records that have a non-NULL systemplate field now will merge the template record before they are passed to the query condition filter. In the old versions, these records were passed to the query filter before they merged the template and were thus incorrectly filtered out. A new parameter (fetchnotnullsystemp) is introduced in sm.ini. You need to set it to "fetchnotnullsystemp:1" to fully enable the template merge functionality. However, it may cause performance issues if the table has more than 10K records whose systemplate field is not NULL. See "Parameter: fetchnotnullsystemp" on page 20.

CR	Problem	Solution
QCCR1E89886	Using a type of TIMESTAMP in a dbdict SQL mapping on an Oracle database causes soap faults and a signal 11 error when saving data into the column. Service Manager will not automatically choose this data type, but users are able to manually map a database field to a SQL type of TIMESTAMP.	SQL type of TIMESTAMP in dbdict on Oracle no longer causes signal 11 when saving data into the column.
QCCR1E52991	In a default Service Manager version 7.11 system that uses an Oracle database, queries that include date and time calculations fail because of to SQL syntax errors. This prevents the creation of a view that shows all the interactions that were closed within 24 hours of being opened.	This issue occurs because the date/time fields arithmetic calculation concerned query results are incorrect in SM. This is true regardless of the database. This is due to the lack of a generic representation of time interval, and the different ways to calculate it in those DB server types. Add a new RAD function datecmp ("DateTimeField1","LogicOperator","DateTimeField2","+/-", "TimeInterval") that translates date/time fields to the correct SQL statement dialect. The function can be used in expert incidents searching, as well as in JavaScript programming. See "RAD function: datecmp" on page 20.
QCCR1E65361	Fields in the generated "make-up" dbdict for ADHOC SQL sometimes have an identical index number.	The index numbers are now different.
QCCR1E65993	Service Manager (SM) background process consumes memory, keeps growing, and then needs to be restarted (once in two days or sometimes once a day). This is due to the fact that several background processes are killed and then restarted by the administrator, due to some other issue in the application.	Now, if an SM session is killed by administrator or an SM session terminates due to a Signal 11, the memory used by the session (via malloc) will force a cleanup.
QCCR1E70833	A complex query that uses a condition for an array field returns no record data.	The complex query will display results as expected.

CR	Problem	Solution
QCCR1E71657	User sessions hang or cannot connect after many different ESS users have logged in because the coordinator process runs out of memory. This behavior may occur even after the other users have logged out.	The coordinator process will no longer run out of memory.
QCCR1E72743	The Web client ignores the "Invisible" settings in the fields of the "Data policy" table.	The Web client no longer ignores the "Invisible" settings in the fields of the "Data policy" table. **Known issue**: If a field is configured as "invisible = true" and it is used in a select() expression as output, this field will still display the value of the field configured as "invisible=true" when this expression is used in a "value list condition" of another field. For example, the "value list condition" of the "New Update Type" field in the "IM.update.incident" form, is set as the following: "select ("activity.name","activitytype","table","probsummary","visible","YES")" If activity.name is configured as invisible, the value list will still be displayed in "New Update Type". **Note**: Another known issue that exists in 7.11.p19 has been fixed in this release. See the SM7.11p19 Release Notes.
QCCR1E72809	After closing a ticket (such as an Interaction or Incident) and returning to the view, the queue is not synchronized correctly.	Now, when detecting a record deletion, SM updates the group information so that the queue synchronizes correctly. **Note**: This works only when a user deletes records. If users update or insert records, the view display issue will still exist. As a workaround, users can click the "Refresh" button to solve the view display issue for the latter case.

CR	Problem	Solution
QCCR1E72834	An administrator cannot terminate a session that is fetching millions of records. This may occur due to a poorly created customer view, which can cause servlets to consume too much CPU and memory, and then terminate servlets.	Now, administrators can terminate a session that is fetching millions of records.
QCCR1E72836	There is no limit on the number of records an SM Process can try to fetch. A limit would be useful if a user runs a poorly created view that causes servlets to consume too much CPU and memory and terminates the servlets.	Added a parameter maxgroupsperview to limit the number of groups allowed in a view. See "Startup parameter: maxgroupsperview" on page 17.
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.	A new parameter, maxmemoryperthread, has been added that specifies the maximum memory allowed for a session (in MB). After the limit is reached, the session is terminated. **Notes**: The minimum is 100 MB, and the maximum is as permitted by the OS (the default value of this parameter is 0, which means using the OS limit). See "Startup parameter: maxmemoryperthread" on page 17.
QCCR1E73782	A "Signal 11" error is generated when initializing LDAP and the following error message is logged in the SM.log file many times: "A signal 11 was raised in native code. Client terminated. Error: Win32 Exception:0xC0000005 (instruction 0x61DFF440 while reading address 0x00000000)"	The "Signal 11" error is no longer generated when initializing LDAP. Now the SM application can handle the exception by logging the following information in the sm.log file: "The ldapserver isn't set in scldapconfig."

CR	Problem	Solution
QCCR1E73864	The server process consumes a lot of memory and time when the "Go to last page" button is clicked from the Web client on the list/detail screen of a query with thousands of returned records. This behavior may occur because of a poorly created view. This behavior can cause the servlets to consume too much CPU and memory and eventually terminate the servlets.	The server process now only lasts for a few seconds with less memory consumed when the "Go to last page" button is clicked on the list/detail screen of a query with thousands of returned records. This behavior will no longer terminate the servlets.
QCCR1E74051	After applying a custom upgrade, users are experiencing sudden session timeouts in the Web tier and "Signal 11" errors in the Windows client. Investigation indicates that the "Signal 11" error is caused by a call to the RCCondition.isCalendarShow function when the Document Engine calls the probsummary master format control.	The "Signal 11" error will not be thrown and will therefore prevent the user session from suddenly terminating. **Note**: This behavior (the "Signal 11" error NOT being thrown) occurs even if the memory for JavaScript is not sufficient to run the JavaScript program. This fix does not address the lack of memory.
QCCR1E74101	"Users cannot log in after starting a servlet, and the following message is logged: RTE E EVP_PBE_CipherInit() failed in desEncryptPasswordFieldWithMD5AndDes()"	This issue occurred because of a concurrent call to the OpenSSL crypto library. This has been resolved so that the call will no longer impact the login to Service Manager.
QCCR1E74528	On ESS, buttons will overlap when display option labels are greater than 10-12 characters.	Now, the ESS client truncates long labels to ensure the buttons do not overlap.
QCCR1E74646	Background event processes consume high memory usage, even though there are no event records to process.	Background event processes can run without consuming excessive memory.

CR	Problem	Solution
QCCR1E74709	Webservice requests get corrupted when they contain inline attachments whose base64 encoding contains carriage return line feeds.	An RTE change is made to prevent inline attachments containing carriage return line feed characters from being corrupted.
QCCR1E75514	WCF client cannot add an MTOM/XOP attachment when calling the SM Web service to create an incident.	WCF client can add MTOM/XOP attachment when calling the SM Web service to create an Incident.
QCCR1E75861	An array of structures nested within an array of structures in a dbdict table does not work in Oracle databases.	An array of structures nested within an array of structures in a dbdict table works as expected in Oracle databases.
QCCR1E76056	Cannot search Change tickets with a Change ID.	Now, tickets that have a Change ID can be searched as expected.

CR	Problem	Solution
QCCR1E76399	Partial System Outage occurs when a node in the cluster quit responding to requests. This behavior occurs when the Transparent Application Failover (TAF) feature on Oracle is enabled. When this issue occurs, the following messages are logged repeatedly: 9568468(36438057) 05/06/2012 13:50:37 RTE E Unable to parse date for column SYSMODTIME 9568468(36438057) 05/06/2012 13:50:37 RTE E Incomplete record, could not process data for table NUMBERM1 in file number identified by key: name="incidents" 9568468(28049409) 05/06/2012 13:50:37 RTE E Error in fetching sequence number for file incidents 9568468(36438057) 05/06/2012 13:50:37 RTE E date format '06-MAY-12' unrecognized in sqlda	Service Manager now detects the TAF configuration and prints warning messages to the sm.log at startup. The warning messages are listed below: 2852(2844) 07/31/2012 13:06:34 RTE !! 2852(2844) 07/31/2012 13:06:34 RTE ServiceCenter does not support Oracle TAF. Please remove TAF configuration and restart ServiceCenter to avoid running into outages. 2852(2844) 07/31/2012 13:06:34 RTE !!
QCCR1E76660	Colon appears in the converted date when using the getTime() JavaScript function.	This issue occurred because the current js_1.5rc6a.dll is built with Microsoft Visual Studio 2003 and there is a defect within the function for converting a double to a string. This issue was resolved by rebuilding the DLL with Microsoft Visual Studio 2008.

CR	Problem	Solution
QCCR1E78485	Sometimes, a poorly constructed query results in a long running transaction. If the user waits for a few minutes, and then terminates the client session, the server session continues to run the query until the session is terminated from system status. However, the session should be terminated automatically when the client is disconnected.	The session is now terminated properly on the server side when the client session expires.
QCCR1E78958	System-generated queries that contain "OR (m1."NUMBER" IS NULL)" or a similar syntax are slow to respond on Oracle 11.	To avoid this issue, system-generated queries will no longer contain "OR (m1."NUMBER" IS NULL)" or a similar syntax.
QCCR1E79917	Libjs.so relies on the gcc library in the RTE/RUN folder on AIX platforms. Therefore, if the user environment does not have gcc installed, Service Manager cannot be started.	Service Manager can be started even if the user does not have gcc installed.
QCCR1E84079	Errors occur when applying an application patch on a Service Manager production environment.	No error occurs when applying an application patch on a Service Manager production environment.
QCCR1E84156	When you open, update, resolve, or close an Incident, warning message appears: Warning,indexing to NULL. The incident takes over 5 minutes to update.	This issue occurs because the old implementation of the "copycurrent" RAD function did not copy a merged file properly. This has been fixed in this solution.
QCCR1E84337	After upgrading to later releases of the Service Manager application and binary files, the functionality that tracked how many logins since the last reset is removed and this information is no longer traced in the operator record.	This functionality is now implemented on the RTE side.
QCCR1E84496	The system navigator is not displayed after login.	Now, users can log in as expected. The system navigator is displayed correctly.

CR	Problem	Solution
QCCR1E84490	When the RTE detects that the IR file is corrupt, a Signal 11 error is received and the system crashes.	The RTE will detect when the IR file is corrupt, and will prevent the crash.
QCCR1E87640	SCAutoListener enters an infinite loop and leads to high CPU utilization. The Service Manager session encounters a signal 6 and produced a core file.	Added new logic to check whether there is any data read by the listener. If no data is read, quit from reading to avoid infinite loop.
QCCR1E87784	When IR detects corruption, Service Manager issues the following, misleading messages: 7532(7124) 10/25/2012 23:15:22 RTE E Error 0 in call irReadInP4 - The operation completed successfully. 7532(7124) 10/25/2012 23:15:22 RTE E irReadInP4: Failure reading 32768 bytes at offset scirexpert:ir.probsummary (52409176), errno=0 (No error) The error messages state "The operation completed successfully" and "No error" which is not the case. This issue occurs when the IR files are internal (i.e, mapped to the scirexpert table).	Now, clear messages will be provided. If Error = 0, the first message will not be issued: "RTE E Error 0 in call irReadInP4 - The operation completed successfully"

CR	Problem	Solution
QCCR1E88044	A TeMIP-SM integration fails with "Out-of-Memory" errors or otherwise becomes unstable. This issue occurs because Service Manager processes queries incorrectly and returns all records for the table when the database is frequently inaccessible.	The "Out-of-memory" error will no longer occur because Service Manager now returns the correct records or error message even if the database is frequently inaccessible. If the object.name is the same as the name in the "extaccess" table, the correct records will be returned. If not, the following xml response will be returned to the client side and the error information will be logged in sm.log: <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"> <SOAP-ENV:Body> <CreateIncidentResponse message="Specified Name Not Found" returnCode="7" status="FAILURE" xmlns="http://schemas.hp.com/SM/7"/> </SOAP-ENV:Body> </SOAP-ENV:Envelope>
QCCR1E88335	A attempt to add an attachment with a file name that ends with a dot, or an attempt to update an object that already has an attachment with a file name ending with a dot results in termination of the session with error "SCStringValue() pos > length".	This issue occurs because a "." at the end of a file is considered as the delimiter for the extension. Now, the sequence for the delimiter is "." + any character.
QCCR1E88468	After you upgrade to SM 7.11 Patch 19, a Signal 11 error occurs and the servlets eventually hang.	Now, the issue has been resolved by rolling back a change introduced in the previous release.
QCCR1E78643	SM handles JournalUpdates incorrectly in an UpdateIncidentRequest Web services call when there is an empty line in JournalUpdates.	SM now handles JournalUpdates as expected when there is an empty line in JournalUpdates.

CR	Problem	Solution
QCCR1E89204	The pagination control bar is floating over record lists in Firefox 17.	The pagination control bar is no longer floating over record lists in Firefox 17. **Known Issue**: The table header of a record list becomes invisible when the user scrolls down the list, however moving the scroll bar to the top will bring the table header back.

Web Client

CR	Problem	Solution
QCCR1E32262	Extra spaces are being added to journalized updates in the web client.	Extra space lines are no longer being added in web client.
QCCR1E32467	Adding a new folder favorite via the navigator takes an excessive amount of time.	Processing for adding a new folder to Favorites has been improved for better performance.
QCCR1E58337	Two timer widgets cannot be displayed on the same format at the same time in the Service Manager web client.	Multiple timer widgets can be displayed correctly on the same format in the web client.

CR	Problem	Solution
QCCR1E60097	When using characters that are treated as illegal (for example, the right-arrow character), the Web client fails with the following error message: "Error: The data %22Test"....is not legal for a JDOM character context: 0x1a is not a legal XML character."	Control characters can be saved on the Windows and Web clients without errors. **Note**: If a control character is entered in a single-line text field of a record, then when Service Manager loads the record, the control character displays as "&#x…; " where "..." represents a hexadecimal number. For example, the right-arrow character will display as "&#x1a;". However, in a multi-line text field, the control character displays exactly as it was entered when the record is loaded.
QCCR1E69476	In the web client, in the Approval Log section of Change Management, the comments column does not display input values after the first row.	The comments column displays input values after the first row in the Approval Log section.

CR	Problem	Solution
QCCR1E71381	On the Web client, when an operator accesses a change ticket with partial approval, and then clicks Save without making any changes to the ticket, the Reset Approvals form is displayed. This form indicates that a change has been made to the ticket even though no change has been made.	When editing contents with multiple lines in a textarea component with a visible/invisible DVD condition, no extra blank lines will be inserted in the contents after saving the record.

CR	Problem	Solution
QCCR1E72468	The Dynamic View Dependency for checkbox controls is evaluated incorrectly in the Web client. For example, if you set the "Selected Condition" property to a variable that evaluates to false, the check box is unchecked in the Windows client but checked in the Web client.	The Dynamic View Dependency for checkbox controls is evaluated correctly in the Web client.
QCCR1E72743	The Web client ignores the "Invisible" settings in the fields of the "Data policy" table.	The Web client no longer ignores the "Invisible" settings in the fields of the "Data policy" table. **Known issue**: If a field is configured as "invisible = true" and it is used in a select() expression as output, this field will still display the value of the field configured as "invisible=true" when this expression is used in a "value list condition" of another field. For example, the "value list condition" of the "New Update Type" field in the "IM.update.incident" form, is set as the following: "select ("activity.name","activitytype","table","probsummary","visible", "YES")" If activity.name is configured as invisible, the value list will still be displayed in "New Update Type". **Note**: Another known issue that exists in 7.11.p19 has been fixed in this release. See the SM7.11p19 Release Notes.

CR	Problem	Solution
QCCR1E73103	Some users are unexpectedly logged out from the Web client when the number of cookies exceeds the limit specified by Internet Explorer.	The issue is fixed by reducing the number of cookies used by the Web client.
QCCR1E77105	The Affected CI fill button retains an old value in the Web client. The fill button works as expected on the Windows client.	Now, the Affected CI fill button behaves correctly in the Web client.
QCCR1E77415	When a record contains special characters in a multi-line text field, the Web client converts the characters into their HTML code representations in Print Preview. For example, quotation marks are replaced by &quot, and a greater than sign (>) by &gt.	Print Preview can display special characters correctly.

CR	Problem	Solution
QCCR1E79109	Web client images are not displayed at the correct size when forms are first rendered in the Web client.	Images are rendered at the appropriate size in the Web client.
QCCR1E78176	When you set the main menu to SC style after you log in, a JavaScript error is received. Additionally, groups cannot be expanded automatically.	There is no JavaScript error in the main menu page, and the first group is expanded by default.
QCCR1E79114	A data changed event fires too late when the focus leaves a radio button in the Web client running in Internet Explorer.	The data changed event fires properly when the focus leaves a radio button in the Web client running in Internet Explorer.

CR	Problem	Solution
QCCR1E79776	After an SM server upgrade, the direct link URL no longer works in the Web client and the following error is thrown: Error: setAttribute: Session already invalidated This issue occurs even with the same SSO setup. If a Web client session is already established before opening the direct link URL, the link works as expected.	Opening a direct link URL of the SM web client now opens the specific location in the SM web client without an error. **Known Issue**: In TSO mode, when users attempt to access the ServiceManager Mail utility directly by entering a URL like http://web-server:port/web-tier/index.do in the browser, a 404 error occurs.
QCCR1E89253	A needless confirmation dialog appears when you click the Cancel button from the View tab without any modifications.	Now, the confirmation dialog no longer appears when you click the Cancel button from the View tab without any modifications.

Windows Client

CR	Problem	Solution
QCCR1E53130	After you change the font size or select the Restore Defaults from **Window** > **Preferences** > **Appearance** on the Windows client, the format no longer fits on the screen. This results in objects falling off the edge of the form and the vertical and horizontal scroll bars are not created. This behavior prevents users from navigating the form.	Now the scroll bars are shown as expected when a larger font is used.
QCCR1E66750	You cannot print a record using the "File > Print" option in the Windows client if the record has an attachment.	You can use the "File > Print" option in the Windows client to print a record.
QCCR1E73743	When a groupby clause is specified, an SM process may attempt to fetch all the records from the database.	When a groupby clause is used, only the last group is retrieved. **Note**: All rows are fetched only when no groupby clause is specified.

Known Problems, Limitations, and Workarounds

This software release has the following known issues and limitations.

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.
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
QCCR1E69449	The user encountered a signal 11 while updating an incident: RTE E Caught XML API exception scxmlapi(40). This is because another user was updating the probsummary dbdict record at the same time.	When modifying a dbdict record, ensure that there are no other users updating records or inserting records in the same file. For example, when updating the probsummary dbdict, make sure that there are no other users updating existing incidents or opening new incidents.
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.

Documentation Errata

The following documentation items are incorrect.

CR	Problem	Solution
QCCR1E79050	The description of RAD function rtecall("sort") in the online help is incorrect. See the following errors.	See the following corrections.

Location:

Online help: the description of $L.type Number of RAD function rtecall("sort")

Error: :

The value for ascending is one (1) or descending zero (0).

Correction:

The value for ascending is zero (0) or descending one (1).

Location:

Online help: the examples of RAD function rtecall("sort")

Error:

Examples

```
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $list, 1, 0)
Returns: $L.list= {{"a", "c", "b", "d"}, {1, 2, 3, 4}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $list, 1, 1)
Returns: $L.list={{"a", "c", "b", "d"}, {1, 2, 3, 4}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $list, 0, 0)
Returns: $L.list={{"a", "b", "c", "d"}, {1, 3, 2, 4}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $list, 0, 1)
Returns: $L.list={{"d", "c", "b", "a"}, {4, 2, 3, 1}}
```

Correction:

Examples

```
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $L.list   , 1, 0)
Returns: $L.list= {{"a", "c", "b", "d"}, {1, 2, 3, 4}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $L.list   , 1, 1)
Returns: $L.list={{"d", "b", "c", "a"}, {4, 3, 2, 1}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $L.list   , 0, 0)
Returns: $L.list={{"a", "b", "c", "d"}, {1, 3, 2, 4}}
$L.list={{"a", "b" ,"d", "c"},{1, 3, 4, 2}}
$L.success.flg=rtecall("sort", $L.return.code, $L.list   , 0, 1)
Returns: $L.list={{"d", "c", "b", "a"}, {4, 2, 3, 1}}
```

Backout Instructions

If you want to restore your Service Manager system to its original state after installing this patch, follow these guidelines.

Server

Before applying the server patch, make a backup of the server installation folder. For example, C:\Program Files\HP\Service Manager 7.11\Server.

To roll back your server to its original state, remove the existing server installation folder and copy the old one back.

Web Tier

Before deploying the new web tier, back up your web.xml file, application-context.xml, splash screen, style sheets, and any other customizations you made, including your webtier-7.11.war (webtier-ear-7.11.ear) file.

To roll back to the old web tier:

1. Delete or uninstall the existing web tier.
2. Redeploy the old web tier.
3. Restore your old customizations.

Windows Client

You can only uninstall the new Windows client, and then reinstall the old version.

Applications

Before loading an unload file

Before loading an unload file, perform the following steps to make a backup of the files to be modified by the unload file:

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.
3. Go to **Tailoring** > **RAD Editor**, search for the files you noted in step 2, and click **More** > **Export/Unload**.

4. In the popup window, specify your backup upload file path/name, and click **Unload Appl**.
   Note: Make sure that **Append to file** is selected.

When applying an application patch

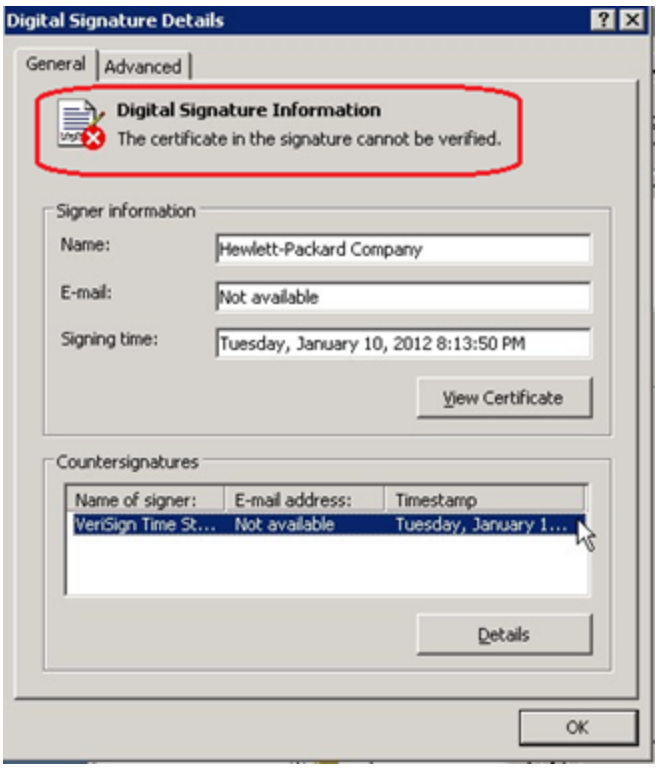
Before applying an application patch, make a backup of your database. To roll back your application changes, restore your database to the backup.

Installation Notes

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

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

Web Tier Installation

The Web Tier update consists of a compressed file, sm711.604-P20_Web_Tier.zip. The specific upgrade process depends on your particular Web application server, but follows the same steps as deploying a new installation. For more information, refer to the Service Manager Installation Guide.

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.

To install the Web Tier update:

1. Back up your web.xml file, splash screen, style sheets, and any other customizations you made, including your webtier-7.11.war (or the .ear) file.
2. Delete or uninstall the existing webtier-7.11.war (or the .ear) file.

   Note: The "Update Application" function in WebSphere Application Server 6.x allows you to redeploy using a new copy of webtier-7.11.war (.ear). First, update the web.xml in the webtier-7.11.war (.ear) file, and then redo the shared library configuration. For more information, see the IBM WebSphere documentation.
3. Deploy the new webtier-7.11.war (or the .ear) file following the instructions in the Service Manager Installation Guide.

   Note: It is best practice to deploy with a unique context root. For example: /webtier-7.11.604
4. Replace the new versions of any files you customized with your customized versions.
5. Make any new customizations necessary for your deployment. Be sure to set the secureLogin and sslPort parameters.
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, sm7.11.604_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.
4. Check the version in **Help** > **About Service Manager Client**.

   The client should be Release: **7.11.604**.

Server Update Installation

The server update for your operating system (OS) consists of a compressed file, `sm`7.11.604-P20_`<OS>.zip` (or `.tar`), which contains the Service Manager server files. These files add to or replace the files in the `[SM Server Root]\ ([SM Server Root]/) RUN, irlang, legacyintegration`, and `platform_unloads` directories.

Note: If you have a load balanced system, you must upgrade all server instances.

Important: This server update will upgrade the embedded Tomcat to version 6.0.36, and therefore requires additional steps.

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. 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. 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 7.11\Server.`
7. For UNIX servers, set the file permissions for all Service Manager files to 755.
8. If you have made any customizations/changes to the original **RUN/tomcat** folder, restore them in the new **RUN/tomcat** folder.
9. Restart the Service Manager server.
10. Restart the Service Manager clients.
11. Check the version in **Help** > **About Service Manager Server**. The server should be Release: 7.11.604.

Application Unload Installation

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 sm7.11.604-P20_<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.

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. Note that this is always the number of the parent CR of a CR family (if any).

- 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 7.11 patch	Used for apps version (s)	Description
QCCR1E71099_ SM711P19.unl	P19	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. See server fix QCCR1E71099.
QCCR1E67072_ SM711P18.unl	P18	7.11	Improves the performance of the Knowledge Management update process (KMUpdate).
QCCR1E67610_ SM711P18.unl	P18	7.11	Enables Service Manager to block potentially dangerous attachments.
QCCR1E49721_ SM711P17.unl	P17	7.11	Allows a translation of Display/Value Lists on dynamic forms. This is a required fix for the Export to Excel redesign.
QCCR1E56678_ SM711P17.unl	P17	7.11	Lists the records in the right group order when a record list is refreshed.
QCCR1E58562_ SM711P17.unl	P17	7.11	Includes applications changes for the Export to Excel redesign.

Unload file	Introduced in 7.11 patch	Used for apps version (s)	Description
QCCR1E59385_SM711P16.unl	P16	7.11	Improves performance by removing the duplicate select from JavaScript sloDisplay.getListSLOs. — If you haven't tailored the JavaScript sloDisplay, load QCCR1E59385_SM711P16.unl file — If you have tailored the JavaScript, see installation for tailored sloDisplay JavaScript in the SM711 patch 17 release notes.
QCCR1E59389_SM711P16.unl	P16	7.11	Improves performance by removing extra selects from the various displayscreen and displaycache records. — If you haven't tailored the display screens, load QCCR1E59389_SM711P16.unl. — If you have tailored the display screens, see installation for tailored displayscreen and displaycache records in the SM711 patch 17 release notes.
QCCR1E55713_SM711p15.unl	P15	7.11	Includes application changes to reduce database I/O on login.
QCCR1E57766_SM711p15.unl	P15	7.11	Includes application changes to reduce jgroups traffic on login.
QCCR1E55852_SM711p14.unl	P14	7.11	Includes a new activity timer that makes the communication between SM processes more efficient.

To load an unload file:

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 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**.

ODBC Diver Update Installation

This release does not include the ODBC Driver patch shipped with SM7.11p19, which you can download from SSO: http://support.openview.hp.com/selfsolve/document/KM1448270.

The ODBC Driver update 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.

Service Manager Compatibility Matrix

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

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 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 7.11 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.