HP Service Manager

For the Supported Windows® and UNIX® operating systems

Software Version: 1.0

Mobile Applications

Document Release Date: July 2011

Software Release Date: July 2011

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*.

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 log on. 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 log on 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

Chapter 1

Getting Started with HP Service Manager Mobile Applications

Welcome to HP Service Manager Mobile Applications! Service Manager Mobile Applications connect your company's people and information by providing your team access to the Change Management and Incident Management applications through the use of smartphones.

Service Manager Mobile Applications enable your Change Management and Incident Management staff to have 24 X 7 mobile access while out of the office so they can:

- approve and deny change requests
- view newly-assigned tickets
- reassign incidents to the proper support group
- continue working on-site with customers

How can Service Manager Mobile Applications be used?

Because field engineers are typically tasked to work with business users at a customer site, they spend most of their time away from the office to resolve tickets. When Change Approvers are away from the office, they need a way to quickly approve or deny changes, so that pending work orders can be assigned. These users can log on to Service Manager Mobile Applications from a smartphone to receive and view work assignments; and review and approve or deny pending change requests. These quick responses improve business metrics, as service level objectives are met.

When users launch Service Manager Mobile Applications, they can:

- log on with their Service Manager user name and password
- check a “Remember Me” option (if enabled)
- tap the log-in button to land on their home page

When logged in, users can:

- view incidents (assigned to me and assigned to my group) or changes (awaiting my approval and assigned to my group)
- view related configuration items
- approve and deny changes
- reassign an incident to another group
- add or update activities
- resolve or close tickets and requests when work is complete

Preparing to launch Service Manager Mobile Applications on your smartphone

To prepare for launching Service Manager Mobile Applications on your smartphone, make sure:

- Your smartphone includes a WebKit-based browser (for example, the i-Phone or Android browser), with the following configuration:
  - Cookies enabled
  - JavaAScript enabled
  - At a minimum, add the Service Manager Mobile Applications host name to the pop-up exception list.
- Your System Administrator has provided you with the web URL needed to access Service Manager Mobile Applications.
  For example: http://<hostname>:8080/mobileItsm
- You have a valid Service Manager login.

Launch Service Manager Mobile Applications on your smartphone

User role: All users

To launch Service Manager Mobile Applications on your smartphone:

1. In the web browser on your smartphone, enter the Service Manager Mobile Applications web URL provided by your System Administrator.

   For example: `http://<hostname>:8080/mobileItsm`

   The Log In page displays.
2. Log in to your home page.
   a. Enter your user name and password.
   b. Select **Remember Me** (if enabled by your System Administrator), so that your log-in information is auto-filled in the log-in screen and you can go directly to your home page.
   c. Tap **Log in** to land on your home page. Your mobile data is automatically synchronized with data in the Service Manager database.
3. Add the Service Manager Mobile Applications web URL to your list of home page bookmarks.

   Note: The Service Manager Mobile Applications icon is automatically added to your smartphone list of applications for future use. You can verify this now by checking your smartphone list of applications.
4. If enabled by your System Administrator, you can connect to an alternate Service Manager server. Add the new URL to your Server settings, as follows:
   a. From your Mobile Applications home page, tap on the options icon and select **Server**.
   b. Type the host name or IP address and port number of the new server URL. For example: **<hostname>:8080/mobileItsm**

c. Tap **Add URL**. You will be logged out of Service Manager Mobile Applications.

d. Log back in to Service Manager Mobile Applications.

You will see categories of incidents or changes displayed according to your user role. You can drill down into each List view to see incident tickets or change requests assigned to you and assigned to your group. If you are a change approver, you will also see change requests waiting for your approval.

Note: When navigating through lists and detail records, you can tap the settings icon to go back to your home page or log out of your mobile session.

Views within Service Manager Mobile Applications

Views available in Service Manager Mobile Applications provide alternate ways for users to access individual and group records.

- Home page: When users log in to Service Manager Mobile Applications, they land on their Home page.
- List view: Allows users to navigate through lists of records to see assigned tickets and change requests, and search for specific records.
- Detail view: Allows users to view and edit tickets and change requests.

Note: When navigating through lists and detail records, you can tap the settings icon to go back to your home page or log out of your mobile session.

Home page

When users log in to Service Manager Mobile Applications, their mobile data is automatically synchronized with the Service Manager database and their home page displays the applicable categories of records. The default configuration supports the following categories:

- Incidents Assigned To Me
- Incidents Assigned To My Groups
- Changes Awaiting My Approval
- Changes Assigned To My Groups

When users display the contents of a view, the query associated with it automatically runs and produces the list of records that meet the query criteria. Views appear as categories on a user's home page.

List view

The List view enables users to browse and sort through lists to search for specific incidents and change requests. In the List view, users can:

- Synchronize mobile data to be current with the Service Manager database of records.
- See the record counts in lists.
- Scroll vertically through a list of records.
- Sort List views based on specified fields.

- Re-synchronize the List view.
- Use the Home button to exit views.
- Use options and settings to:
  - Search for records by record ID.
  - Return to the home page.
  - Log out of your mobile session.

Detail view

The Detail record view enables users to view the details of a record. In the Detail view, users can:

- See the title (for example, the incident ID number) and description of a record.
- See the default fields of a record.
- Update the status of a record.
- Review activities in a record.
- Use click-to-dial functionality. When users drill into the contact information of a record, they can click on a telephone number, a call dialog box displays.
- Use click-to-email functionality. When users click on an email address, the email function opens. For example, if a field engineer wants to notify a customer that he is going to stop by, he can drill into the contact information of a record and use the single-click method to call or email the customer.

Note: When navigating through lists and detail records, you can tap the settings icon to go back to your home page or log out of your mobile session.

View my assignments and my group's assignments

User role: All users

When users are logged into their Service Manager Mobile Applications home page, they can view their assigned tickets and the assigned tickets for their group. This enables users to address any critical and pending issues that need immediate attention.

Field engineers can also receive email notification for those high priority tickets that have just been assigned to them. When notified of a high priority ticket, a field engineer can log into Service Manager to view the record by clicking on the URL in the email notification. Once logged in, Service Manager Mobile Applications automatically synchronizes the user's mobile data with the information in the Service Manager database, and then searches for the record by name and displays it. If the record is not in the cached database, Service Manager will be queried to fetch the record.

Note: When navigating through lists and detail records, you can tap the settings icon to go back to your home page or log out of your mobile session.

Incident Management mobile application

When incidents are escalated from Service Desk interactions, opened by support staff, or reported by event monitoring tools, the Incident Management mobile application provides the Incident Management staff the ability to perform the following tasks from their smartphone:

- Browse and review incidents.
- Assign or reassign an incident.
- Investigate incidents.
- Update incidents. For example, a field engineer can add an activity (or journal entry) update to an incident record and set the customer-visible flag to make the update available for customer viewing on the customer support portal.
- Resolve or close a ticket (not both). When a field engineer attempts to resolve or close an incident, Service Manager determines the business logic and displays Resolve or Close accordingly.

  Note: Use the Fill function in the Closure Code field to select a closure code.

Set the customer-visible flag for an incident's activity

User role:All users

When you want to publish the activity (or journal entry) details of an incident for customer viewing, you can set the customer-visible flag in a new activity entry.

To set the customer-visible flag in a new activity (or journal entry) entry.

1. Select an incident to view.
2. Drill down into the Incident's Activities field.
3. Tap **New Entry** and then tap **Customer Visible**.
4. Add the details for the new activity (or journal entry), and then tap **Add New Entry**. The details of the new activity entry will become available for customer viewing on your customer support portal.

Change Management mobile application

When a change request is logged, the Change Analyst assesses the change request, implements a plan for delivering the change, and then notifies the Change Coordinator as to the impact of the change. The change request is then submitted for approval by the Change Approver, or Change Advisory Board (CAB). Service Manager Mobile Applications provides the Change Management staff the ability to perform the following tasks from their smartphone:

- review change requests
- approve or deny changes
- coordinate change implementation
- handle emergency change requests
- assign or reassign change requests
- add activity (or journal entry) entries
- review and close change requests

An example of a change approver's possible actions for a change record include approving or denying change requests. To deny a pending change request, a Change Approver would do the following:

- Drill down into a single record.
- Deny the ticket.
- In the Update field, type detailed notes about the denied request.

Users can also drill down to the details of a field within a record. For example, if the Change Management staff wants to add an activity (or journal entry) update to a change request, they would do the following:

- Search for the change record.
- Drill down into the record's activities.
- Add the necessary activity update.
- Make any other necessary changes.

Chapter 2

Customizing personal settings

All users like to personalize their work environment for efficiency. For example, they may need to add an additional server to access their tickets, or set default fields for easy access to the urgent tickets in their queue. You can change these things with the settings on your home page. If your System Administrator has enabled these options for you, your changes will be immediately available on your home page.

Customize personal settings

User role: All users

Service Manager Mobile Applications supports customization and configuration to improve performance and user experience. The following can be edited in the home page and List records view:

Setting	Default value	Description
Server	The current Web URL	This home page setting allows users to do the following: ▪ Select pre-configured server connections. To edit the server connection, select a server from the server connections list. ▪ If enabled by your System Administrator, add a custom URL. To add a new server (URL) connection: a. Tap **Add URL**. b. Type the host name or IP address and port number of the new server URL. For example: **http://<hostname>:8080/mobileltsm** c. Tap **Add URL**. You will be logged out of the Service Manager Mobile Applications. d. Log back in to Service Manager Mobile Applications. You will be connected to the new server.

Chapter 3

System administration

Out-of-box, Service Manager includes a bundle of published tables, fields, and display actions collectively known as the Service Manager Web Services application program interface (API). Service Manager Mobile Applications is a framework deployed to Apache Tomcat server. It uses the Service Manager Web Services API to give users mobile access to Service Manager records to review, deny, approve, assign, update, and resolve issues. As a System Administrator, you will install, set up, and configure Service Manager Mobile Applications.

Data model

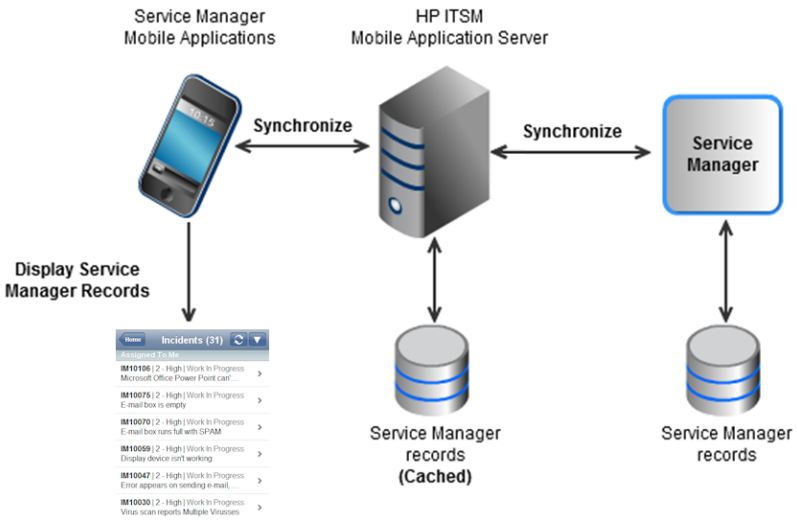
The Service Manager Mobile Applications data model is based on the Business Technology Optimization (BTO) software Data Model (BDM), which is the standard data model for integrations between HP BTO products.

This standard data model allows the System Administrator to:

- Set up the Service Manager Mobile Applications server
- Add tables and fields
- Update field maps
- Enable or disable user settings in Service Manager Mobile Applications

Data flow

The system architecture includes the following components for the data flow from Service Manager to Service Manager Mobile Applications.



This illustration depicts the flow of Service Manager record data from the Service Manager server to the HP Information Technology Service Management (ITSM) Service Manager Mobile Applications server.

- Service Manager records are stored in the relational database management system (RDBMS).
- The ITSM Service Manager Mobile Applications server synchronizes records from Service Manager into the Mobile Applications cache.

Introduction to installing and configuring Service Manager Mobile Applications

This document provides details on how to install and configure Service Manager Mobile Applications to support your business processes.

As the System Administrator, you must:

- Have already installed Service Manager 9.30 on a web accessible location. For installation information, see the *HP Service Manager 9.30 Interactive Installation Guide.*
- Install the Java Development Kit (JDK).
- Set JAVA_HOME to the location where the JDK was installed.
- Install Service Manager Mobile Applications using the self-contained installer on the HP Service Manager installation DVD.
- Set up an ITSM Service Manager Mobile Applications server to connect with the Service Manager server.
- Review the browser requirements for smartphones.
- Configure Mobile Applications.
- Configure Service Manager.

Install Service Manager Mobile Applications

When you have finished preparing for your installation (see Introduction to installing and configuring Service Manager Mobile Applications), you can install Service Manager Mobile Applications.

Important: Before you start installing Service Manager Mobile Applications, do the following:

- Install a Java Development Kit (JDK).
- Set JAVA_HOME to the location where the JDK was installed.

To install Service Manager Mobile Applications.

1. Insert the Service Manager installation DVD into the applicable drive of the server.
2. **Using the Installation wizard**:
   - Navigate to the DVD directory.
   - Open **ClickMe.html**.
   - Select the Installers tab.
   - Click **Install HP Service Manager Mobility Application**.

     Note: If you are installing on a system that has auto-run enabled, the DVD browser starts automatically. If auto-run is disabled, start the DVD browser manually.
3. If you are using the text-based installer:
   - Open the zip file to manually decompress the zip file.
   - In the InstData folder, select **Windows** or **GenericUnix**.
4. To complete the installation, follow the instructions in the self-contained installer.

Installation considerations

When installing Mobile Applications, consider the following:

- Specify Tomcat ports, or accept the default ports listed:
  - **Tomcat Port**: 8080
  - **Tomcat SSL Port**: 8443
  - **Tomcat Shutdown Port**: 8005

    Important: Be sure these ports are open for incoming and outgoing communications, and that there are no conflicts with other applications running on the same server (for example, if you installed other HP products such as the Web Tier).
- If the Tomcat server is being installed as a Windows Service:
  - Choose 32-bit JVM or 64-bit JVM. The name of the Windows Service is **Apache Tomcat SMmobility**.

    Note: When Tomcat is started as a Windows Service, you have the option to change the Service name. This can be useful if you have more than one instance of Mobile Applications running on the same server (for example, you could rename two separate instances as **SMmobility1** and **SMmobility2**).
  - Run the Tomcat config utility.
    - Stop the Tomcat Windows Service, if it has already started.
    - From a command prompt, go to the bin directory for the Mobile Applications-installed Tomcat.
    - Enter the following command: **tomcat6w //ES//SMmobility**.
      Note:Unix has an equivalent to the Windows Service, which deals with daemons. Instead of entering the command, you can start the service/daemon.

- When Tomcat is not started as a Windows service, do the following:
  - At a command prompt, point to the Tomcat bin folder.
  - Type the following at the command prompt: **catalina run**
    The Tomcat server starts.

Uninstall Service Manager Mobile Applications

You can uninstall Service Manager Mobile Applications as follows:

Windows

1. Go to the Mobile Applications installation directory. For example, the default directory is: C:\Program Files\HP\Service Manager 9.30\
2. Click **Uninstall SM-Mobility.exe**.
3. Choose one of the following:
   - Complete Uninstall
   - Uninstall Specific Features
4. Click **Next**. The uninstaller begins to remove features. When the uninstall is complete, a list of the files that have been removed displays.

Unix

1. Go to the HP root folder (or root folder where you installed Mobile Applications).
   Caution: If you go directly to the Service Manager 9.30 folder and select Uninstall SM-Mobility, not all the files will uninstall properly.
2. At a command prompt, type the following:
   sh ./HP/SM_Mobility/Uninstall SM_Mobility
   The uninstaller is prepared.
3. Choose one of the following:
   - 1-Completely remove
   - 2-Specific features

     The uninstaller begins to remove features. When the uninstall is complete, a list of the files that have been removed displays.

Configure Service Manager Mobile Applications

When you have finished installing Mobile Applications, you need to configure the following in Mobile Applications:

- Configure global settings in the AppConfig.groovy file
- Configure SOAP settings in the CustomConfig.groovy file
- Configure Mobile Applications views in the CustomConfig.groovy file

Note: For information on editing the configuration files, see Edit Service Manager Mobile Applications configuration files.

Edit Service Manager Mobile Applications configuration files

You can configure the Service Manager ITSM Mobile Applications server without setting Service Manager Mobile Applications preferences, but the ITSM Service Manager Mobile Applications server will not accept client connections until you set them.

The settings that you will configure are stored in the sample configuration files stored in the WEB-INF/customConfig file in the web applications directory.

The files you will customize are as follows:

- **AppConfig.groovy**:The settings you customize in the AppConfig.groovy file apply globally.
- **CustomConfig.groovy**: The settings you customize in the CustomConfig.groovy file determine the client preferences for and apply to all Service Manager Mobile Applications users.

IMPORTANT: Before you start customizing settings with your preferences, you need to copy the configuration files to save the original sample files.

Save: **AppConfig.groovy.sample** and **CustomConfig.groovy.sample**
Customize: **AppConfig.groovy** and **CustomConfig.groovy**

To configure the Web Services API and SSL settings.

Notes:

--To exclude settings from the mobile environment, you need to comment out (//) those settings in the newly-created file.
--To include settings that were previously excluded from the mobile environment, you need to un-comment those settings in the newly-created file.

1. Locate the sample configuration files in the following directory:

   WEB-INF/customConfig/AppConfig.groovy.sample
   WEB-INF/customConfig/CustomConfig.groovy.sample

2. Open a blank text (.txt) file and save it in the WEB-INF/customConfig folder with a new name, as follows:

   WEB-INF/customConfig/AppConfig.groovy
   WEB-INF/customConfig/CustomConfig.groovy

3. From the sample files, cut complete sections starting with"itsm." and ending with a semicolon, and then paste these sections into the newly-created files saved in the WEB-INF/customConfig folder.

   Note: You will copy only those blocks of configuration file settings that you want to override with your preferences.

4. Once all the applicable sections are copied and pasted, modify the new files to meet your business needs.

   Note: For information about the configuration file settings, see Configure global settings in the AppConfig.groovy file, Configure SOAP settings in the CustomConfig.groovy file, and

Configure Mobile Applications views in the CustomConfig.groovy file.

An example block of configuration file settings looks like the following:

```
/*
 * Web service connection information settings visible in Server list in UI
(when itsm.soapServerSettingVisible is true)
 * Add or remove rows below as needed, specifying the server URLs and some
appropriate label meaningful to a user.
 * The tag to the left of the :[ can be any unique string and is used when
specifying the default server below.
 */
itsm.soapServers = [

production:[url:'http://localhost:13080',label:'production'],
                test:[url:'http://localhost:13090',label:'test'],
             ];

// default SM soap connection, should reference one of the tags specified
above.
itsm.default.soapServer = itsm.soapServers.production;

//Allow users to see and customize soap settings - set to false to disable
these capabilities
itsm.soapServerSettingVisible = true;
itsm.soapServerAddEnabled = true;
```

5. When you have finished configuring settings, save the configuration files and restart the web application server.

Configure global settings in the AppConfig.groovy file

As the System Administrator, you need to configure the AppConfig.groovy file to customize the global settings, including:

- Security -- SSL settings between Mobile Applications and the browser
- Data source connection pool settings
- SSL between Mobile Applications and Service Manager

For information on editing this file, see Edit Service Manager Mobile Applications configuration files.

Setting	Purpose
Set security - SSL settings between Mobile Applications and the browser	
grails.plugins.springsecurity.secureChannel.definition = itsm.secureChannel.definition.loginOnly	Uncomment this line to enable SSL for login.
grails.plugins.springsecurity.secureChannel.definition = itsm.secureChannel.definition.fullSSL	Uncomment this line to enable SSL for the entire Service Manager Mobile Applications site.
grails.plugins.springsecurity.portMapper.httpPort=8080	Uncomment this line to set this port if yours is different.

Setting	Purpose
grails.plugins.springsecurity.portMapper.httpsPort=8443	Uncomment this line to set this secure port if yours is different.
Security information for configuring SSL between Mobile Applications and Service Manager	
itsm.ssl.enabled	Set to true to enable SSL between the Mobile Applications server and the Service Manager server. To disable, set to **false**.
itsm.ssl.trustStorePath	The absolute path to the trust store where the web server's SSL certificate is stored. **Note**: This string should be quoted. For example: **"c:/certificates/smclient.truststore"**
itsm.ssl.trustStorePassword	The password used by the trust store. **Note**: This string should be quoted. For example: **"changeit"**
itsm.ssl.keyStorePath	The absolute path to the key store where the web server's SSL key is stored. **Note**: This string should be quoted. For example: **"c:/certificates/sm.client.keystore"**
itsm.ssl.keyStorePassword	The password used by the key store. **Note**: This string should be quoted. For example: **"changeit"**
Data source connection pool settings	
itsm.datasource.connections.maxActive	Specifies the maximum number of database connections that can be connected to Service Manager Mobile Applications. If you have a lot of concurrent users, this number should be increased. If you have a minimal number of connections, this number should be decreased.
itsm.datasource.connections.maxIdle	Specifies the maximum number of database connections that can be idle before they are disconnected from the server.

Setting	Purpose
itsm.datasource.connections.minIdle	Specifies the minimum number of database connections that can be idle before they are disconnected from the server.
itsm.datasource.connections.initialSize	Specifies the initial number of database connections that you want connected to Service Manager Mobile Applications.
Datasource statistics logging information	
itsm.datasource.StatsLoggingPeriodSec	Monitors, in the Tomcat log file, how many records, such as, activites (or journal entries), incidents, and change requests are in your in-memory cache. This is an indication of the size of the cache. You can set the period (or frequency) of how often to write to the log. For example, 3600 seconds represents every hour. Setting the value to 0 disables logging.

Configure SOAP settings in the CustomConfig.groovy file

As the System Administrator, you will need to configure the SOAP settings in the CustomConfig.groovy file to:

- Set up the list of supported SOAP servers.
- Define the default SOAP server.

The list of SOAP settings in this configuration file are listed below.

For information on editing this file, see Edit Service Manager Mobile Applications configuration files.

Setting	Purpose
itsm.soapServers	List of supported SOAP servers: production: [url:'http://localhost:13080',label:'production'] test:[url:'http://localhost:13090',label:'test'] . **Note**: You can add other servers to the server list, as needed. **Important**: If you add a new server to this list and expect it to become the default Service Manager server to which Mobile Applications should connect, update the default server value in the **itsm.default.soapServer** setting.
itsm.default.soapServer	Defines the default Service Manager server to

Setting	Purpose
	which Mobile Applications should point. The default server is currently production. However, you can change this setting to meet your needs.
itsm.soapServerSettingVisible	When set to true, the SOAP server setting is visible in the smartphone.
itsm.soapServerAddEnabled	When set to true, the setting to add another SOAP server is enabled.
itsm.soapServerMaxRecordCount	Specifies the maximum number of records to fetch from the SOAP server in a single request. **Caution**: If this number is increased, it could impact performance.
itsm.soapServerResponseTimeMsec	Specifies the SOAP server maximum response time, in milliseconds.(Example: 120000 milliseconds = 120 seconds)

Configure Mobile Applications views in the CustomConfig.groovy file

As the System Administrator, you can configure settings in the CustomConfig.groovy file to customize the mobile environment views for all users. You can:

- Configure what is shown in list and detail views. For both list and detail views, you can specify fields to display, captions for fields, and the sort order for those fields.
- Modify detail views to specify the individual view of a record and how information is displayed for a person, organization, and functional group.
- Change the sort order of lists.
- Change suffixes or captions.
- Add styling.

Notes:

Detail view

- Allows you to change the order of how fields are displayed.
- If you want to add fields that are not currently displayed, uncomment the lines for those fields you want displayed in the Detail view.

List view

- Contains separators between fields for display purposes.
- Allows you to set the sort order for records listed.
- Allows you to place a field (for example, Description) on a new line by setting newline:true.

For information on editing this file, see Edit Service Manager Mobile Applications configuration files.

Setting	Purpose
itsm.detailView.Task	Defines the detail view of task records.
itsm.listView.Task	Defines the order of task records, how fields are sorted, and the sort order of those fields. **Note**: Fields can be sorted in ascending (asc) order or descending (desc) order.
itsm.detailView.Incident	Defines the detail view of an incident record.
itsm.listView.Incident	Defines the list view of incident records.
itsm.detailView.Party	Defines the detail view of the abstract for a person, an organization, and a functional group. **Important**: If the Person and Organization settings are to be different than this setting, then the content of this setting can be copied to either the Person or Organization setting.
itsm.detailView.Person	Defines the detail view of users. **Important**: If this setting is supposed to inherit any changes made to the Party setting, then the Person line containing clone() must be included in the CustomConfig.groovy file.
itsm.detailView.Organization	Defines the detail view of an organization. **Important**: If this setting is supposed to inherit any changes made to the Party setting, then the Organization line containing clone() must be included in the CustomConfig.groovy file.
itsm.listView.FunctionalGroup	Defines the list view of functional work groups.
itsm.listView.ConfigurationItem	Defines the list view of configuration items.
itsm.detailView.JournalEntry	Defines the detail view of an activity (or journal entry).
itsm.listView.JournalEntry	Defines the list view of journal entries (or activities).
itsm.detailView.Change	Defines the detail view of a change record.
itsm.listView.Change	Defines the list view of change records.

Setting	Purpose
itsm.detailView.ChangeSchedule	Defines the detail view of the Change Management schedule.
itsm.detailView.ApprovalSet	Defines a detail view of the approval set of records.
itsm.listView.ApprovalSet	Defines the list view of the approval set of records.
itsm.detailView.Approval	Defines the detail record view of approvals.
itsm.listView.Approval	Defines the list view of approvals.
itsm.detailView.ConfigurationItem	**Warning**: This setting should not be modified.
itsm.detailView.EnumElement	Enumeration elements are equivalent to global lists in Service Manager. **Warning**: This setting should not be modified.
itsm.listView.EnumElement	Enumeration elements are equivalent to global lists in Service Manager. **Warning**: This setting should not be modified.
itsm.detailView.FunctionalGroup	**Warning**: This setting should not be modified.
itsm.enumMaps	Maps the approval status types to one of the three grouping values (approved, denied, and pending). **Warning**: This setting should not be modified.
itsm.errorNotificationEnable	When set to true, error notifications will be sent via email.
itsm.default.errorNotificationEmailAddress	Set the email address where error notifications should be delivered.
itsm.sessionInactiveMaxSec	Specifies the maximum amount of time, in seconds, that the server should remain idle before a user session is logged out due to inactivity. (Example: 1800 seconds = 30 minutes)
itsm.default.loginRememberMeEnabled	When enabled (set to true), users can select "Remember Me" so that their log-in information is auto-filled in the log-in screen, allowing them to go directly to their home page.
itsm.initDemoData	When set to true, you can demonstrate Service Manager Mobile Applications without a connection to Service Manager.

Configure Service Manager

When you have finished installing Mobile Applications, you can configure the following in Service Manager:

- Set up SSL to protect communications between Service Manager Mobile Applications and the Service Manager server
- Add SOAP API capability for user access
- Enable multiple user sessions
- Set up email notifications to include URL links

Set up SSL to protect communications between Service Manager Mobile Applications and the Service Manager server

To protect communications between Service Manager Mobile Applications and the Service Manager server, you need to set up a Secure Sockets Layer (SSL) between Service Manager Mobile Applications and the Service Manager server.

Important: Before you begin to set up SSL, you need to configure the Security - SSL settings in the **AppConfig.groovy** file. For more information, see Configure global settings in the AppConfig.groovy file.

To set up SSL to protect communications, complete the steps in the following sections:

- Part I: Set up SSL between Mobile Applications and the Service Manager server
- Part II: Set up SSL between the browser and Mobile Applications

Part I: Set up SSL between Mobile Applications and the Service Manager server

To set up SSL, do the following:

- A. Set up OpenSSL
- B. Create SSL certificates
- C. Add certificates to the truststores
- D. Configure the sm.ini file
- E. Configure the sm.cfg file
- F. Enable SSL in the configuration (AppConfig.groovy) file
- G.Configure the Service Manager client

A. Set up OpenSSL

1. Download and install an OpenSSL toolkit to implement SSL and TLS protocols with full strength cryptography on your system. To learn about downloading and using the toolkit for Windows, go to the following URL:

http://code.google.com/p/openssl-for-windows/downloads/detail?name=openssl-0.9.8k_WIN32.zip&can=2&q=

2. You can also download and install something like 7-Zip, which is an open source Windows utility for manipulating archives. To learn more about 7-Zip, go to the following URL:

   http://www.google.com/search?hl=en&biw=1042&bih=478&q=7-zip&aq=f&aqi=g5g-s1g4&aql=&oq=

3. Note the directory where the OpenSSL is installed.
4. Go to the root of the OpenSSL directory and open the openssl.cnf file in Wordpad.

   Note: Notepad does not handle the carriage returns in the file properly.

5. Search for the following lines and make sure they are not commented out:

   x509_extensions = user_cert
   x509_extensions = ve_ca
   req_extensions = v3_req

6. Search for the line **[v3_req]** and add the following line in this section:

   Note: Replace **YOUR_IP_HERE** with the IP address of the machine where the client will be running.

   subjectAltName = IP: YOUR_IP_HERE
   For example: subjectAltName = IP:15.178.178.165

B. Create SSL certificates

1. Follow the instructions in the following online Help topic:

   Example: Generating a server certificate with OpenSSL at the following Help server link

2. In step 26 of the Help topic instructions, enter the following command at the DOS prompt (instead of the command specified in the Help topic):

   Note: Replace **[CERTLOCATION]** with the directory where the certificates are being created.

   openssl x509 -req -days 365 -in c:\[CERTLOCATION]\smserver_certrequest.crs -CA c:\[CERTLOCATION]\mycacert.pem -CAkey c:\[CERTLOCATION]\cakey.pem -CAcreateserial -out c:\[CERTLOCATION]\smserver_cert.pem -extfile ../openssl.cnf -extensions v3_req

3. Verify that everything worked by etnering the following command at the DOS prompt:

   Note: Replace **[CERTLOCATION]** with the directory where the certificates are being created.
   openssl x509 -text -noout -in :\[CERTLOCATION]\smserver _cert.pem

   You should see sections marked with **X509v3** extensions with a Subject Alternative Name that has your IP in it. You have created your server certificates.

4. Complete the steps in the online Help topic:
   Example: Generating a server certificate with OpenSSL at the following Help server link
5. Next, follow the instructions in aseparate example online Help topic for generating a client certificate with OpenSSL. The online Help topic is titled:

   Example: Generating a client certificate with OpenSSL
6. In step 13 of the Help topic instructions for *Example: Generating a client certificate with OpenSSL*, enter the following command at the DOS prompt
   (instead of the command specified in the Help topic):

   Note: Replace **[CERTLOCATION]** with the directory where the certificates are being created.

   openssl x509 -req -days 365 -in
   c:\[CERTLOCATION]\smwebtier_certrequest.crs -CA
   c:\[CERTLOCATION]\mycacert.pem -CAkey
   c:\[CERTLOCATION]\cakey.pem -CAcreateserial -out
   c:\[CERTLOCATION]\smwebtier_cert.pem -extfile ../openssl.cnf
   -extensions v3_req
7. Verify that everything worked by entering the following command at the DOS prompt:

   Note: Replace **[CERTLOCATION]** with the directory where the certificates are being created.

   openssl x509 -text -noout -in :\[CERTLOCATION]\swebtier _cert.pem

   You should see sections marked with X509v3 extensions with a Subject Alternative Name that has your IP in it. You have created your client certificates.
8. Complete the steps in the online Help topic:
   Example: Generating a client certificate with OpenSSL

C. Add certificates to the truststores

1. Open a DOS prompt and run the following command:

   cd %JAVA_HOME\bin
2. Run the following commands at your DOS prompt:

   Notes:
   --Replace **[CERTLOCATION]** with the directory where the certificates are being created.
   --Replace **[SERVERALIAS]** with the text that was used to specify the server's alias (for example, smserver).
   --Replace **[CLIENTALIAS]** with the text that was used to specify the client's alias (for example, smclient).

   keytool -export -alias [SERVERALIAS] -keystore c:\[CERTLOCATION]
   servercert.keystore -file c:\[CERTLOCATION]\ smserver.cert

   keytool -import -alias [SERVERALIAS] -file

c:\[CERTLOCATION]\smserver.cert -keystore
c:\[CERTLOCATION]\smserver.truststore

keytool -export -alias [CLIENTALIAS] –keystore
c:\[CERTLOCATION]\clientcerts.keystore -file
c:\[CERTLOCATION]\smclient.cert

keytool -import -alias [CLIENTALIAS] -file
c:\[CERTLOCATION]\smclient.cert -keystore
c:\[CERTLOCATION]\smclient.truststore

keytool -import -alias [CLIENTALIAS] -file c:\[CERTLOCATION]
smclient.cert -keystore c:\[CERTLOCATION]\smserver.truststore

keytool -import -alias [SERVERALIAS] -file
c:\[CERTLOCATION]\smserver.cert -keystore c:\[CERTLOCATION]
smclient.truststore

D. Configure the sm.ini file

1. Add the following lines to the **sm.ini** file located in the RUN directory where the Service Manager server was installed:

   Notes:
   -- In **<keystore password>**, enter the password and leave out the brackets.
   --In **<truststore password>**, enter the password and leave out the brackets.

   # SSL configuration
   keystoreFile:smserver.keystore
   keystorePass:<keystore password>
   truststoreFile:smserver.truststore
   truststorePass:<truststore password>

   Note: For **keystoreFile:smserver.keystore** and **trustoreFile:smserver.truststore**, enter the absolute path.

   For example:
   C:/Program Files/Java/jdk1.6.0_24/bin/servercert.keystore

2. Comment out the following line: sslConnector:0
   For example:
   # sslConnector:0

E. Configure the sm.cfg file

Edit the following line in the sm.cfg file located in the RUN directory where the Service Manager server was installed.

From:
sm -httpPort:13080

To:
sm -httpPort:13080 -httpsPort:13443

F. Enable SSL in the configuration (AppConfig.groovy) file

Edit the following settings in the **AppConfig.groovy** file. For information on editing this file, see Edit Service Manager Mobile Applications configuration files.

- **itsm.ssl.enabled**: Set to true (without quotes) to enable SSL between the Mobile Applications server and the Service Manager server.
- **itsm.ssl.trustStorePath**: Specify the absolute path to the trust store where the web server's SSL certificate is stored. This string should be quoted.
  For example: "c:/certificates/smclient.truststore"
- **itsm.ssl.trustStorePassword**: Specify the password used by the trust store. This string should be quoted. For example: "changeit"
- **itsm.ssl.keyStorePath**: Specify the absolute path to the key store where the web server's SSL key is stored. This string should be quoted.
  For example: "c:/certificates/smclient.keystore"
- **itsm.ssl.keyStorePassword**: Specify the password used by the key store. This string should be quoted. For example: "changeit"

G. Configure the Service Manager client

1. Log onto Service Manager as a System Administrator.
2. Go to **Windows > Preferences**.
3. Type **Security** in the filter.
4. Point everything to the right CA certs file (which is in the security folder of your Java installation).
5. Point to the client keystore and enter the password.
6. Try to connect with SSL enabled.
   a. Go to **File > Connect >Connections...**.
   b. Click on the connection which you are using to connect to your local machine.
   c. Go to the advanced tab and click on **Use SSL Encryption**.
   d. Save your changes.

Part II: Set up SSL between the browser and Mobile Applications

The following steps will set up SSL between the browser and Service Manager Mobile Applications:

A. Generate the keystore file

B. Configure the Apache Tomcat server to use the keystore file

C. Configure your web application to work with SSL

A. Generate the keystore file

1. Open a command prompt in Windows and type the following:
   cd%JAVA_HOME%/bin
   You will land in the Java bin directory.
2. Type the followign command:
   keytool -genkey -alias mobility -keypass admin -keystore mobil.bin -storepass admin

   Note: Notice keypass and storepass should be the same.
   A questionnaire starts.
3. Answer all questions accordingly.
4. Once all the steps are completed successfully, the mobile.bin file is created in the Java bin directory.
5. Copy the mobile.bin file to the webapps directory in the Tomcat server.

B. Configure the Apache Tomcat server to use the keystore file

You will make some changes to the server.xml file inside the Apahce Tomcat server files, so that the Tomcat server knows the path to the keystore to be used.

Note: This was the path set in the configuration file in step G.

1. Inside the Apache Tomcat server files, open the **server.xml** file.
2. Find the connector element which has port ="8443" and uncomment it (if not already done).
3. Add the following lines:

   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\mobile.bin" keystorePass="admin"/>

C. Configure your web application to work with SSL

1. Go to the custom config directory of Mobile Applications.
2. Make a copy of the AppConfig.groovy.sample file and rename it to **AppConfig.groovy**.
3. Uncomment the following line to enable ssl for the Mobile Applications:

grails.plugins.springsecurity.secureChannel.definition = itsm.secureChannel.definition;
Note: Save your changes.

Add SOAP API capability for user access

Capability words provide a security mechanism to control access to Service Manager applications. To grant secure user access to Service Manager Mobile Applications, you can assign the SOAP API capability to user operator records.

To add the SOAP API capability to user operator records:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Search for operator records with user roles that have access to Service Manager Mobile Applications. For example, search for operator records with the change manager user role. A list of operator records displays.
3. Click **Mass Update** and answer **Yes** to proceed with updating all the records in the list.
4. Click **Complex Update**.
5. In the **Instructions for action on EACH RECORD** field, type the following:

   cap.exec in $file=insert(cap.exec in $file, 0, 1, "SOAP API")
6. Click **Execute**. All records in the list will be updated with the SOAP API capability.
7. Repeat these steps for each user role that has access to Service Manager Mobile Applications.

Enable multiple user sessions

The System Administrator can set the number of user sessions for those operators who need to open multiple Mobile Applications user sessions.

To set up multiple user sessions:

1. Click **System Administration > Ongoing Maintenance > Operators**.
2. Find the operator record to be edited.
3. Select the **Security** tab.
4. In the **Max Logins In the User Session Information** section, select **Unlimited Sessions**.
5. Save your changes.

Set up email notifications to include URL links

The System Administrator can set up email notifications to include the mobility URL so that when tickets are assigned, field engineers can receive email notification and click on the URL link to go directly to the assigned ticket.

The System Administrator updates the System Information record so that:

- Field engineers receive an email notification when a ticket is assigned to them.
- Email messages contain a direct URL to the assigned tickets.

Service Manager Mobile Applications automatically synchronizes users' mobile data with information in the Service Manager database. When an email notification is sent to a field engineer, Service Manager Mobile Applications searches for the record by name and then displays it. If the record is not in the cached database, Service Manager will be queried to fetch the record.

To set up email notifications:

1. Restart the ITSM Service Manager Mobile Applications server.
2. Log onto the Service Manager server as a System Administrator.

3. Click **System Administration > Base System Configuration > Miscellaneous > System Information Record**.
4. Select the **Active Integrations** tab.
5. In the **Mobility URL** field, type the fully-qualified URL to your ITSM Service Manager Mobile Applications server. For example:

   ```
   http://myserver.mydomain.com:myport/mobileItsmWebApp/
   ```

   Where you replace the following:

   myserver = server host name

   mydomain.com = domain name of the server running the ITSM Service Manager Mobile Applications

   myport = communications port that your ITSM Service Manager Mobile Applications web server listens to for HTTP requests

   The server stores the value of this field in the **$L.mobility.url** global variable.
6. Save your changes.

Performance tuning

Service Manager Mobile Applications uses an in-memory lazily loaded cache to optimize performance. Objects loaded in the cache are shared by all users connected to the same mobile web application. Therefore, the cache size will grow as users log in, navigate to view incident tickets and change requests, and enter activities (or journal entries). It is possible performance will degrade if the cache grows too large, or if insufficient resources are allocated to the web server's Java Virtual Machine (JVM) instance.

If a noticeable degradation in performance occurs, do the following:

- Restart the web application server hosting Service Manager Mobile Applications.
- If this becomes a recurring issue, increase JVM resources. For information on increasing JVM resources, you can search the knowledgebase in Knowledge Management or visit the HP Software Customer Support web site for a variety of best practice documents and published white papers.

When configured, the logs include statistics indicating the number of records loaded periodically. A typical log entry looks like:

2011-06-07 11:15:55 INFO: DataSourceStatistics - Record counts: User=152, Authorization=17376, FunctionalGroup=294, Person=153, Organization=0, Incident=1376, Change=1707, JournalEntry=5376, ConfigurationItem=4, ApprovalSet=0, Approval=0,


Java™
COMPATIBLE