

HP Service Manager Exchange with SAP Solution Manager

Software Version: 1.10 patch 2

Service Manager Version: 9.x

Installation and Administration Guide

Document Release Date: May 2016
Software Release Date: October 2015



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 Notices

© Copyright 2016 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved. SMSSMEX uses software from the Apache Jakarta Project including Apache Axis2, Apache Tomcat 5.5, Log4j Apache License, and Spring Framework.

Trademark Notices

Java and Oracle® are registered trademarks of Oracle and/or its affiliates.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Itanium® and Pentium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

SAP® is a registered trademark of SAP AG in Germany and in several other countries.

Documentation Updates

This guide's title page 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:

<https://softwaresupport.hp.com>

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

You can visit the HP Software Support Online web site at:

<https://softwaresupport.hp.com>

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

HP Software Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

Introduction	9
Purpose of Document	9
HP Incident Exchange	9
Existing Fragmented Incident Management Workflow	10
SAP Solution Manager Service Desk	10
HP Service Manager	10
Deployment Scenarios	11
High Level Overview	11
Components	11
Installing and Configuring SMSSMEX	13
Installing SMSSMEX	13
Prerequisites	13
Install SMSSMEX	13
Uninstall SMSSMEX	13
SMSSMEX Installed Files	14
Configuring Tomcat	14
Setting up Database	15
Oracle	15
MS-SQL 2008	16
MS-SQL 2012 and 2014	18
Configuring ovictex.properties	18
Configuring File ovictexInternal.properties	19
External Helpdesks	20
Configuring FieldMapping.xml	21
Verifying Configuration	21
Deploying on WebLogic	21
Starting/Stopping SMSSMEX (Tomcat only)	22
Upgrading SMSSMEX V1.10 to V1.10 patch 2	23
Customizing HP Service Manager	25
Importing Customizations Using Unload	25
Core Unload	25
Enabling the Integration	25
Creating a Service Manager User for Web Service	26
Configuring Incident Form (Non-PD Only)	27
Configuring Incident Form (PD Only)	29

Configuring WSDL Mapping	30
Adding Instance in SMIS and Configuring Parameters	31
Configuring SAP Solution Manager	33
Prerequisites	33
Configuring SAP Solution Manager External Service Desk Interface	34
Release Web Service	35
Assign Roles to the Communication User	36
Create HTTP Connection	37
Create a Logical Port	38
Configure Interface to SAP Solution Manager Service Desk	40
Define Value Mapping for the Service Desk Interface	40
Define Extended Interface Mapping for Service Desk	40
Get SAP Solution Manager Service Port	40
Solution Manager Tracing	41
Enable tracing	41
Download Trace File	41
Configuring Security	43
Security between SAP Solution Manager and Tomcat	43
Configure SAP Solution Manager for SSL	43
Checking SAP SSL Configuration	43
Creating a Client PSE in Trust Manager	45
Setting Up an Outgoing Connection in SAP Solution Manager	47
Set up an Incoming Connection in SAP Solution Manager	48
Set up SSL between SAP and SMSSMEX	50
Create Keystore and Truststore	50
Configure Tomcat SSL Use	51
Configure Property Files	51
Security Between HP Service Manager and SMSSMEX	53
Configure HP Service Manager for SSL	53
Configure SMSSMEX for SSL Communication with Service Manager	53
Licensing	55
License Types	55
License Management	55
Status Page	57
Troubleshooting	59
checker.bat and encryptPasswords.bat Fail	59
Incident not Sent to SAP AGS	59
java.lang.OutOfMemoryError	59
Record in EventIn is not Executed	60
Incident Update or Process Action Fails	62
Information is not Updated in SAP Solution Manager	64
Incident Exchange Details	65
Database Tables	65

Tools	66
Field Mapping Configuration	67
Types of Mapping	67
Structure of FieldMapping XML file	67
Composite Field Mapping	68
Field Value Mapping	69
Field Mapping Schema	69
Default Field Mapping File and Customization	72
Prerequisites	72
Adding Fields to fieldMapping.xml	73
Additional Information	74
Changeable Mappings	76
Person Synchronization Details	76
SAP Solution Manager to Service Manager	76
SMSSMEX Version	77
Installing and Configuring SAPCRYPLIB	79
Logging	81
Deploying Button Icons	83
Windows Client	83
Web Client	83
SAP System Landscape Directory Registration	85
Prerequisites	85
Registering System Landscape Directory	85

1 Introduction

This HP integration product implements HP Service Manager Exchange with SAP Solution Manager. This version only implements Service Manager Incident Exchange with SAP Solution Manager. Therefore, you can refer to this document for HP Incident Exchange.

Purpose of Document

This document describes installation, configuration, administration and maintenance of HP Incident Exchange and the HP Incident Exchange web service. This document is not an end user document. Instead, this guide is intended for use by HP consultants and application administrators that install and maintain HP Incident Exchange. HP strongly recommends you to read this manual carefully before installation and follow the instructions herein because SMSSMEX 1.10 patch 2 significantly differs from the previous releases.

HP Incident Exchange

Businesses today increasingly rely on their mission-critical SAP applications. Disruptions in the SAP environment have a severe business impact. Keeping the system continuously available has never been more vital for success. In any SAP landscape, business process disruptions caused by an application or infrastructure incident must be proactively prevented. If disruptions do occur, they need to be quickly and efficiently resolved. HP and SAP have teamed up to solve this issue.

Incident management in enterprises today consists of disconnected incident management systems that often implement divergent processes. This situation diminishes collaboration within IT operations, lowers quality of service and productivity.

The integration of SAP Solution Manager Service Desk with HP Service Manager provides a cohesive Incident and Service Request Management solution for the entire enterprise, resulting in higher enterprise availability, improved service quality and reduced IT costs.

HP Incident Exchange builds a dynamic link between HP Service Manager Software and SAP Solution Manager Service Desk and improves the Incident and Service Request Management Process throughout the entire enterprise. HP Incident Exchange offers dynamic integration between HP Service Manager and SAP Solution Manager Service Desk for improved incident workflow.

The interface to exchange support messages between HP Service Manager and SAP Solution Manager Service Desk was designed and developed jointly by HP and SAP and is certified by SAP.

Existing Fragmented Incident Management Workflow

Performance monitoring of an SAP environment must include SAP and non-SAP applications.

SAP Solution Manager Service Desk

To monitor and manage SAP environments, IT operations management uses the SAP Solution Manager Service Desk to collect information about SAP systems and serves as an internal help desk for SAP installations. Users and administrators can create support messages from any SAP system. The messages are processed centrally in the Solution Manager Service Desk.

If the support message involves an SAP application, a solution may be available in the SAP Service Marketplace or from SAP Active Global Support or from the in-house SAP support team. But if the issue is not caused by the SAP application, the message will be forwarded to the administrators responsible for the non-SAP systems. The support call needs to be entered in a second or third service desk and tracked until resolved. In the meantime, the SAP Service Desk team waits for feedback before closing the call and informing the originator, who is temporarily left “in the dark”.

HP Service Manager

An incident can also be reported to the service desks monitoring non-SAP applications and infrastructure hardware and software. Many SAP customers have integrated these tasks in the HP Service Manager, which is able to support nearly all IT application and infrastructure components.

If a support call, for example, pertains to a “printing issue from an SAP application” and the HP Service Manager team detects no issue with the printer hardware or software, the call will be forwarded to the SAP service desk team to check whether it is related to the SAP application. Again the service call must be re-entered in a service desk, in this case in the SAP Solution Manager Service Desk. Additional information or attachments regarding the error or error resolution must be forwarded manually. The HP Service Manager team has to wait for feedback before informing the requesting user and closing the call.

In both cases the disconnected service desks and the fragmented incident management workflow impede the service desk team’s ability to resolve problems. Disadvantages of this non-integrated workflow are

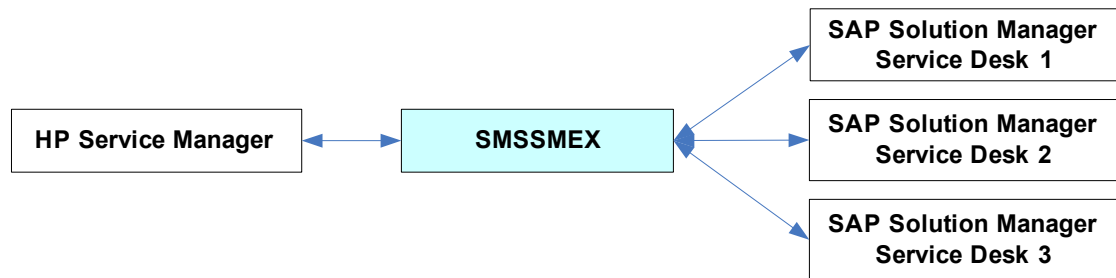
- Only limited and often inconsistent information about the incident is available.
- It is difficult to monitor, track and report incidents or to work together toward resolution.
- Manual workarounds are required for the handover of incidents between the SAP and non-SAP service desks and for information updates.
- There is insufficient synchronization. The same incident may get reported, recorded and tracked in separate service desks, or the incidents may get lost or ‘dropped’.
- Expertise about the interrelationships of SAP applications with non-SAP applications and other IT components is lost.

This results in productivity loss and reduced quality of service.

2 Deployment Scenarios

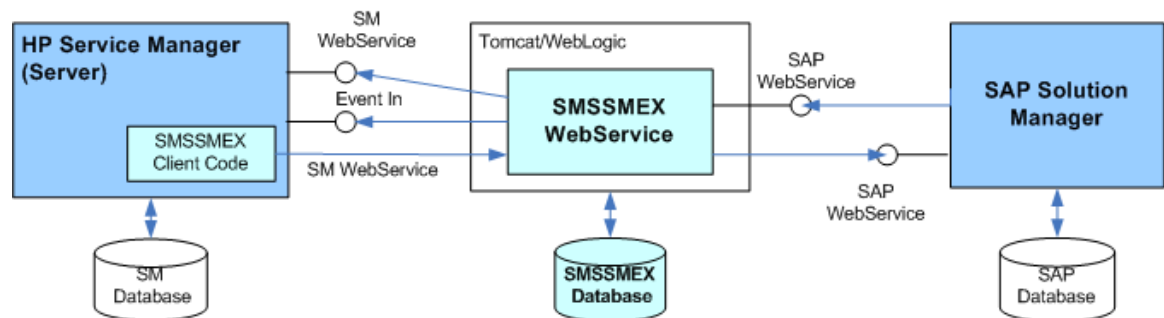
High Level Overview

SMSSMEX integrates a single Service Manager server with multiple external helpdesk systems.



Components

The following diagram shows the component details.



- HP Service Manager Server is the HP service desk system.
- Service Manager DB provides persistent storage for HP Service Manager.
- SMSSMEX Client Code consists of RAD and Java scripts, table definitions and GUI formats. The SMSSMEX webservices are called from this client code.
- WebServer is a Tomcat Web Application Server or WebLogic Application Server that hosts the SMSSMEX WebService (deployed as a .war file).
- SMSSMEX WebService exposes the incident webservice of HP Service Manager in the SAP format and transfers client requests to SAP Solution Manager webservices.
- SMSSMEX Database provides persistent storage for the SMSSMEX WebService.
- SAP Solution Manager is the Service Desk.

3 Installing and Configuring SMSSMEX

Installing SMSSMEX

The HP Service Manager Exchange with SAP Solution Manager product DVD includes an autorun program for installation.



Some installation and configuration steps are required only for Tomcat or for WebLogic, whereas some are required for both. Unless otherwise noted in the step heading, a step is required for both.

Prerequisites

It is NOT recommended to install SMSSMEX and Service Manager on the same server.

Install SMSSMEX

- 1 Log in to the operation system as a super user.
- 2 The installer is in:
 - <SMSSMEX1.10p2 Release Package>\InstData\Windows\install.exe (Windows Server 2008 and 2012)
 - <SMSSMEX1.10p2 Release Package>\InstData\Linux\install.bin (Linux)
- 3 Run install.bin or install.exe. The Introduction dialog appears.
- 4 Click **Next**. The license agreement appears.
- 5 Select **I Accept the terms of License Agreement**.
- 6 Click **Next**. The Choose Install Folder page displays. For example, the default installation folder on Windows Server 2012 is C:\Program Files (X86)\HP\SMSSMEX.
- 7 Click **Next**. Review the summary information.
- 8 Click **Install**. The files are installed.
The Install Complete dialog appears.
- 9 Click **Done** to close the installer.

Uninstall SMSSMEX

To uninstall SMSSMEX on Windows, execute <SMSSMEX_installDir>\Uninstall SMSSMEX\Uninstall SMSSMEX.exe.

Or simply go to **Start** → **Programs** → **SMSSMEX** → **Uninstall SMSSMEX**.

To uninstall SMSSMEX on Unix, execute `<SMSSMEX_installDir>/Uninstall SMSSMEX/Uninstall_SMSSMEX`.

SMSSMEX Installed Files

After installation, the SMSSMEX folder has the following contents.

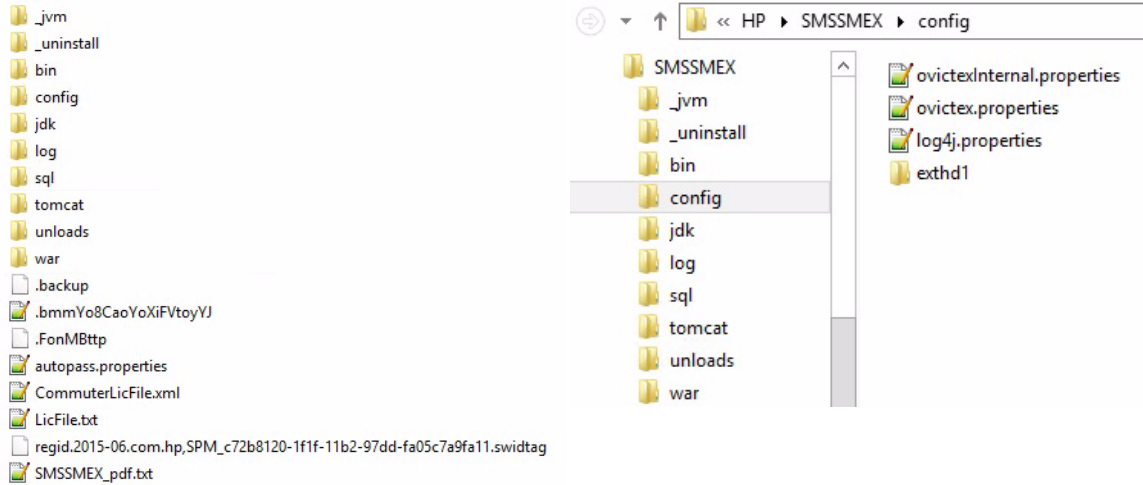


Table 1 Contents of \SMSSMEX

Directory	Content
bin	Executable commands and product description file
config	Web service configuration files The config\exthd1 folder stores the template for an external helpdesk configuration
sql	Database table creation/deletion scripts
unloads	Service Manager customization unload files
log	Log files
jdk	Internal JDK 8
tomcat	Tomcat 7.0.62
Uninstall SMSSMEX	Executable file for uninstallation

Configuring Tomcat

The connector for deploying the web service must be enabled. Uncomment the port specification in `<SMSSMEX_installDir>\tomcat\conf\server.xml`. For example:

```
<Connector port="8080"
  redirectPort="8443"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

```
enableLookups="false" acceptCount="100" debug="0"  
connectionTimeout="20000" disableUploadTimeout="true" />
```

You can modify the ports if necessary.

Setting up Database

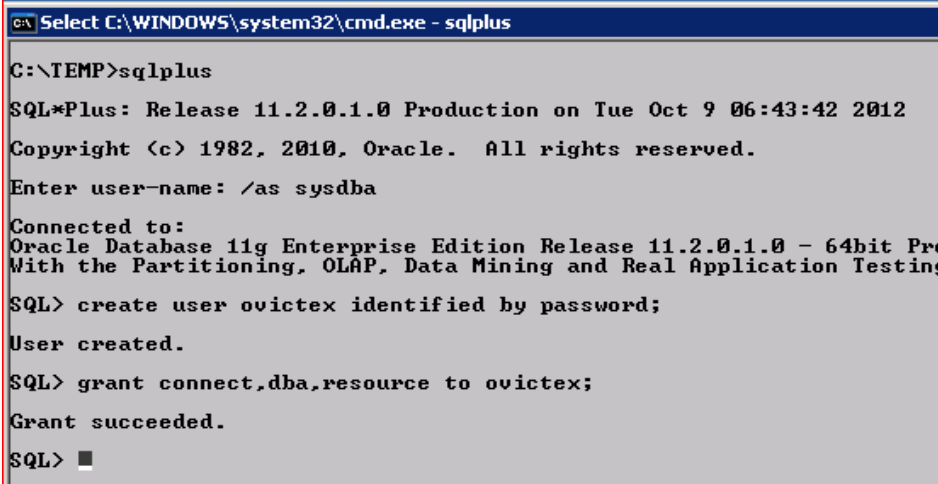
This section describes how to setup the database.

- ▶ The SMSSMEX web service uses a database to store metadata. The SMSSMEX web service must be able to read table `v$database` (Oracle) or execute function `SERVERPROPERTY('ProductVersion')` (SQLServer). These system tables are queried when validating the database connections.

Oracle

To setup the Oracle database do the following:

- 1 Create a user.



```
cx Select C:\WINDOWS\system32\cmd.exe - sqlplus  
C:\TEMP>sqlplus  
SQL*Plus: Release 11.2.0.1.0 Production on Tue Oct 9 06:43:42 2012  
Copyright (c) 1982, 2010, Oracle. All rights reserved.  
Enter user-name: /as sysdba  
Connected to:  
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Pro  
With the Partitioning, OLAP, Data Mining and Real Application Testin  
SQL> create user ovictex identified by password;  
User created.  
SQL> grant connect,dba,resource to ovictex;  
Grant succeeded.  
SQL> ■
```

- 2 Give the user the right to do a select on table `v$database`. This system table is queried by the SMSSMEX web service to validate database connections.

- 3 Login as the user and run the script create_tables_oracle.sql (log in from path <SMSSMEX_installDir>\sql so that the script is found). This creates all required tables.

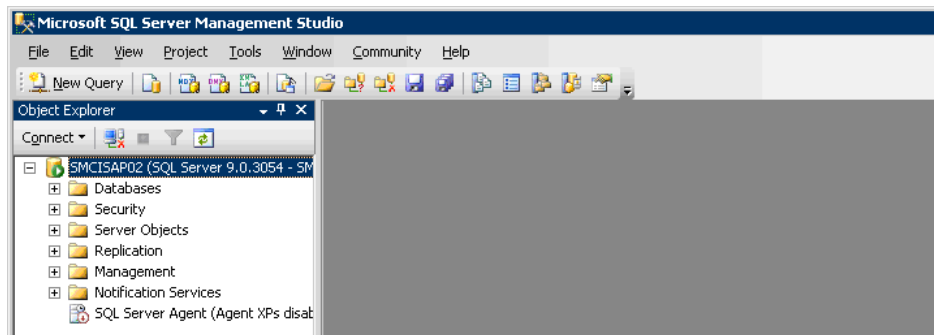
```
C:\WINDOWS\system32\cmd.exe - sqlplus
C:\TEMP>sqlplus
SQL*Plus: Release 11.2.0.1.0 Production on Tue Oct 9 06:51:04 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.
Enter user-name: ovictex
Enter password:
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing
SQL> @create_tables_oracle
Table created.
Table created.
Table created.
Table created.
Table created.
SQL> _
```

These tables are created within the schema of the database user (the tables are logically separated and do not interfere with each other).

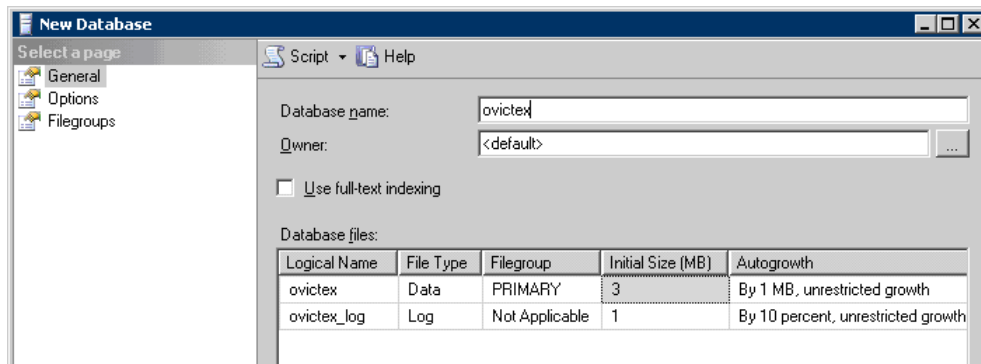
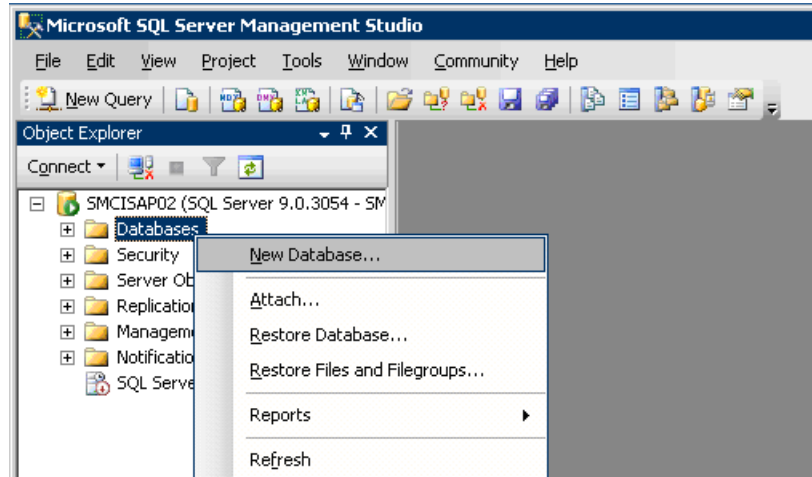
MS-SQL 2008

Do the following to create the required separate database for SMSSMEX tables:

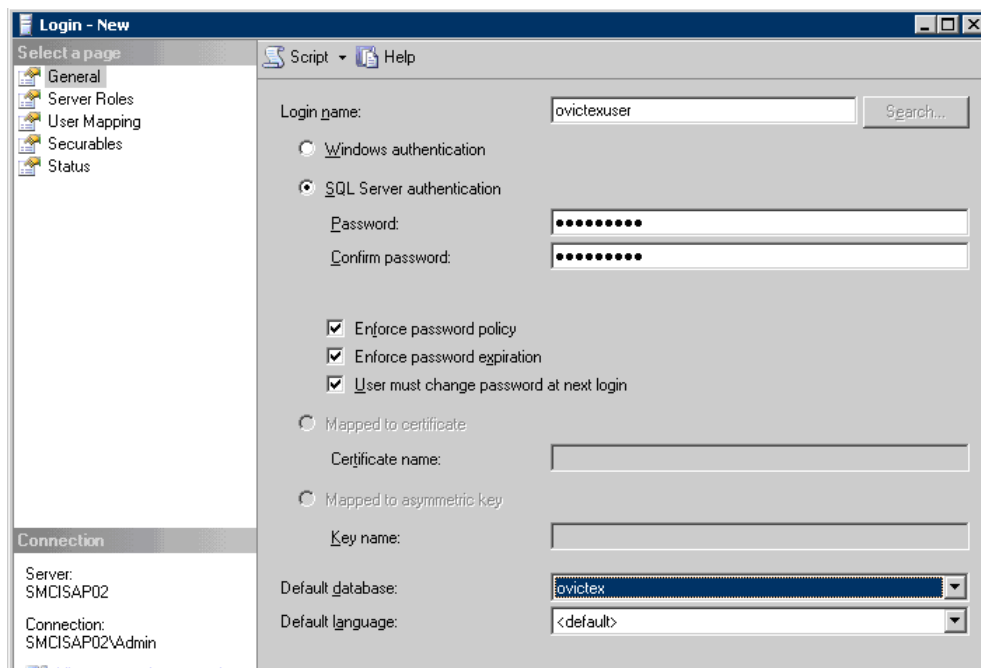
- 1 Launch SQL Server Management Studio.

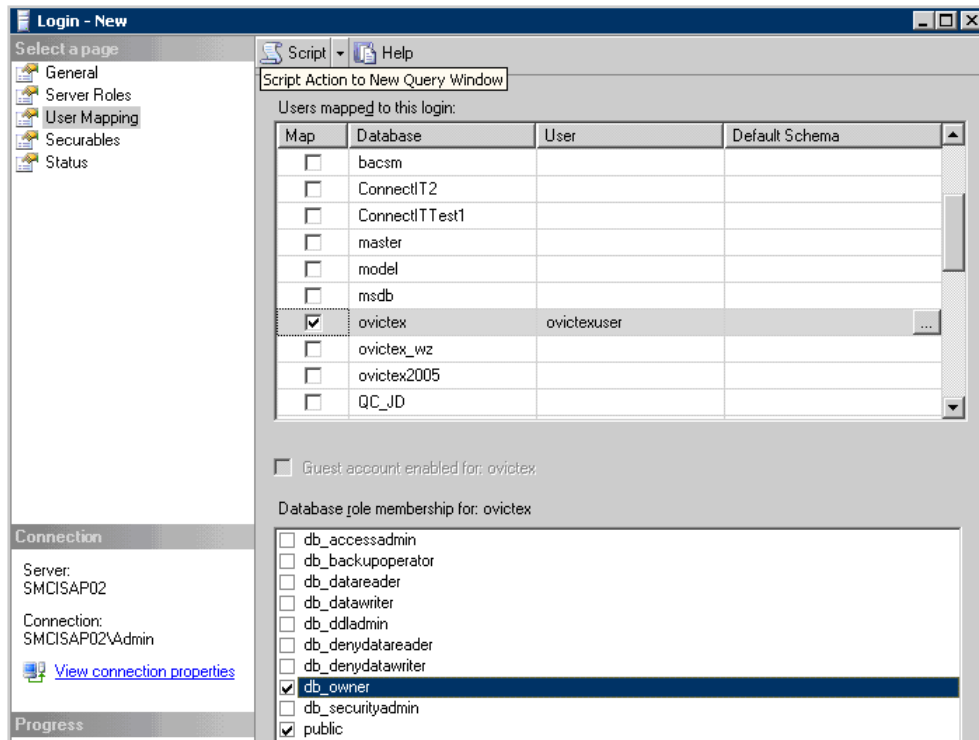


- 2 Create a new database (ovictex). Right-click on **Databases** and choose **New Database**.



- 3 Create a database user (ovictexuser) with permission for database ovictex. Right-click on **Security/Login** and select **New Login**.





- 4 Create the SMSSMEX tables.
 - a Click **New Query** on the toolbar and select database **ovictex**.
 - b Copy and execute the SQL scripts under folder `<SMSSMEX_installDir>\sql\create_tables_sqlserver.sql`.

MS-SQL 2012 and 2014

The DB setup for MS-SQL 2012 and 2014 is similar to the MS-SQL 2008 setup. Refer to *MS-SQL 2008* on page 16 for detail information.

Configuring ovictex.properties

File `<SMSSMEX_installDir>/config/ovictex.properties` must specify the local helpdesk installation. The file comments describe how to do this.



To configure the passwords, use command line application `<SMSSMEX_installDir>/bin/encryptPasswords.bat | sh` (do not enter the password directly in the file; passwords are stored in encrypted format). There are several sensitive fields that must be encrypted. These fields are discussed below. For more information about using `encryptPasswords.bat | sh`, see *Tools* on page 66.

The following parameters must be configured:

- Service Manager web service endpoint

- To connect to a Service Manager:

```
sc.webservice.endpoint = http://<ServiceManager host>:<Port>/
sc62server/PWS
```

- To connect to a ServiceCenter:

```
sc.webservice.endpoint = http://<ServiceCenter host>:<Port>/sc62server/ws
```

- The following are required parameters:

```
sc.user=<web service endpoint access user name>
sc.password=<encrypted password>
```

► `sc.password` must be filled by `encryptPasswords.bat | sh`. SMSSMEX supports SSL connections to Service Manager, but the parameter values are different than above and additional parameters must be set (see *Security between SAP Solution Manager and Tomcat* on page 43).

- SMSSMEX database configuration information:

```
ovictex.db.type= <oracle | sqlserver>
ovictex.db.host=<database server address>
ovictex.db.port=<database server port number>
ovictex.db.instance=<sqlserver database server instance>
ovictex.db.name=<database name or oracle DB SID>
ovictex.db.user=<database user name>
ovictex.db.password=<database password>
```

► `ovictex.properties` contains examples. `ovictex.db.password` must be filled by `encryptPasswords.bat | sh`.

- One or more External Helpdesk instance names.
 - Parameters are `exthd.instances.id.<number>`, where `<number>` is a number {1,...,n}.
 - First number must be 1 and each number must be greater than the previous.
 - `ExtHdInstanceName` differentiates multiple External Helpdesks and is the name of the subfolder in `<SMSSMEX_installDir>/config` and the `ExtHd` configuration file.
- Incident category in Service Manager.
- Property `ovhd.incident.informationlog.entry.separator` should be configured to a unique value that is not contained in messages exchanged between Helpdesks. By default it is configured to “----”. Service Manager must be configured to use this separator to append information to the Journal. If this separator is contained in a message then duplicate information could be sent to the external Helpdesk (no data is lost).

Configuring File `ovictexInternal.properties`

The property file for internal configurations is in the `<SMSSMEX_installDir>/config` directory of the SMSSMEX installation. There is typically no need to configure this file.

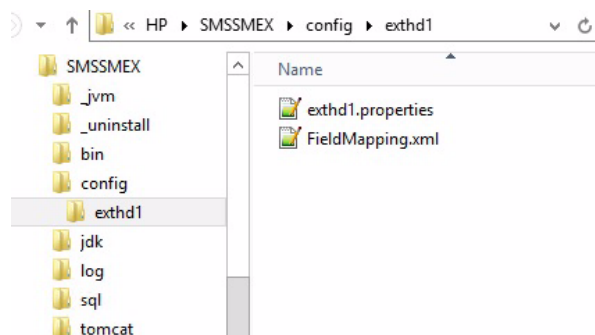
External Helpdesks

Main configuration file `<SMSSMEX_installDir>/config/ovictex.properties` must define all External Helpdesk Instances. For example:

- `exthd.instances.id.1 = exthd1`
- `exthd.instances.id.2 = SAP_exthd2`
- `exthd.instances.id.3 = NY200BM`

Each external helpdesk has the following configuration files:

- `<ExtHdInstanceName>.properties`
- `FieldMapping.xml`



- ▶ The same names (such as `exthd1`, `SAP_exthd2`, `NY200BM`) must be used for the names of subfolders with specific configuration file names. The names must not contain spaces or special characters. The default configuration comes with a defined `exthd1` sample External Helpdesk configuration.

To create a new instance:

- 1 Add a new line in the `ovictex.properties` file for the new `ExtHd`.
`exthd.instances.id.2 = exthd2`
- 2 Create the new subfolder `<SMSSMEX_installDir>/config/exthd2`.
- 3 Copy the configuration files for `exthd1` to `exthd2`.
- 4 Rename `<SMSSMEX_installDir>/config/exthd2/exthd1.properties` to `<SMSSMEX_installDir>/config/exthd2/exthd2.properties`.
- 5 Make the required changes to the new files.
- 6 The following parameters must be configured in `<ExtHdInstanceName>.properties`:
`exthd.webservice.endpoint = http://<SolutionManager host>:<Port>/sap/bc/srt/rfc/sap/ICT_SERVICE_DESK_API?SAP-CLIENT=<SAP client number>`
`exthd.webservice.authentication.scheme = BASIC`
`exthd.webservice.authentication.username = <SAP client user name>`
`exthd.webservice.authentication.password = <encrypted SAP client user password>`

IMG activity guides you to SAP transaction `/nsmicm`. Select the activity in menu **Goto** → **Services**.

ICM Monitor - Service Display

Active Services							
No.	Log	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind
<input type="checkbox"/>	1	HTTP 8003	gmmorra.deu.hp.com	30	60	✓	
<input type="checkbox"/>	2	HTTPS 8001	gomorra.deu.hp.com	30	60	✓	

This transaction shows the host and port for access to the SAP Solution Manager Service Desk web service. Specify the host/port in `<ExtHdInstanceName>.properties` as the endpoint entry.

▶ `exthd.webservice.authentication.password` must be filled by `encryptPasswords.bat | sh`.

Configuring FieldMapping.xml

The files `<SMSSMEX_installDir>/config/<ExtHdInstanceName>/FieldMapping.xml` must be adjusted to send/receive special/customized fields to/from the external Helpdesk. For detailed information see *Field Mapping Configuration* on page 67.

Verifying Configuration

Verify the configuration with the checker tool before trying to exchange incidents between Service Manager and SAP Solution Manager. The checker error messages are much more helpful for troubleshooting than Service Manager and Solution Manager error messages.

To execute the checker, run the following command:

```
<SMSSMEX_installDir>/bin/checker.bat | sh
```

Checker checks the environment, database and HTTP connections and configuration of Service Manager. No incidents are exchanged. The following are the possible results:

- OK
- ERROR (partial failure; checks that the check depends on have failed)
- FAIL (with troubleshooting recommendations)

You can re-run a check by passing the number of the check to the executable. You can also examine the Incident Exchange log messages or run a trace. For more information about using `checker.bat | sh`, see *Tools* on page 66.

Deploying on WebLogic

- 1 Before starting the WebLogic server, set an environment variable named "SMSSMEX_HOME" to the pathname where this application is installed.

For example, if the WebLogic server is installed in the /opt/HP/SMSSMEX directory, set the environment variable to the following:

```
$ export SMSSMEX_HOME=/opt/HP/SMSSMEX
```

- 2 Start the WebLogic server and launch the WebLogic administration console.
- 3 Deploy the ovictex.war file in the /opt/HP/SMSSMEX/war directory. See the following steps for an example:
 - a Select **Domain Structure > Deployments** and click **Install**.
 - b Use the Install Application Assistant to locate the ovictex.war file.
 - c Select **Install this deployment as an application** and click **Next** until last step.
 - d Click **Finish** to exit the installation wizard.

For advanced configuration, refer to *BEA WebLogic Server Administration Console Online Help* for more information.



HP recommends you to deploy SMSSMEX on WebLogic 12 or later because there is a known issue QCCR1E128427 for WebLogic 11(version: 10.3.6.0).

Starting/Stopping SMSSMEX (Tomcat only)

Starting from Windows:

```
<SMSSMEX_installdir>\bin\setup startup
```

Stopping from Windows:

```
<SMSSMEX_installdir>\bin\setup shutdown
```

Starting from Linux:

```
<SMSSMEX_installdir>/bin/setup.sh startup
```

Stopping from Linux:

```
<SMSSMEX_installdir>/bin/setup.sh shutdown
```

4 Upgrading SMSSMEX V1.10 to V1.10 patch 2

Follow these steps to upgrade SMSSMEX v1.10 to v1.10 patch 2 on Tomcat:

- 1 Stop SMSSMEX v1.10.
- 2 Back up the following configuration files:
 - All files in the <SMSSMEX_installDir>\config folder.
 - (Optional) The <SMSSMEX_installDir>\tomcat\conf\server.xml file.

▶ If you have not customized the Tomcat configurations, skip this step.

 - Other configuration files which have been customized.
- 3 Backup the database.
- 4 Uninstall SMSSMEX v1.10.
- 5 (Optional) Uninstall HP OpenView Autopass if it is used by SMSSMEX only. Otherwise, if another HP product on this computer also use Autopass for license management, do not uninstall Autopass.
- 6 Install SMSSMEX v1.10 patch 2.
- 7 Configure SMSSMEX v1.10 patch 2.

You can copy parameter values from the backup configuration files to configure SMSSMEX v1.10 patch 2. Do not just copy and replace `ovictex.properties` and `FieldMapping.xml` because these files have been updated in SMSSMEX v1.10 patch 2.

Some differences between the configuration files in SMSSMEX v1.10 and v1.10 patch 2 are listed as follows:

- SMSSMEX v1.10 patch 2 adds the following codes to the `ovictex.properties` file:

```
# default category
ovhd.incident.default.category = incident
```

- SMSSMEX v1.10 patch 2 introduces the following code changes to the FieldMapping.xml file:

v1.10	v1.10 patch 2
<pre><FieldMapping ExtHDFField="IctHead/AgentId"> <OutOvHDFField>AssigneeName</OutOvHDFField> <OutDataType>Person</OutDataType> <InOvHDFField>AssigneeName</InOvHDFField> <InDataType>Person</InDataType> </FieldMapping></pre>	<pre><FieldMapping ExtHDFField="IctHead/AgentId"> <OutOvHDFField>Assignee</OutOvHDFField> <OutDataType>Person</OutDataType> <InOvHDFField>Assignee</InOvHDFField> <InDataType>Person</InDataType> </FieldMapping></pre>
<pre><FieldMapping ExtHDFField="IctHead/ShortDescription"> <OutOvHDFField>BriefDescription</OutOvHDFField> <InOvHDFField>BriefDescription</InOvHDFField> </FieldMapping></pre>	<pre><FieldMapping ExtHDFField="IctHead/ShortDescription"> <OutOvHDFField>Title</OutOvHDFField> <InOvHDFField>Title</InOvHDFField> </FieldMapping></pre>
<pre><FieldMappingExtHDFField="IctIncidentStatement/Text"> <OutOvHDFField>Resolution</OutOvHDFField> <InOvHDFField>Resolution</InOvHDFField> <KeyFieldOutVal>SU99</KeyFieldOutVal> <KeyFieldInVal>SU01</KeyFieldInVal> </FieldMapping></pre>	<pre><FieldMapping ExtHDFField="IctIncidentStatement/Text"> <OutOvHDFField>Solution</OutOvHDFField> <InOvHDFField>Solution</InOvHDFField> <KeyFieldOutVal>SU99</KeyFieldOutVal> <KeyFieldInVal>SU01</KeyFieldInVal> </FieldMapping></pre>

- 8 Manage the license. See *License Management* on page 55.
- 9 Start SMSSMEX v1.10 patch 2.

5 Customizing HP Service Manager

This chapter describes the customization required for HP Service Manager for the SAP Solution Manager integration.



Some configuration topics are required only for PD environment or for non-PD environment, whereas some are required for both. Unless otherwise noted in the step heading, a topic is required for both.

Importing Customizations Using Unload

This section describes how to configure Service Manager using unload. Additional customization of Service Manager is later required for the integration.

Core Unload

Unloads are used to transfer customizations from one Service Manager installation to another Service Manager installation. The Incident Exchange provides core unloads in <SMSSMEX1.10p2 Release Package>\unloads\SM9.34-9.4x\core.unl for Service Manager 9.34, 9.35, and 9.4x.

This unload contains new Service Manager records that are unique to Incident Exchange and do not override any existing Service Manager records.

To import the unload do the following:

- 1 In the Service Manager client select **Tailoring** → **Database Manager**.
- 2 Select **Import/Load** from the menu.
- 3 Select <SMSSMEX1.10p2 Release Package>\unloads\SM9.34-9.4x\core.unl for Service Manager 9.34, 9.35, and 9.4x.
- 4 Click **Load FG** to start the import.

Enabling the Integration

Follow these steps to enable the HP Service Manager integration with SAP Solution Manager:

- 1 Log on to Service Manager Windows client as a system administrator.
- 2 Type `s1` in the Service Manager command line field, and then press **Enter**.
- 3 Type `SMSAP_Enable` in the Name field, and then click **Search**.
- 4 (Optional) Locate the following codes:

```

var incidentCategory = "incident";
var isCustomizeSMFormat = true;
var isGenerateIntegrationDemoData = true;
var isGenerateIntegrationDemoUser = true;

```

You can update the values as follows:

- The value of `incidentCategory` must be consistent with that in the `ovictex.properties` file.
 - When setting `isCustomizeSMFormat` to `true`, the integration enablement script customizes the Service Manager forms and you can skip the steps as described in [Configuring Incident Form \(Non-PD Only\)](#) on page 27 and [Configuring Incident Form \(PD Only\)](#) on page 29.
 - When setting `isGenerateIntegrationDemoData` to `true`, the integration enablement script generates the `sapinstance200` CI and the `sapinstance300` CI, and two CI relationships, respectively.
 - When setting `isGenerateIntegrationDemoUser` to `true`, the integration enablement script creates an operator named `ovictex` with the password of `Ovictex123`. You can skip the steps as described in [Creating a Service Manager User for Web Service](#) on page 26.
- 5 Click **Execute**. When the process is completed, the **enable SM SAP integration done!** message is displayed in the Messages tab.
 - 6 Log out and log in again for the configuration to take effect.



In PD environment, the integration enablement script creates a new workflow named Incident for SAP, and adds necessary rulesets, actions and transitions.


Creating a Service Manager User for Web Service

Incident Exchange uses one Service Manager user to connect to Service Manager web services. The user and the user role should be dedicated for the integration. The user requires the following permissions:

The screenshot shows the configuration for a user role named 'OVICTEX'. The description is 'Automated Incident Exchange user role'. Under the 'Profiles' tab, the following profiles are assigned to 'SYSADMIN':

- Service Profile: SYSADMIN
- Incident Profile: SYSADMIN
- Problem Profile: SYSADMIN
- Configuration Profile: SYSADMIN
- Contract Profile: SYSADMIN
- SLA Profile: SYSADMIN
- Change Profiles: SYSADMIN
- Request Profiles: SYSADMIN

Do the following:

- 1 Log in to Service Manager with a System Administrator account.
- 2 Select **System Administration** → **Ongoing Maintenance** → **User Roles**.
- 3 Search for **system administrator** on Service Manager 9.x and above.
 -  In case your database is configured to case sensitive, try to use all lowercase search keyword instead of all UPPERCASE one, or vice versa.
- 4 Enter **OVICTEX** as the User Role.
- 5 Change Description to **Automated Incident Exchange user role**.
- 6 Click **Add**.
- 7 Select **System Administration** → **Ongoing Maintenance** → **User Quick Add Utility**.
- 8 Enter **ovictex, INCIDENT EXCHANGE, Incident, Exchange, ovictex@hp.com**.
- 9 Click **Next**.
- 10 For **User to clone** select **falcon**.
- 11 Click **Finish**.
- 12 Click **Save**.
- 13 Go to **System Administration** → **Ongoing Maintenance** → **Operators**, enter **ovictex** in the Login Name field, then click **Search**.
- 14 Change User Role to **OVICTEX**.
- 15 In the Security tab:
 - a Enter the operator password for Password.
 - b Uncheck Expire Password.
 - c Check Never Expire Password.
- 16 Click **Save**.

Configuring Incident Form (Non-PD Only)

Incident Exchange must be integrated into the incident management workflow. The operator working on the incident must be able to control and trigger Incident Exchange. If more than one external helpdesk is connected to Service Manager, then the target system must be selected.



If you are working with SM 9.40 Classic, you must apply the QCCR1E127035_SM940_SM940.unl unload file to fix QCCR1E127035. The unload file is available in the %SMSSMEX_HOME%\unloads\SM9.34-9.4x directory.

Follow these steps to configure incident forms in non-PD environment:

- 1 Open all Incident Forms that are parts of the Incident workflow.
 - IM.open.incident
 - IM.update.incident
 - IM.close.incident

2 Embed the created subform on the Incident form in a new Notebook tab (or in a new section on Service Manager 9.2x and above).

3 Add a Notebook tab or section to the following forms:

IM.open.incident

IM.update.incident

IM.close.incident

Property	Value
Caption	Sap Solution Manager
Visible condition	[\$SMSAP]=true

4 add a subform control to the SAP Solution Manager tab or section.

Property	Value
X	1
Y	0
Width	151
Height	28
Format	hp.sap.solution.sub

▼ Sap Solution Manager

SAP Solution Manager

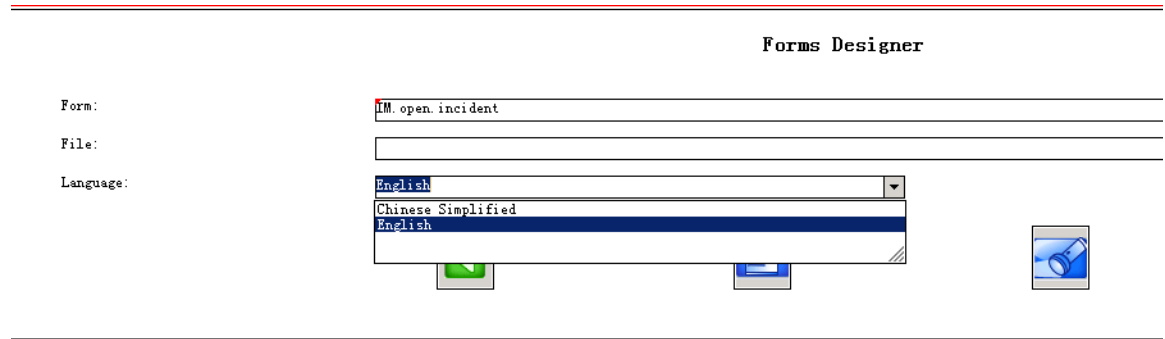
Exchange Status

Date	Update
10/24/15 04:27:03	Created incident in External Helpdesk :SAP Solution Manager. Incident Id at External Helpdesk is 8000001268. External Helpdesk is now processing the incident IM10214
10/24/15 04:35:55	Incident : IM10214 has been closed in the External Helpdesk: SAP Solution Manager



If multiple Language packs are applied to HP Service Manager, do the following to update the incident related forms for other languages.

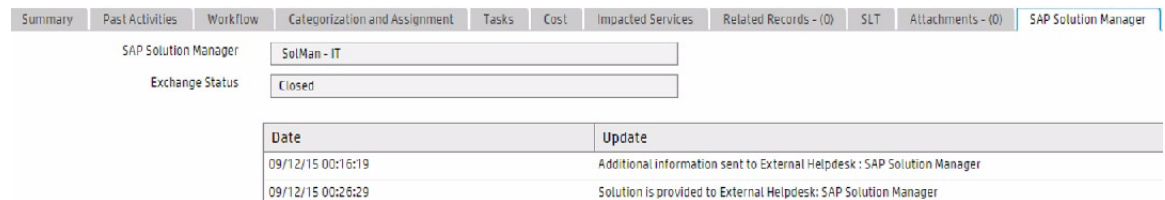
- 1 Copy the `hp.sap.solution.sub` form from English to other languages and perform translation.
- 2 Repeat aforementioned [step 3](#) and [step 4](#) for `IM.open.incident`, `IM.update.incident` and `IM.close incident` for other languages.



Configuring Incident Form (PD Only)

To configure the incident form in PD environment, follow these steps to add a SAP Solution Manager tab for the following formats:

- `im.incident.categorization`
- `im.incident.investigation`
- `im.incident.recovery`
- `im.incident.review`
- `im.incident.closure`





If you are working with either SM 9.40 Codeless or SM 9.41 Hybrid, pay attention to the following items before adding add SAP Solution Manager tabs for various incident formats.

- If you are working with SM 9.40 Codeless, you must apply the QCCR1E127035_SM940_SM940.unl unload file to fix QCCR1E127035. The unload file is available in the %SMSSMEX_HOME%\unloads\SM9.34-9.4x directory.
- If you are upgrading SM 9.31 with PD3 to SM 9.41 Hybrid, you must apply a hotfix for QCCR1E128778 during the upgrade process. The hotfix is available from HP Software Support.

- 1 Click **Tailoring** → **Forms Designer**.
- 2 Type `im.incident.categorization` and click **Search**.
- 3 Add a new notebook tab with the following configurations:

Property	Value
Name	sapsolutionmanager
Visible	True
Visible condition	[\$SMSAP]=true
Caption	Sap Solution Manager

- 4 Add a subform control to the SAP Solution Manager tab.

Property	Value
Format	hp.sap.solution.sub

- 5 Click **Save**.
- 6 Search for `im.incident.investigation`, `im.incident.recovery`, `im.incident.review`, and `im.incident.closure` respectively and repeat [step 3](#) to [step 5](#).

Configuring WSDL Mapping

Configure the IncidentManagement WSDL Mapping table in WSDL Configuration of Service Manager as follow:

Field name	Caption
action	Description
assignee.name	Assignee
brief.description	Title
initial.impact	Impact

Field name	Caption
assignment	AssignmentGroup
product.type	ProductType
resolution	Solution
subcategory	SubCategory
severity	Urgency

Adding Instance in SMIS and Configuring Parameters

The SMSAP instance in SMIS integration is used to enable and disable the SMSAP integration. By configuring the SMSAP instance, you can also specify the integration parameters such as SMSSMEX accessing URL and SAP clients. After the SMSAP instance is enabled, the customization to incident is visible and you can select a SAP Solution Manager client for incident information exchange. If the SMSAP instance is disabled or removed, the incident form customization for incident exchange with SAP Solution Manager will be invisible to the end users. Note that the incident information exchange from SAP SolMan to HP Service Manager will not be affected by SMSAP SMIS configuration. For more information about SMIS, refer to *Service Manager Web Help > Integrations > Integration Manager*.

The SM-SAP integration operates only when the SMSAP instance in SMIS is enabled. Do the following to add a new instance in SMIS and configure the parameters:

- 1 Log in to Service Manager with a System Administrator account.
 - 2 Select **Tailoring** → **Integration Manager**. Integration Manager opens.
 - 3 Click **Add** to open the wizard.
 - 4 Select **SMSAP**, click **Next**.
 - 5 Click **Next** to configure the parameters.
 - a Configure the baseurl for connection to SMSSMEX.
Replace <host> and <port> according to the middleware installation.
 - b Configure SAP Solution Manager clients.
Add general parameters for each of your SAP Solution Manager clients configured in SMSSMEX `ovictex.properties`. For example, `exthd.instances.id.1`, `exthd.instances.id.2` and so on.
- Make sure to set your SAP Solution Manager client instance ID in the Name field, and **SolutionManager** in the Category field of each record. Value of each SAP Solution Manager client instance ID is the reference in HP Service Manager.

Name	Value	Category
baseurl	http://16.183.92.73:8080/ovictex/servlet/OvHDTrigger	General
exthd1	SAP SolMan - HR	SolutionManager
exthd2	SAP SolMan - IT	SolutionManager

- 6 Click **Next** twice to the end of the wizard and click **Finish** to save the configurations.
- 7 Select the SMSAP instance and click **Enable** to enable the SM-SAP integration.

6 Configuring SAP Solution Manager

This chapter describes how to configure the SAP Solution Manager.

Prerequisites

The prerequisites are:

- SAP Solution Manager 7.0 SP 12 (or higher) or SAP Solution Manager 7.1
- SAP Solution Manager SP12 if copying of business transaction SLFN for customization in a customer name space (for example ZLFN) is required
- SAP Solution Manager SP12. Required to copy a business transaction into a customer name space for customization (for example, to copy business transaction SLFN into customer name space ZLFN)
- Configured SAP Solution Manager Service Desk

Configured SAP Solution Manager Service Desk SSL encryption between SAP Solution Manager and Apache Tomcat requires:

- Sapcryptolib 5.5.5C or higher
- SSL Server and SSL Client PSE
- SSL Server and SSL Client certificates trusted against a CA

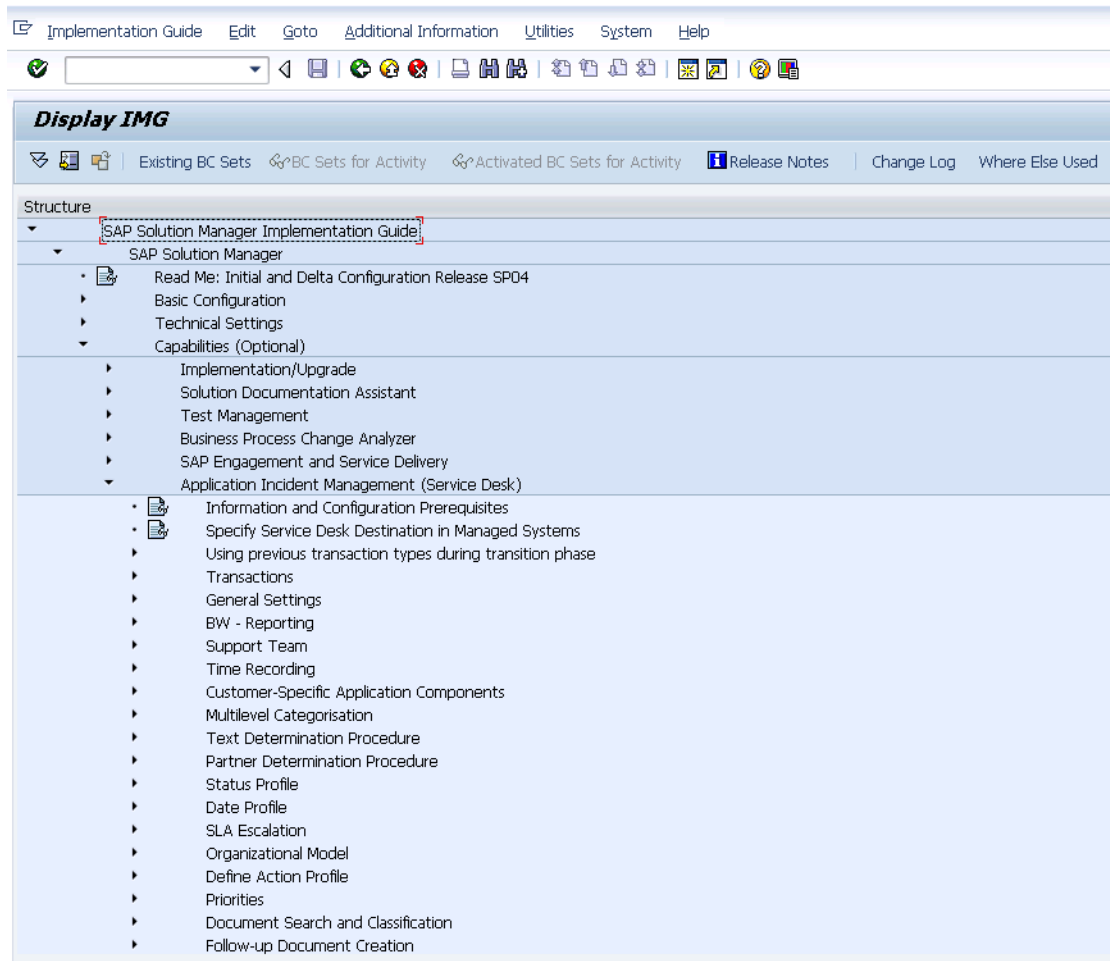
Integration with HP Service Manager requires implementation of the latest SAP notes (SAP application area SV-SMG-SUP-IFA) for the SP level stack of SAP Solution Manager. The following diagram shows the search results of SAP notes in the SAP Support Portal.

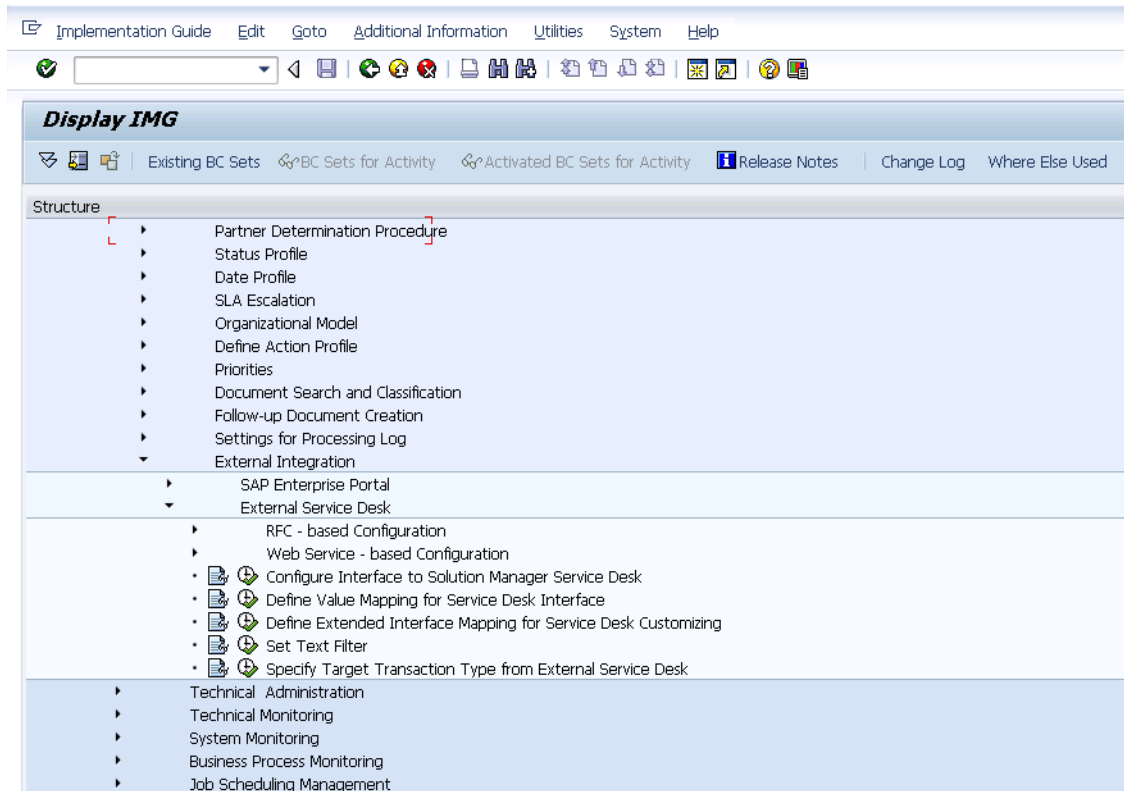
The screenshot shows the SAP Support Portal interface. The address bar displays <https://websmp106.sap-ag.de/notes>. The page header includes the SAP logo, 'SUPPORT PORTAL', and a welcome message for Peter Kreienbring. A navigation menu is visible with options like HOME, Help & Support, Downloads, Keys & Requests, Data Administration, Maintenance & Services, SAP Support Infrastructure, Release & Upgrade Info, and Knowledge Exchange. The main content area is titled 'Search for SAP Notes' and shows search filters such as 'Not satisfied?', 'Restrict your search by:' (Priority, Category, More Terms, ATTACHMENT), and 'Search Discussion Forums at SDN'. The search results are displayed in a table with columns for Ranking, Application Area, Number, Short text, and Last Changed On. The results show 21 SAP Notes found, with the first 9 listed below.

Ranking	Application Area	Number	Short text	Last Changed On	
1.	1.000	SV-SMG-SUP-IFA	1123416	No status change for proposed solution	11.12.2007
2.	1.000	SV-SMG-SUP-IFA	926682	Error handling in partner interface	10.12.2007
3.	1.000	SV-SMG-SUP-IFA	1091156	Dates are only transferred with time zone GMT	11.09.2007
4.	1.000	SV-SMG-SUP-IFA	1089075	No status change for message transfer	05.09.2007
5.	1.000	SV-SMG-SUP-IFA	1088339	System transfers texts of documents incorrectly	05.09.2007
6.	1.000	SV-SMG-SUP-IFA	1078629	User data is not transferred for texts and attachments	13.08.2007
7.	1.000	SV-SMG-SUP-IFA	1078622	Notes are not transferred correctly	08.08.2007
8.	1.000	SV-SMG-SUP-IFA	1054007	Problems with iBase components and assigned notes	11.05.2007
9.	1.000	SV-SMG-SUP-IFA	1050675	Problems with customer-defined actions	02.05.2007

Configuring SAP Solution Manager External Service Desk Interface

SAP provides the Implementation Guide “External Service Desk” for configuring the external help interface. The Implementation Guide is located in SAP transaction /nspro under path \SAP Solution Manager ImplementationGuide\SAP Solution Manager\Capabilities (Optional)\Application Incident Management (Service Desk)\External Integration\ External Service Desk. The following diagrams show the Implementation Guide for configuring the connection to the external Service Desk.



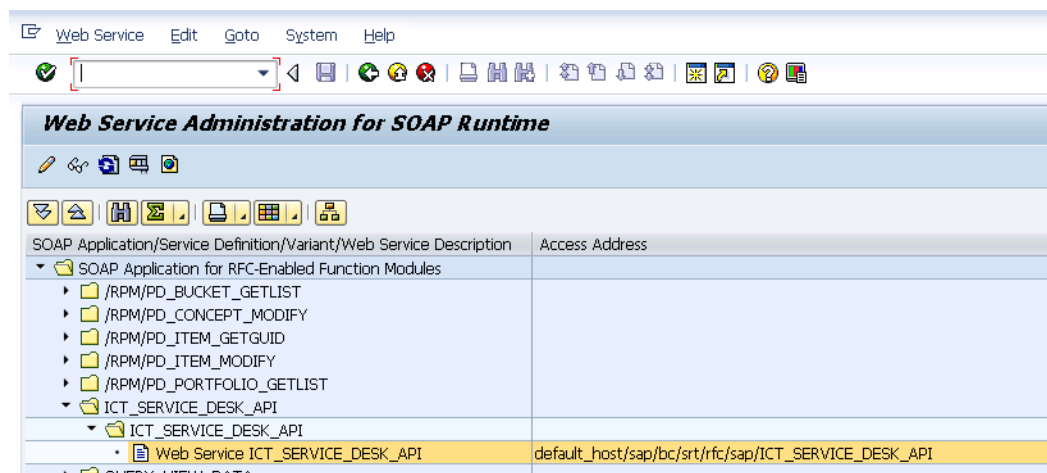


Click the leftmost text sign to view configuration steps. Click the clock sign to enter the corresponding transaction and edit the configuration.

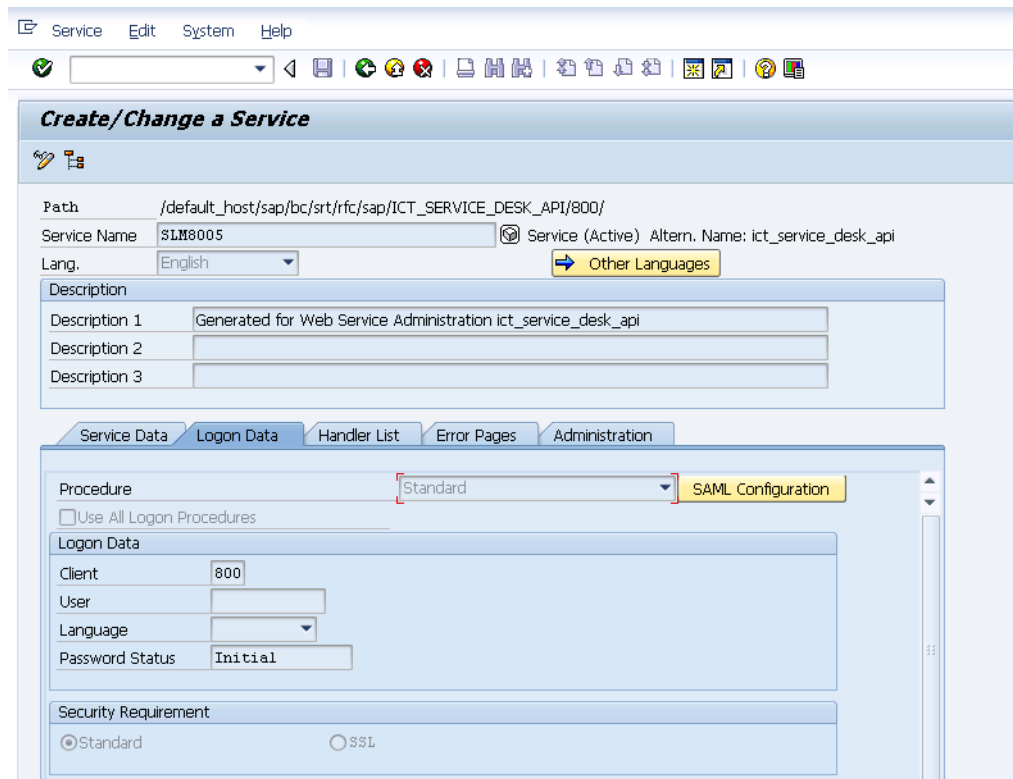
Release Web Service

The Incident Exchange Web Service is deactivated by default. It is required to release the WEB-Service in the Internet Communication Manager Service tree.

- 1 The transaction to release a Web Service is `/nwsconfig`. After the Web Service is released the WS is in SAP transaction `/nwsadmin`.



- 2 To determine the logon procedure of the Web Service for incoming requests, go to SAP transaction `/nsicf`.
- 3 Enter `ICT_SERVICE_DESK_API` as the service name.
- 4 Click **Execute** to execute the search.
- 5 Double-click the Service to edit or navigate to the path `/default_host/sap/bc/srt/rfc/sap/` and select `ICT_SERVICE_DESK_API`.
- 6 In the Logon tab of Create/Change a Service dialog , select **Standard**.



➤ The security section of this manual contains additional information for setting up SSL communications. Adding a user is not required. The Incident Exchange Web Service will use the user and password that is configured in the properties file for HTTP Basic authentication. This user must exist as an SAP user. It is not recommended to use a dialog user for this purpose.

Assign Roles to the Communication User

Configure an SAP user with permission to manage incidents in SAP Solution Manager Service Desk. Follow the instruction in the Implementation Guide and add the roles `SAP_SUPPDESK_PROCESS` and `SAP_SUPPDESK_INTERFACE` to the user. Exchanging a business partner with a default configuration interface requires the additional role `SAP_CRM_BUSINESS_PARTNER`.

To configure a user:

- 1 Select transaction `/nsu01`.
- 2 Input the name of the user.

3 Click **Display** . The user configuration transaction appears.

- ▶ • A person who is assigned to an incident in HP Service Manager but does not exist in Solution Manager will be created as a Business Partner when the incident is forwarded to Solution Manager. Without the business partner role `SAP_CRM_BUSINESS_PARTNER` the incident can not be created or updated in Solution Manager and the error code 99 appears.
- A communication user is recommended, but not necessary.

Sending support messages to SAP AGS requires assigning an SAP Support Portal contact to Solution Manager users who will communicate with the SAP Support Portal via RFC connections. The contact maintained corresponds to the S-user in the SAP Support Portal without “S”. See SAP Note 834534 and the SAP Solution Manager configuration guide for details of Solution Manager roles and authorizations.

Create HTTP Connection

Define the endpoint of the SMSSMEX Web-Service for communication between SAP Solution Manager and Apache Tomcat.

- 1 Select transaction `/nsm59`.
- 2 Create an RFC destination of type **G** (HTTP connection to external server).
- 3 Go to the tab **Technical settings** and specify the endpoint of the SMSSMEX Web-Service. The default is:

Target Host: `<host>`

Service No: `<port>`

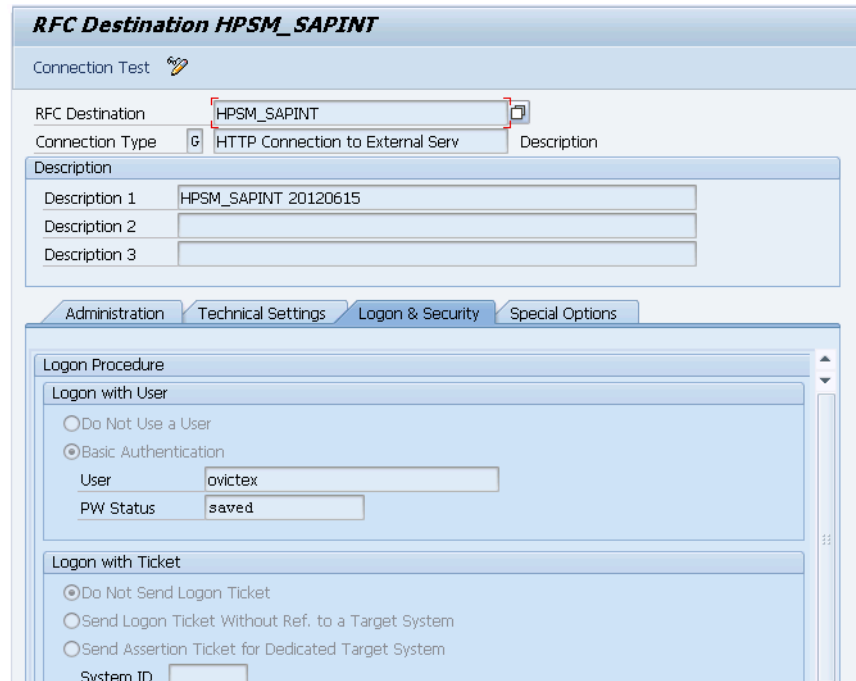
Path Prefix: `/ovictex/services/ICT_SERVICE_DESK_APISoapBinding`

- 4 Add the endpoint in the RFC destination. Your network configuration may require specification of a proxy. The following example shows the RFC destination for host `itsamqavm130`.

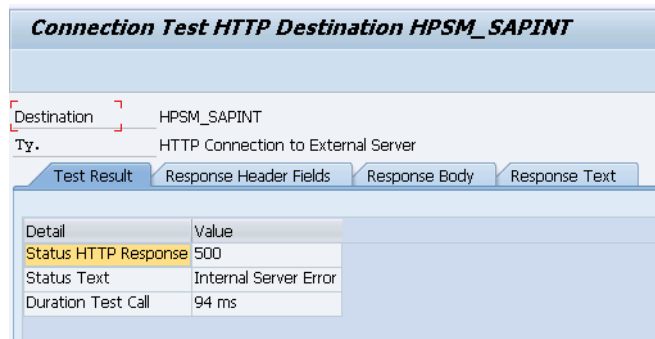
The screenshot shows the SAP configuration interface for an RFC Destination named **HPSM_SAPINT**. The interface is divided into several sections:

- Header:** **RFC Destination HPSM_SAPINT**
- Connection Test:** A button with a pencil icon.
- Basic Information:**
 - RFC Destination: `HPSM_SAPINT`
 - Connection Type: `G` (HTTP Connection to External Serv)
 - Description: A text area with three lines, the first containing `HPSM_SAPINT 20120615`.
- Navigation Tabs:** Administration, **Technical Settings** (selected), Logon & Security, Special Options.
- Target System Settings:**
 - Target Host: `16.186.77.240`
 - Service No.: `8080`
 - Path Prefix: `/ovictex/services/ICT_SERVICE_DESK_APISoapBinding`
- HTTP Proxy Options:**
 - Global Configuration: A yellow button.
 - Proxy Host: Empty text field.
 - Proxy Service: Empty text field.
 - Proxy User: Empty text field.
 - Proxy PW Status: `is initial`

- 5 In the Logon & Security tab define the security settings for outgoing requests. Select **Basic Authentication** for HTTP basic authentication. Add the user and password specified in **ovictex.properties** for HTTP basic authentication. The more secure SSL communication configuration is described in the security chapter of the manual. You can also select **No Logon** which is the default selection for “Logon&Security”.



The following diagram shows the SMSSMEX Web service returning error 500. This result indicates the connection between SAP and SMSSMEX is established.

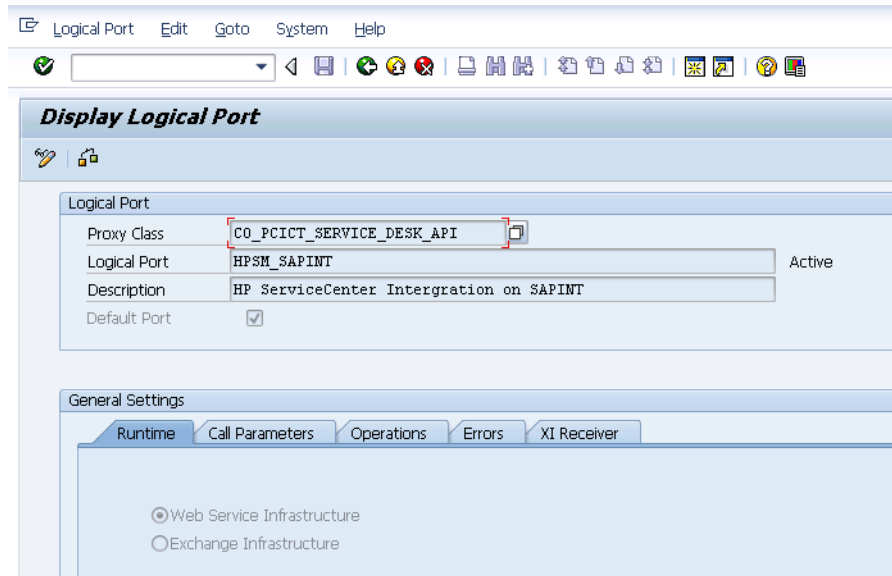


Create a Logical Port

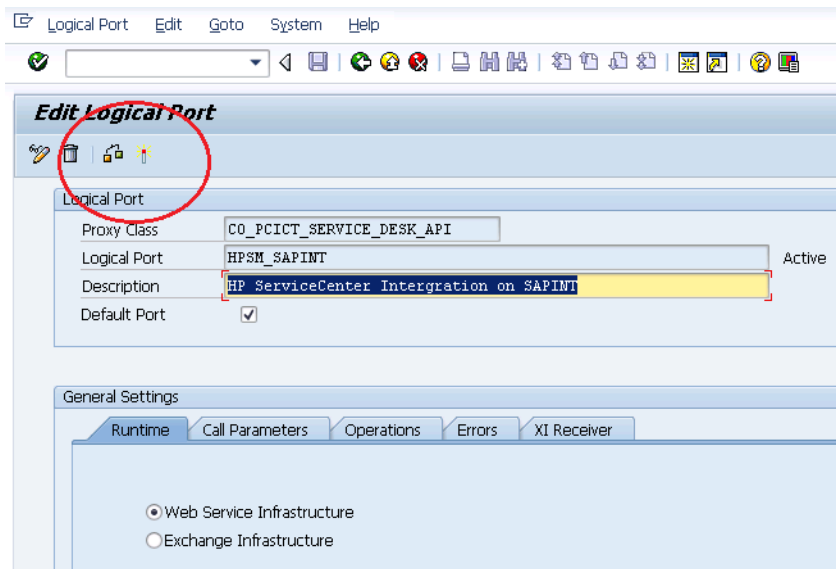
The logical port is the container that encapsulates the outgoing requests. Define the logical port as specified in the Implementation Guide instructions.

- 1 Go to transaction **/nlpconfig**.
- 2 Select **CO_PCICT_SERVICE_DESK_API** as the Proxy Class name.

- 3 In Call Parameters tab add the HTTP destination configured in the previous chapter.

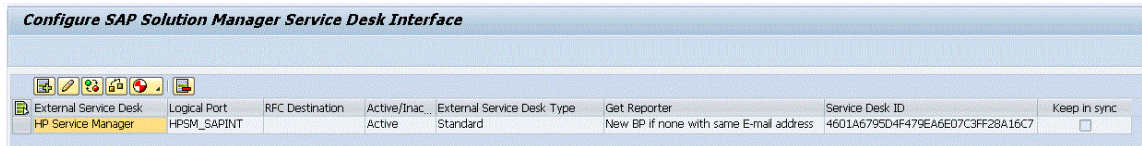


- The port must be activated. Click **Active** to activate the logical port.



Configure Interface to SAP Solution Manager Service Desk

This activity configures the interface between the SAP Solution Manager service desk and the HP Service Manager. Follow the instructions in the Implementation Guide. The configuration requires that Apache Tomcat and the web service are configured and running. In this implementation step the SMSSMEX web service must deliver a unique Service Desk ID. If the Service Desk ID is changed, then the configuration must be repeated.



External Service Desk	Logical Port	RFC Destination	Active/Inac.	External Service Desk Type	Get Reporter	Service Desk ID	Keep in sync
HP Service Manager	HPSM_SAPINT		Active	Standard	New BP if none with same E-mail address	4601A679504F479EA6E07C3FF28A16C7	<input type="checkbox"/>

Use the **Check** button to verify the configuration. Any error message will be displayed in the output window. Use transaction `/nictconf` to jump to configuration transactions.

- ▶ Do not select the **Keep in sync** checkbox when configuring the interface to SAP Solution Manager service desk.
- ▶ If the check fails, try **Generate Default Mapping** → **Overwrite Old Values** and then run the check again. After configuration, click **Save** to save the configured interface.

Define Value Mapping for the Service Desk Interface

This IMG activity configures the value mapping between SAP Solution Manager Service Desk and SMSSMEX for ingoing and outgoing requests. Changing the default value mapping of the SAP Solution Manager is not required. If changes are necessary, use the field mapping file of the SMSSMEX configuration file. To change the default Mapping of the SAP Solution Manager, consult the instructions in the implementation guide.

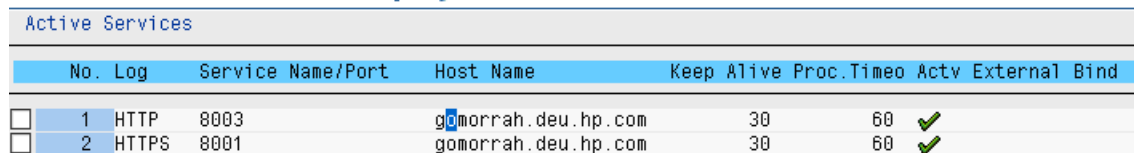
Define Extended Interface Mapping for Service Desk

If SAP Solution Manager Service Desk is highly customized (not using standard SAP objects) then it might be necessary to change the interface mapping. The IMG activity instructions provide more information.

Get SAP Solution Manager Service Port

Go to SAP transaction `/nsmicm`. Select **Goto** → **Services**.

ICM Monitor - Service Display



Active Services							
No.	Log	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv	External Bind
<input type="checkbox"/>	1	HTTP 8003	gomorrah.deu.hp.com	30	60	✓	
<input type="checkbox"/>	2	HTTPS 8001	gomorrah.deu.hp.com	30	60	✓	

This transaction shows the host and the port required for access to the SAP Solution Manager Service Desk web service. Specify in `ovictex.properties` the host/port as the endpoint entry.

Solution Manager Tracing

SolutionManager is able to trace incoming and outgoing web-service XML messages. The messages can be downloaded and used for failure analysis.

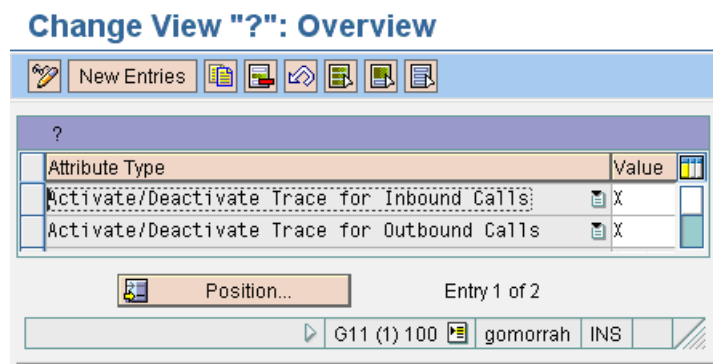
Enable tracing

To enable tracing, implement a SolutionManager Implementation Guide in transaction /**nspro**.

```
spro -> SAP Reference IMG ->
      SAP SolutionManager Implementation Guide ->
      SAP SolutionManager ->
      Configuration ->
      Scenario-Specific Settings ->
      Service Desk ->
      Connecting an External Service Desk ->
      Define Extended Interface Mapping for Service Desk Customizing
```

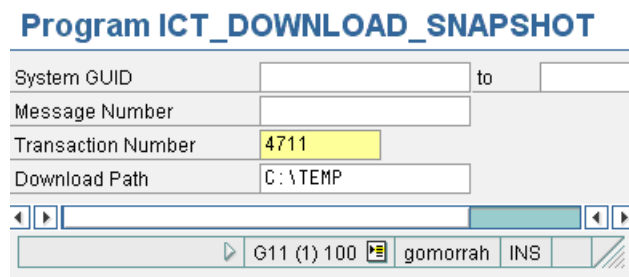
Add new entries to enable tracing for incoming and outgoing calls:

- Activate/Deactivate Trace for Inbound Calls = **X**
- Activate/Deactivate Trace for Outbound Calls = **X**



Download Trace File

To download the trace file, run **ict_download_snapshot** in transaction /**nse38**. Enter the SolutionManager incident id in the field Transaction Number and run the program (**F8**). The trace file will be downloaded to the local computer (for example, incident 4711 traces will be downloaded to C:/TEMP).



7 Configuring Security

This chapter describe the required security configuration settings.

Security between SAP Solution Manager and Tomcat

This section describes the security configuration between SAP Solution Manager and Tomcat.

Configure SAP Solution Manager for SSL

This section describes how to configure SAP Solution Manager for SSL.

Checking SAP SSL Configuration

SAP WEB AS does not support or allow self-signed certificates for communication between Solution Manager and the SMSSMEX Web Service. All certificates must be trusted against a CA.

Before configuring SSL for the External Help Desk interface, check if the WEB AS that hosts the SAP Solution Manager is configured for using SSL.

ICM (Internet Communication Manager) HTTPS service is required for SSL communication. Check if SSL communication is possible in SAP transaction `/nsmicm` (select menu entry **GOTO** and select **Services** or press **SHIFT+F1**).

If SSL communication is possible then an active HTTPS service that is listening to a port is visible. In the example below, the HTTPS port is 8001. This port must be configured in the SMSSMEX web service properties file.

ICM Monitor - Service Display

Active Services						
No.	Log	Service Name/Port	Host Name	Keep Alive	Proc.Timeo	Actv External Bind
<input type="checkbox"/>	1	HTTP 8003	gomorrah.deu.hp.com	30	60	✓
<input type="checkbox"/>	2	HTTPS 8001	gomorrah.deu.hp.com	30	60	✓

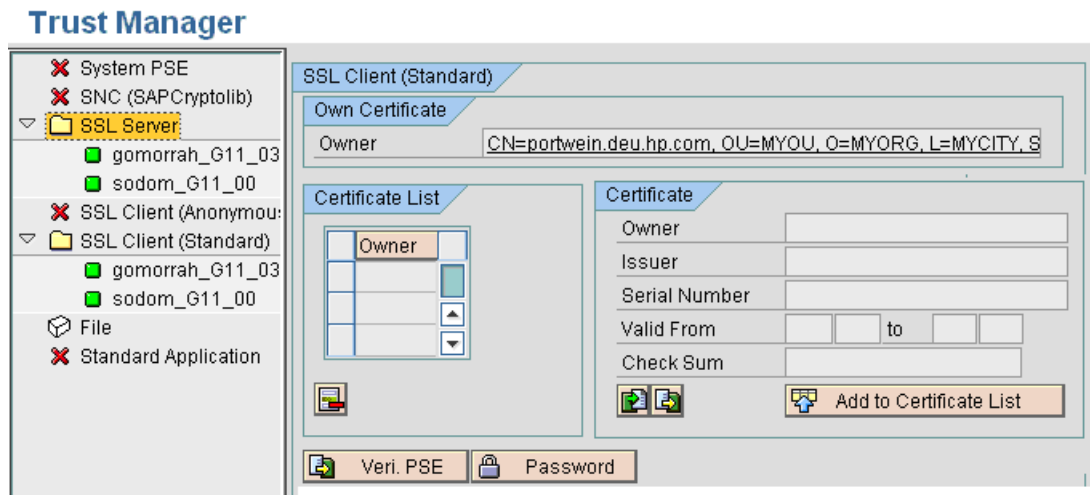
If an HTTPS service in the ICM monitor is not visible, then check the SSL Server configuration in Trust Manager. Start the Trust Manager with SAP transaction `/nstrust`.

If the the PSE entries SSL Server and SSL Client (Standard) are not shown in the Trust Manager status section, then install and configure the SAP `sapcryptolib` library.

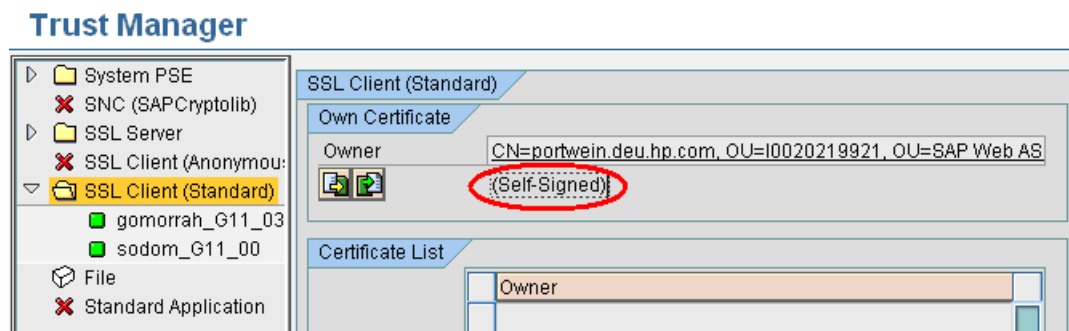


Installing and configuring `sapcryptolib` requires a restart of the SAP WEB AS instance. The installation instructions are in the SAP online help. For more information, see [Appendix B, Installing and Configuring SAPCRYPLIB](#).

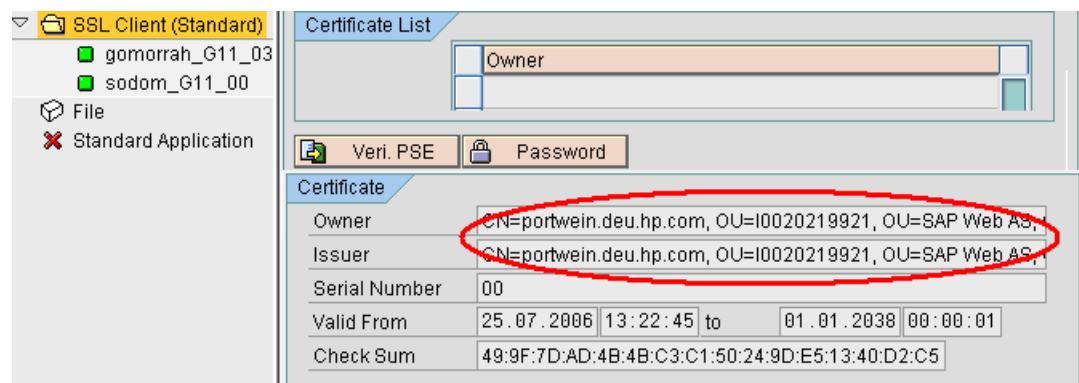
The following diagram shows the Trust Manager with the created PSE “SSL Server” and “SSL Client (Standard)”. The red X in front of the other PSE's indicates that the PSE's have not been created. The PSE “SSL Server” and “SSL Client (Standard)” must be created.



In the next diagram the certificate of the PSE “SSL Client (Standard)” is “Self Signed”. Self-signed certificates are not supported for communication with Apache Tomcat (the certificate must be signed against a CA). If the certificate is signed the 'Self signed' certificate text will disappear.



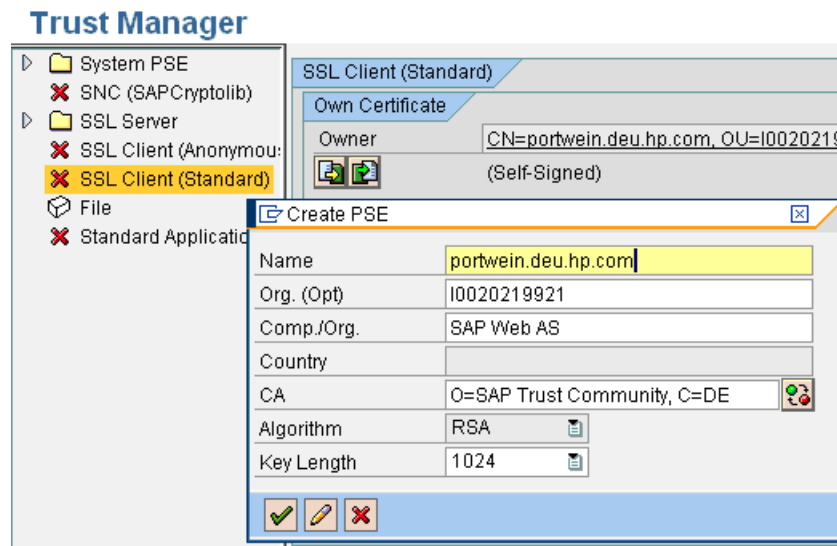
Check the certificate by double-clicking the Owner attribute. The certificate details are shown in the Certificate section. If the Owner and Issuer have the same DN the certificate is self-signed.



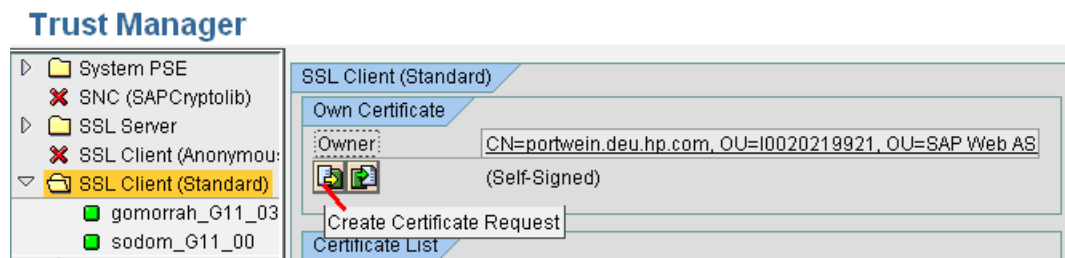
Creating a Client PSE in Trust Manager

To create a client PSE in Trust Manager, do the following:

- 1 Start the Trust Manager.
- 2 Select the **PSE SSL Client (Standard)** in the status section of the Trust Manager.
- 3 Click **Create**.



- 4 For the CN (Name) enter the fully qualified hostname of the SAP WEB AS system. All other entries must not be changed. The key length should be 1024.
- 5 Save the settings.
- 6 Double click **SSL Client (Standard)** in the status section. The Own certificate in the Own Certificate section is shown.
- 7 Click **Create Certificate Request**.



- 8 The Certification Request is shown. Copy the request to the Clipboard.

9 Certify the request with a CA.

```

Certificate Request
-----BEGIN CERTIFICATE REQUEST-----
MIIBiDCB8gIBADBjMwEwYDQKEwptQVAgV2ViIEFTMRQwEgYDVQQLewtJMDAy
MDIxOTkyMTEcMBoGA1UEAxMTCG9ydHdlYW4uZGV1LmhwLmNvbTCBnzANBgkqhkiG
9w0BAQEFAA0BjQAwgYkCgYEA//VPq6qNPamqc3W6YBZBbZK8gR2p1nKqzLjL1y1c
yMqdRnIVqOk7jKs24sfbHPjJxn+Sy819an3A/jig4H0xYUJ0tGEF10nZaVUverpv
+Dmp4SiuJ5fnJI+EEHJpW89TRuAsGzc6x0BBbPL/ijIuKxwUPUPRgUtPneLxfy+3
0GECawEAAaAMA0GCSqGSIb3DQEBBQUAA4GBAK6tBiiz+V41Yr0epGcEiShkYXs6
nKcNxPVz6kJC0Dctnzn+zSkIJ6CILcJcAIu355xq330KpUS+9x2Vsdgunwk4Re7
k9a5Pflfj3Tk0qNaaBr48dU689Yf3/OpEhz15U0W4z199AUUKr0vxp5NYTNSKCB
QqjBdaK6E/TBsBPD
-----END CERTIFICATE REQUEST-----

```

▶ SAP offers a two-month test period for signed certificates in the SAP Service Marketplace at <http://www.service.sap.com/ssltest>.

10 Request an SSL Server Test Certificate as shown in the following diagram (select the PKCS#7 chain format).

The screenshot shows the SAP Support Portal interface for ordering an SSL Server Test Certificate. The page title is "Order SSL Server Test Certificate". There are two steps in the process: "1 Enter Certificate Request" and "2 Import Certificate". A note states: "When generating the certificate request, please do not use an email address in the Distinguished Name (DN) since this is not supported." The "Enter data for public key" section contains a text area with the following certificate request:

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBiDCB8gIBADBjMwEwYDQKEwptQVAgV2ViIEFTMRQwEgYDVQQLewtJMDAy
MDIxOTkyMTEcMBoGA1UEAxMTCG9ydHdlYW4uZGV1LmhwLmNvbTCBnzANBgkqhkiG
9w0BAQEFAA0BjQAwgYkCgYEA//VPq6qNPamqc3W6YBZBbZK8gR2p1nKqzLjL1y1c
yMqdRnIVqOk7jKs24sfbHPjJxn+Sy819an3A/jig4H0xYUJ0tGEF10nZaVUverpv
+Dmp4SiuJ5fnJI+EEHJpW89TRuAsGzc6x0BBbPL/ijIuKxwUPUPRgUtPneLxfy+3
0GECawEAAaAMA0GCSqGSIb3DQEBBQUAA4GBAK6tBiiz+V41Yr0epGcEiShkYXs6
nKcNxPVz6kJC0Dctnzn+zSkIJ6CILcJcAIu355xq330KpUS+9x2Vsdgunwk4Re7
k9a5Pflfj3Tk0qNaaBr48dU689Yf3/OpEhz15U0W4z199AUUKr0vxp5NYTNSKCB
QqjBdaK6E/TBsBPD
-----END CERTIFICATE REQUEST-----

```

Below the text area, there is a "Choose server type" section with a dropdown menu set to "PKCS#7 certificate chain".

11 Click **Continue**. The SSL Server Certificate is created.

The screenshot shows the "Import Certificate into Webserver" section. It contains the following text:

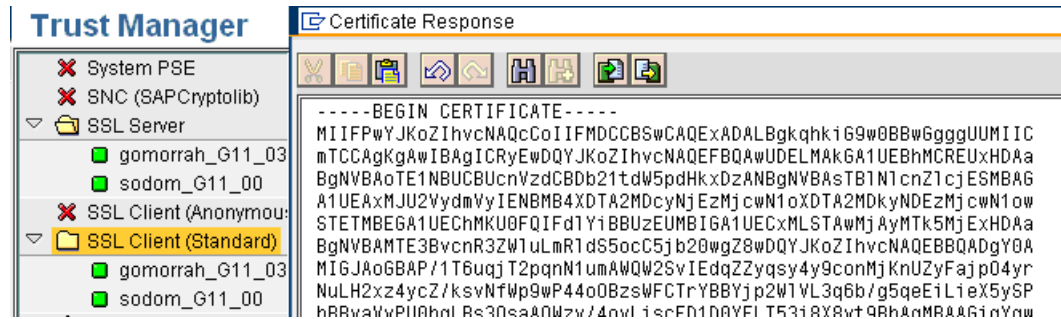
Below is the test certificate for your webserver (as a PKCS#7 certificate chain). Please copy & paste the text beginning with "-----BEGIN CERTIFICATE -----" and ending with "-----END CERTIFICATE -----" into a local text file on the server.

```

-----BEGIN CERTIFICATE-----
MIIFPwYJKoZIhvcNAQcCoIIFMDCCBSwCAQExADALBghkiG9w0BBwGgggUUMIIC
mTCCAgKgAwIBAgICRyEwDQYJKoZIhvcNAQEFBQAuDELMakGA1UEBHMCREUxHDAa
BgNVBAoTElNBUCBUcnVzdCBDb21tdW5pdHkxZDZANBgNVBAsTElN1cnZlcjESMBAG
A1UEAxMJU2VydWVyeiENBMB4XDTA2MDcyNjEzZjcwN1oXDTA2MDkyNDEzZjcwN1ow

```

- Copy the Certificate response to your client PSE.



The certificate is now trusted against a CA. The required steps are different for other CA's. Contact the Trust Center for details. A certificate for the SSL Server PSE is also required.

Setting Up an Outgoing Connection in SAP Solution Manager

The outgoing connection from SAP Solution Manager to HP Apache Tomcat must be configured in SAP transaction `/nsm59`. Add a new or change an existing HTTP RFC destination with type G.


- In SAP transaction `/nsm59` configure the HTTPS port of the Tomcat Server. A redirect from the HTTP port to the HTTPS port of Apache Tomcat will not work with the SAP WEB AS. The HTTPS port is defined in the `server.xml` configuration file of the Tomcat Server.
- The SSL configuration of Apache Tomcat is switched off by default. Enable the configuration.
- In the settings for the SSL HTTP connector, set the Tomcat default port for SSL communication to **8443**.
- The diagram below shows the example configuration of the RFC Destination (in the Target Host field enter the server name (case sensitive) instead of the IP address).

RFC Destination HPSC_SMCINT-HELENHTTPS

Connection Test	
RFC Destination	HPSC_SMCINT-HELENHTTPS
Connection Type	G HTTP Connection to External Serv Description
Description	
Description 1	HP SERVICE CENTER integration to solution manager
Description 2	
Administration Technical Settings Logon & Security Special Options	
Target System Settings	
Target Host	helen2006.asiapacific.hpqcorp.net Service No. 8443
Path Prefix	/ovictex/services/ICT_SERVICE_DESK_APISoapBinding
HTTP Proxy Options	
Global Configuration	
Proxy Host	
Proxy Service	
Proxy User	
Proxy PW Status	is initial

- 5 In the Logon&Security tab of the RFC configuration define the logon procedure and the security protocol. Basic authorization with SSL communication and certificates is not supported by Apache Tomcat. Set the Logon Procedure to **No Logon**.
- 6 In the security protocol status enable SSL and select a PSE from the certification list. SAP provides PSE “ANONYM SSL Client” and “DEFAULT SSL Client (Standard)”.

RFC Destination HPSC_SMCINT-HELENHTTPS

Connection Test 

RFC Destination: HPSC_SMCINT-HELENHTTPS

Connection Type: G HTTP Connection to External Serv Description

Description

Description 1: HP SERVICE CENTER integration to solution manager

Description 2:

Administration Technical Settings **Logon & Security** Special Options

Security Options

Logon Procedure

No Logon

Basic Authentication

Send SAP Logon Ticket

Status of Secure Protocol

SSL Inactive Active

SSL Client Certificate: DEFAULT SSL Client (Standard) Cert. List

Authorization for Destination:

Logon

User:

PW Status: is initial

- 7 Check with the SAP Basis Administrator what client PSE should be used. In most cases this will be the PSE “SAP Client (Standard)”.
- 8 After assigning a client Certificate to the RFC destination, save the settings. The RFC destination is configured for using SSL with Apache Tomcat. A connection test will fail if the Server certificate in Apache Tomcat is not trusted against a CA.
- 9 Create a logical port (see *Create a Logical Port* on page 38).
- 10 Configure the interface between the SAP Solution Manager Service Desk and the HP Service Manager for the SSL outgoing connection (see *Configure Interface to SAP Solution Manager Service Desk* on page 40).

Set up an Incoming Connection in SAP Solution Manager

Configure the incoming connection in the ICF Service tree in SAP transaction `/nsicf`.

- 1 In SAP transaction `/nsicf` enter `ICT_SERVICE_DESK_API` as service name.
- 2 Execute the search of the service.
- 3 Double-click the Service to edit (or navigate to `/default_host/sap/bc/srt/rfc/sap/` and select `ICT_SERVICE_DESK_API`).

- 4 Open the **Create/Change a Service** dialog.
- 5 In the Logon tab select **Required with client Certificates (SSL)**.
- 6 Save the settings. Service **ICT_SERVICE_DESK_API** is configured for SSL connection only. In this procedure the lowest possible security level is specified. If “Required with Logon Data” is configured, then connecting via SSL and the client certificate is allowed.

Create/Change a Service

The screenshot shows the SAP 'Create/Change a Service' dialog. The 'Logon Data' tab is selected. The 'Procedure' dropdown menu is open, showing options: Standard, Alternative Logon Procedure, Required with Logon Data, and Required with Client Certificate (SSL) (highlighted in orange). The 'Client' field is set to 100. The 'User' field is empty. The 'Password' field is empty. The 'Language' field is empty. The 'Password Status' field is set to Initial. The 'Description 1' field contains 'Web Service ICT_SERVICE_DESK_API'. The 'Service Name' is SMD20025. The 'Path' is /default_host/sap/bc/srt/rfc/sap/. The 'Lang.' is English. The 'Service (Active)' checkbox is checked. The 'Altern. Name' is ICT_SERVICE_DESK_A.

- For SSL communication, ensure that the ICM uses HTTPS.

Define the user mapping to the DN of the Certificate. The different ways of mapping are described in the SAP online help. Defining a user mapping to a DN is described below.

- 7 In SAP transaction **/nse16** open the view **VUSREXTID** (enter **VUSREXTID** in the table Name field).
- 8 Select the Work Area **DN of Certificate X.500**.
- 9 In the user mapping dialog, as an external ID add the DN of the client certificate of Apache Tomcat (see *Create Keystore and Truststore* on page 50). Specify the exact DN of the certificate. For example:
 CN=helen2006.asiapacific.hpqcorp.net, OU=TEST, O=GDCC, L=SH, SP=CN, C=CN
- 10 For **Seq.** No enter **000, 001...** (for internal use only).
- 11 Assign the SAP user for the Web Service. This user has all required permissions for managing incidents in SAP Solution Manager.

New Entries: Details of Added Entries

The screenshot shows the 'New Entries: Details of Added Entries' dialog. The 'External ID type' is DN. The 'External ID' is CN=tcwm112.deu.hp.com, OU=DEPP, O=MYORG, L=MYCITY, SP=MYST. The 'Seq. No.' is 000. The 'User' is SERVICE_DESK. The 'Min. date' field is empty.

Set up SSL between SAP and SMSSMEX

This section describes how to setup SSL between SAP and SMSSMEX.

Create Keystore and Truststore

SMSSMEX requires

- Two separate stores that contain the certificates used to authenticate and encrypt communication.
- The following certificates
 - Signed certificate with the long hostname of the SMSSMEX server in the CN section (for example `CN="server.hp.com"`). This certificate must be mapped to an SAP user in SAP Solution Manager.
 - Certificate of the root CA used to sign the certificate of the SAP Solution Manager.
 - Certificate of the root CA used to sign the certificate of the SMSSMEX certificate.

The keystore must contain the following certificates:

- Root CA certificate used to sign the SMSSMEX certificate
- SMSSMEX certificate

The truststore must contain the root certificate used to sign the certificate of the SAP Solution Manager.

Any tool can be used to create and manage the key- and truststores. The following examples use the Java JDK tool `keytool` to create and import a signed certificate.

- 1 Create a self-signed certificate. The keypass and the storepass must be identical.

```
keytool -genkey -alias <alias> -keyalg RSA -keystore <keystorefile>
-storepass <password> -keypass <password> -dname "CN=<serverhost>,
OU=<MYOU>, O=<MYORG>, L=<MYCITY>, ST=<MYSTATE>, C=<MY>"
```

For example:

```
keytool -genkey -alias ovictex -keyalg RSA -keystore "C:\Program
Files\HP\SMSSMEX\config\certs\ovictex.keystore" -storepass ovictex
-keypass ovictex -dname "CN=helen2006.asiapacific.hpqcorp.net, OU=TEST,
O=GDCC, L=SH, ST=CN, C=CN"
```

- 2 Create a certificate request:

```
keytool -certreq -keystore <keystorefile> -alias <alias> -storepass
<password>
```

For example:

```
keytool -certreq -keystore "C:\Program
Files\HP\SMSSMEX\config\certs\ovictex.keystore" -alias ovictex -storepass
ovictex
```

- 3 Use the resulting certificate request to acquire a signed certificate from SAP Web (<https://websmp102.sap-ag.de/SSLTest>) with chain PKCS#7. Copy the signed response `<filename>.p7b` (for example, `sap_rp.p7b`).
- 4 Download the root certificate file for the following web site:
<https://tcs.mysap.com/invoke/tc/getCert?SAPServerCA.der>.
- 5 Import the root certificate from the Certificate Authority (CA) into the keystore.

```
keytool -import -v -alias <alias2> -keystore <keystorefile> -storepass
<password> -file <rootcertificatefile>
```

For example:

```
keytool -import -v -alias saproot -keystore "C:\Program
Files\HP\SMSSMEX\config\certs\ovictex.keystore" -storepass ovictex -file
"C:\Program Files\HP\SMSSMEX\config\certs\getCert.cer"
```

- 6 Import the answer from the Certificate Authority into the keystore. Use the same keystore file and alias the request was created from.

```
keytool -import -v -alias <alias> -keystore <keystorefile> -storepass
<password> -file <certificatefile>
```

For example:

```
keytool -import -v -alias ovictex -keystore "C:\Program
Files\HP\SMSSMEX\config\certs\ovictex.keystore" -storepass ovictex -file
"C:\Program Files\HP\SMSSMEX\config\certs\sap.p7b"
```

To import the certificates into the truststore, use the same command as in the step above, but instead of **<keystorefile>** use the filename of the truststore (if it does not exist, it will be created automatically). For example:

```
keytool -import -v -alias saproot -keystore "C:\Program
Files\HP\SMSSMEX\config\certs\ovictex.truststore" -storepass ovictex -file
"C:\Program Files\HP\SMSSMEX\config\certs\getCert.cer"
```

Configure Tomcat SSL Use

To enable SSL with Tomcat, configure a new connector in the `server.xml` configuration file. The standard `server.xml` contains a connector definition that has been commented out. The following attributes are required:

```
port=<port>
scheme="https"
secure="true"
clientAuth="false"
sslProtocol = "TLS"
keystoreFile=<keystorefile>
keystorePass=<keystorepass>
truststoreFile=<truststorefile>
truststorePass=<truststorepass>
```

For example:

```
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:/Program Files/HP/SMSSMEX/config/certs/ovictex.keystore"
keystorePass="password"
truststoreFile="C:/Program Files/HP/SMSSMEX/config/certs/ovictex.truststore"
truststorePass="password"
/>
```

Configure Property Files

- 1 Modify `exthd.properties`.

- a In the SAP configuration files in property `exthd.webservice.endpoint` specify the new port (default is 8443) and use **https://** as the protocol. For example:

```
exthd.webservice.endpoint = https://watermelon.chn.hp.com:8001/sap/bc/srt/rfc/sap/ICT_SERVICE_DESK_API?sap-client=300
```

- b Set the `exthd.webservice.authentication.scheme` to **HTTPS**.

- 2 Add the following configuration entries in `ovictex.properties`:

```
<saphostname>.keystore=C:/Program Files/HP/SMSSMEX/certs/ovictex.keystore
<saphostname>.keystore.password=~X1~H+7JAOrCX/R6kO5diPxV0w==
<saphostname>.truststore=C:/Program Files/HP/SMSSMEX/certs/ovictex.truststore
<saphostname>.truststore.password=~X1~H+7JAOrCX/R6kO5diPxV0w==
```

For example:

```
watermelon.chn.hp.com.keystore= C:/Program Files/HP/SMSSMEX/certs/ovictex.keystore
watermelon.chn.hp.com.keystore.password=~X1~H+7JAOrCX/R6kO5diPxV0w==
watermelon.chn.hp.com.truststore= C:/Program Files/HP/SMSSMEX/certs/ovictex.truststore
watermelon.chn.hp.com.truststore.password=~X1~H+7JAOrCX/R6kO5diPxV0w==
```

Security Between HP Service Manager and SMSSMEX

This section describes how to configure security between HP Service Manager and SMSSMEX.

Configure HP Service Manager for SSL

For more information about how to configure HP Service Manager for SSL, refer to the *HP Service Manager Help Center* documentation.

Configure SMSSMEX for SSL Communication with Service Manager

To configure SMSSMEX for SSL communications with Service Manager, do the following:

- 1 Import the root CA into the trust keystore.

```
keytool -import -trustcacerts -alias <alias> -keystore <keystorefile>
-file <certificatefile>
```

For example:

```
keytool -import -trustcacerts -alias scca -keystore ovictex.truststore
-file mycacert.pem
```

- 2 Configure `ovictex.properties`.

- a Set `sc.webservice.endpoint`.


```
sc.webservice.endpoint = http://<smhostname>:<port>/sc62server/PWS
```

- b Add the following configuration entries in `ovictex.properties`.

```
<smhostname>.keystore=<ovictex keystore file>
<smhostname>.keystore.password=<keystore password>
<smhostname>.truststore=<ovictex truststore file>
<smhostname>.truststore.password=<truststore password>
```

For example:

```
sc.webservice.endpoint = http://SMCI02.chn.hp.com:13080/sc62server/PWS
.....
SMCI02.chn.hp.com.keystore=C:/Program Files/HP/SMSSMEX/config/certs/
ovictex.keystore
SMCI02.chn.hp.com.keystore.password=~X1~eD+6cy6OMNxdK9tcCQVBww==
SMCI02.chn.hp.com.truststore=C:/Program Files/HP/SMSSMEX/config/certs/
ovictex.truststore
SMCI02.chn.hp.com.truststore.password=~X1~eD+6cy6OMNxdK9tcCQVBww==
```

-  The `keystore.password` and `truststore.password` should use `<SMSSMEX_installDir>/bin/encryptPasswords.bat` to encrypt. For usage of `encryptPasswords.bat`, refer to *Tools* on page 66.

8 Licensing

This chapter describes licensing.

License Types

The following license types are available:

- InstantOn license provides full access to all features for 60 days.
- Permanent license is node-locked (restricted to a range of IP addresses).

License Management

Follow these steps to manage the license:

- 1 Rename the license file to LicFile.txt.
- 2 Copy and paste LicFile.txt to the SMSSMEX installation path, such as C:\Program Files (x86)\HP\SMSSMEX.

▶ The Instance On license is installed during SMSSMEX installation. However, considering the Windows 2012 Security Right Control feature, the Instance On license may not be successfully installed during installation. In this case, you must manually run the InstantOn.bat batch script in the bin folder to add the Instance On license to SMSSMEX or to replace the license file with the existing license data.

9 Status Page

The HP Incident Management Service provides a comprehensive overview of the status of the incident exchange systems and services and provides extensive information for troubleshooting. The URL of the status page is

`http://<hostname>:<port>/ovictex/servlet/OvHDTrigger?status`

The following is an example status page.

HP Integrated Incident Management Service

Product info	ServiceDesk Host: http://hefehell.9999/sc62server/ws	Database Host: alfacon2
Version: 02.03.002	ServiceDesk Version: servicecenter6.2	DB Status: Alive
Created: 2007-06-05 10:39:29	GUID: ALFACON2_BORYS123456789	Is Proxy Mode: FALSE
License: Unlimited license	ServiceDesk Status: Alive	Attachment Mode: LOCAL

External Helpdesk Instance Name	Status	GUID	URL
exthdl	Alive	AA3DD5EE16387E4AB0AA5AED62D66A14	http://portwein.84/sap/bc/srt/rfc/sap/ICT_SERVICE_DESK_API?sap-client=200

Page generated at: 2007-09-28 13:48:26

When a service becomes unavailable, the status changes from Alive to Dead.

HP Integrated Incident Management Service

Product info	ServiceDesk Host: http://hefehell.9999/sc62server/ws	Database Host: alfacon2
Version: 02.03.002	ServiceDesk Version: servicecenter6.2	DB Status: Dead
Created: 2007-06-05 10:39:29	GUID: ALFACON2_BORYS123456789	Is Proxy Mode: FALSE
License: Error during license check	ServiceDesk Status: Alive	Attachment Mode: LOCAL

External Helpdesk Instance Name	Status	GUID	URL
exthdl	Alive	AA3DD5EE16387E4AB0AA5AED62D66A14	http://portwein.84/sap/bc/srt/rfc/sap/ICT_SERVICE_DESK_API?sap-client=200

Page generated at: 2007-10-08 16:54:49

HP Integrated Incident Management Service

Product info	ServiceDesk Host: http://hefehell.9999/sc62server/ws	Database Host: alfacon2
Version: 02.03.002	ServiceDesk Version: servicecenter6.2	DB Status: Dead
Created: 2007-06-05 10:39:29	GUID: ALFACON2_BORYS123456789	Is Proxy Mode: FALSE
License: Error during license check	ServiceDesk Status: Alive	Attachment Mode: LOCAL

External Helpdesk Instance Name	Status	GUID	URL
exthdl	Dead	AA3DD5EE16387E4AB0AA5AED62D66A14	http://portwein.84/sap/bc/srt/rfc/sap/ICT_SERVICE_DESK_API?sap-client=200

Page generated at: 2007-10-08 16:56:43

10 Troubleshooting

This chapter describes how to troubleshoot common problems. The checker tool (see [Verifying Configuration](#) on page 21) is a good aid for troubleshooting.

checker.bat and encryptPasswords.bat Fail

Problem

The exception “Class not found” appears in the console when running `checker.bat` or `encryptPasswords.bat`.

Cause

The library files that checker requires were not extracted to the required Tomcat.

Solution

- 1 Run `setup startup`. Tomcat extracts `ovictex.war` and a copies the required jar files.
- 2 Restart Tomcat.

Incident not Sent to SAP AGS

Problem

Incident is not sent to SAP AGS when using a newly configured priority in Solution Manager.

Cause

Incidents that have set new priorities in Solution Manager can not be sent to SAP AGS (only default priorities can be sent).

Solution

`fieldMapping.xml` maps to default priorities.

java.lang.OutOfMemoryError

Cause

Too many incidents with big attachments are exchanged simultaneously.

Solution

Increase the Java Virtual Machine heap size in `catalina.bat` (Tomcat).

```
set JAVA_OPTS=-Xms512m -Xmx1024m
```

Record in EventIn is not Executed

Problem

The record in table EvenIn is not executed. After Service Manager sends the incident to Solution Manager, the process is finished, but the following problems occur:

- Integration buttons for the incident are not shown correctly.
- Field `hidden.meta.info` is not updated.

Cause

The Event In process threads are not started when the Service Manager server starts, so in the Input Events window (**Tailoring** → **Event Services** → **Input Events**) the input events are not handled (as shown in the following diagram).

The screenshot shows the SAP Event Services Input Queue interface. At the top, there is a table with columns: Type, Checkpoint, Event Time, User ID, and evfields. The table contains several rows of event data. Below the table is a toolbar with buttons for OK, Cancel, Previous, Next, Add, Save, Delete, Find, and Fill. Below the toolbar is the 'Event Services Input Queue' header, followed by a form for editing an event. The form includes fields for Event Code, Status, System Sequence, Time Stamps (First Expiration, Time Processed), User Information (User Name, Password, User Sequence), Incident Information (Network Name, Cause Code, Incident ID), Filter Information (Count, Next Expiration), System Option, and Field Separation Character. At the bottom of the form, there is a text area containing the event's evfields value: `IM16008^Requester:ProviderProcessing^800000314^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at External Helpdesk is 800000314. External Helpdesk is now processing`.

Type	Checkpoint	Event Time	User ID	evfields
hpsapepmu	0EF1AAD279...		ovictex	IM16010^Requester:ProviderProcessing^800000318^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at E...
hpsapepmu	11F21BD25B7...		ovictex	IM16003^Provider:ProviderProcessing^^true^Failed to process action addinfo as the incident is locked by the external helpdesk. Request ...
hpsapepmu	14498DE25B6...		ovictex	IM16002^Provider:ProviderProcessing^^true^Additional information sent to External Helpdesk : SAP Solution Manager
hpsapepmu	27D136E279A...		ovictex	IM16013^Requester:ProviderProcessing^800000321^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at E...
hpsapepmu	520599D463D...		ovictex	IM16008^Requester:ProviderProcessing^800000314^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at E...
hpsapepmu	52E73F925B7...		ovictex	IM16003^Provider:ProviderProcessing^^true^Failed to process action addinfo as the incident is locked by the external helpdesk. Request ...
hpsapepmu	58832C625B6...		ovictex	IM16001^Requester:ProviderProcessing^800000306^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at E...
hpsapepmu	58CD60B2639...		ovictex	IM16006^Provider:SolutionProvided^^false^Solution is provided to External Helpdesk: SAP Solution Manager
hpsapepmu	638432A2799...		ovictex	IM16012^Requester:ProviderProcessing^800000320^false^Created incident in External Helpdesk :SAP Solution Manager. Incident Id at E...

Solution

To handle the input events, start the event in process threads.

1 Go to **System Status**

TOTAL USERS: 1 - use Refresh Display to refresh statistics

Refresh Display

Start Scheduler

Broadcast

Show Locks

Display Options

System Monitor

Summary

Execute Commands

Command	User N...	PID	Device ID	Login Time	Idl...	TID	Session ID
	ovictex	3208	Soap-Windows...	08/07/23 17:...	00:...	4416	3271
	KMUpdate	3056	SYSTEM	08/07/21 11:...	00:...	4512	48
	sync	3056	SYSTEM	08/07/21 11:...	00:...	4564	47
	alert	3056	SYSTEM	08/07/21 11:...	00:...	4588	46
	ocm	3056	SYSTEM	08/07/21 11:...	00:...	4584	45
	contract	3056	SYSTEM	08/07/21 11:...	00:...	4580	44
	availability	3056	SYSTEM	08/07/21 11:...	00:...	4508	43
	event	3056	SYSTEM	08/07/21 11:...	00:...	3404	42
	linker	3056	SYSTEM	08/07/21 11:...	00:...	4568	40
	lister	3056	SYSTEM	08/07/21 11:...	00:...	4524	39
	marquee	3056	SYSTEM	08/07/21 11:...	00:...	2812	37
	agent	3056	SYSTEM	08/07/21 11:...	00:...	3300	36
	sla	3056	SYSTEM	08/07/21 11:...	00:...	4420	35
	change	3056	SYSTEM	08/07/21 11:...	00:...	4424	34
	problem	3056	SYSTEM	08/07/21 11:...	00:...	4432	33
	report	3056	SYSTEM	08/07/21 11:...	00:...	4428	32
	spool	3056	SYSTEM	08/07/21 11:...	00:...	4336	31
	system....	3056	SYSTEM	08/07/21 11:...	2 0...	-1	30
	Thread...	3208	SYSTEM	08/07/21 11:...	2 0...	-1	29

2 Click **Start Scheduler**.

Name	Description
agent	query/chart agent
alert.processor	Standard Alert processor
availability.startup	availability processor
change.startup	ChM alert/notification processor
contract	contract background agent
event.startup	Event Services processor
gie.startup	Generic Input Event Services processor
inactive.startup	dismiss inactive users
KMUpdate	Checks for update records and sends them to the indexer
linker.startup	Problem/Incident Sync Task
lister.startup	Global List Builder Routine
marquee	marquee agent
ocm.startup	OCM processor
printer.startup	print scheduler
problem	IM alert and message processor
report.startup	report processor
scauto.startup	SCAUTO startup
scemail.startup	SCEMAIL startup
SLA	SLA background agent
startup	system startup default
Sync	

3 Start `event.startup` and dependent process threads.

Incident Update or Process Action Fails

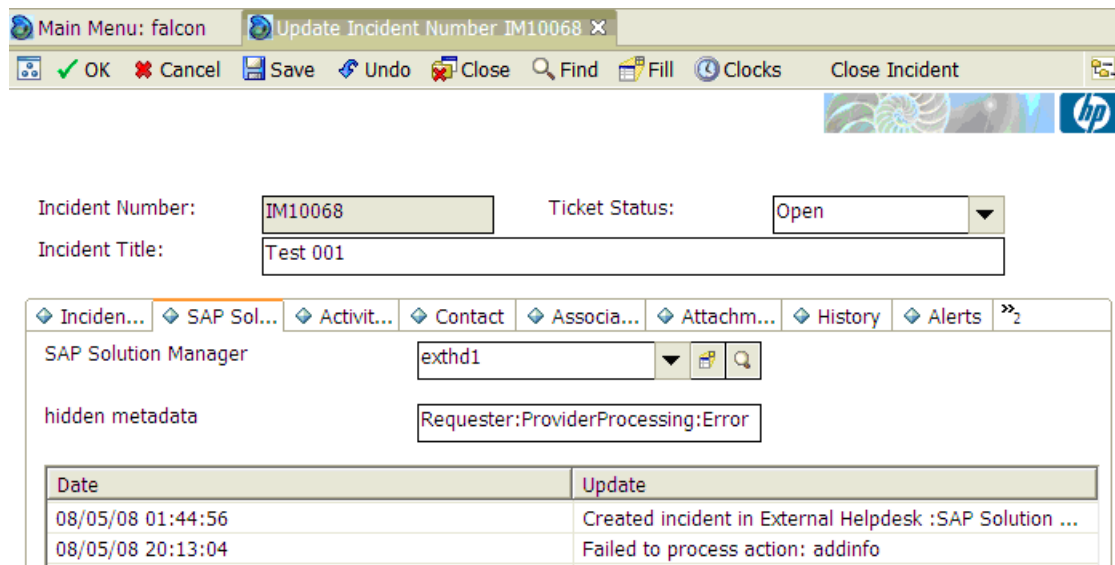
Problem

Some incidents are not exchanged between Service Manager and SAP Solution Manager. The log file or console message of SMSSMEX displays WARN or FATAL level information as described below.

1 Service Manager sends an incident to SAP Solution Manager:

```
WARN com.hp.ov.ictex - Failed to process action addinfo as the incident
is locked by the external helpdesk. Request will be sent again later.
```

The following alert may appear in Service Manager:



The screenshot shows a web application window titled "Update Incident Number IM10068". The interface includes a menu bar with options like OK, Cancel, Save, Undo, Close, Find, Fill, Clocks, and Close Incident. Below the menu, there are input fields for "Incident Number" (IM10068) and "Ticket Status" (Open), and a text field for "Incident Title" (Test 001). A navigation bar contains tabs for Incident, SAP Sol..., Activit..., Contact, Associa..., Attachm..., History, and Alerts. The main content area shows "SAP Solution Manager" with a dropdown menu set to "exthd1" and a search icon. Below this, "hidden metadata" is displayed as "Requester:ProviderProcessing:Error". At the bottom, a table shows incident updates:

Date	Update
08/05/08 01:44:56	Created incident in External Helpdesk :SAP Solution ...
08/05/08 20:13:04	Failed to process action: addinfo

2 SAP Solution Manager updates the incident to Service Manager.

```
DEBUG com.hp.ov.ictex - Failed to update incident. id:IM10068
DEBUG com.hp.ov.ictex - Response code = 3. Probably an Incident: IM10068
is locked.
FATAL com.hp.ov.ictex - Saving of incident failed. Received Message from
ServiceCenter: Resource Unavailable
null
FATAL com.hp.ov.ictex - An error ocured while processing incident ID
IM10068. Message: Resource Unavailable
null
DEBUG com.hp.ov.ictex - An error ocured while processing incident ID
IM10068. Message: Resource Unavailable
null
com.hp.ov.ictex.ovhdaccess.OvHDException: Resource Unavailable
null
at com.hp.ov.ictex.ovhdaccess.servicecenter.Incident.save(Unknown Source)
at
com.hp.ov.ictex.exthdrequesthandler.OvictexServer.updateIncident(Unknown
Source)
...
```

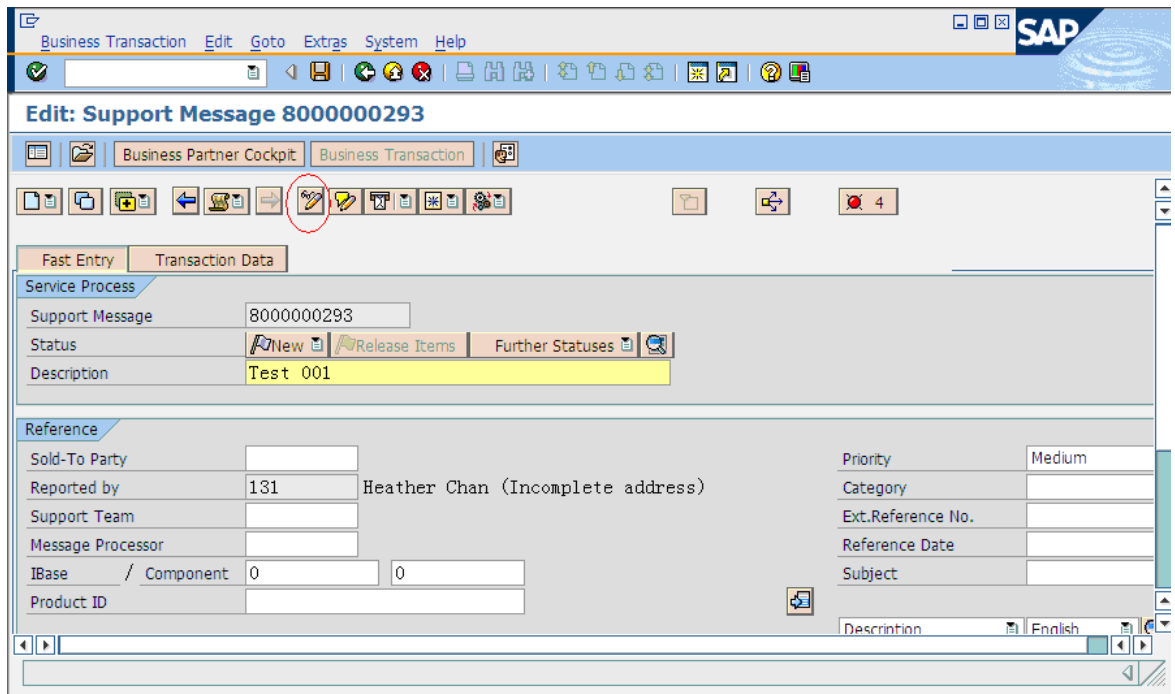
Cause

The incident in HP Service Manager or SAP Solution Manager is locked:

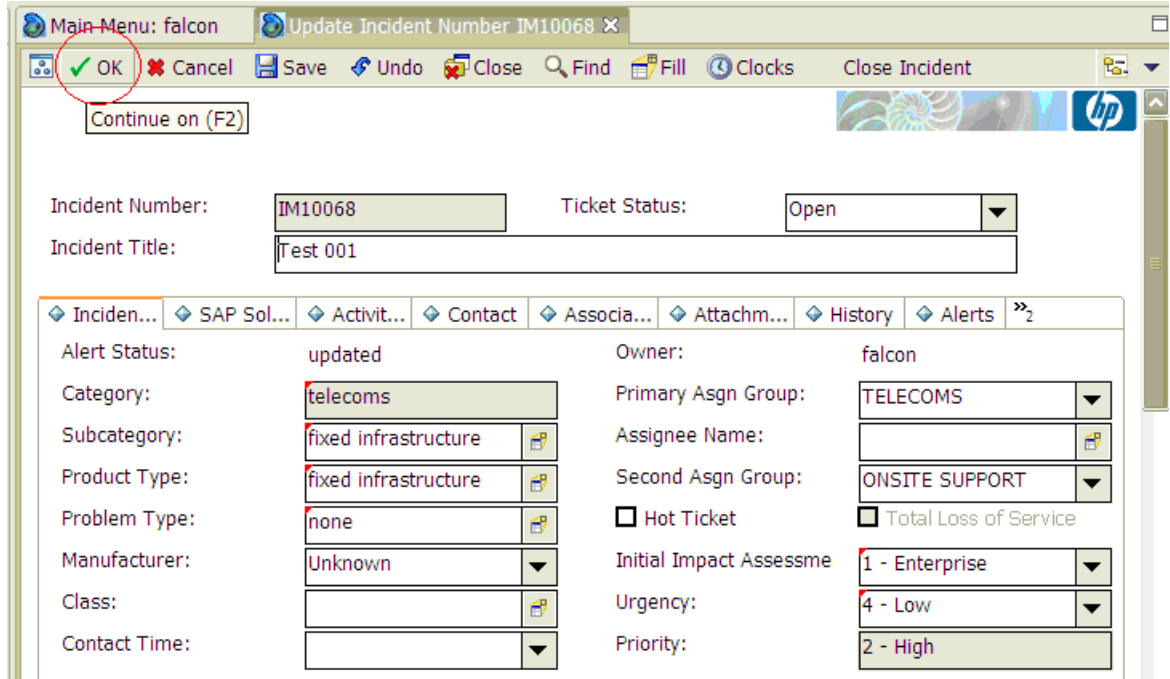
- 1 In SAP Solution Manager, if the user does not click the button **Display/Change Trans.** to release an incident write lock, HP Service Manager can not update or send a message to SAP.
- 2 In HP Service Manager, if the user does not click **OK** to release an incident write lock in time, the incident maintains the “Updating” status and no message from SAP can be accepted (until the status changes).

Solution

In SAP Solution Manager always click **Display/Change Trans.** after finishing or updating an activity.



In HP Service Manager click **OK** after finishing or updating an activity.



Information is not Updated in SAP Solution Manager

Problem

An open support message is not changed after synchronization from Service Manager to SAP.

Cause

SAP solution manager does not refresh the support message automatically.

Solution

In SAP GUI, exit from the current transaction and execute transaction `crmd_order`.

A Incident Exchange Details

Database Tables

The database tables required to operate the exchange service are created with the SQL scripts `create_tables_oracle.sql` or `create_tables_sqlserver.sql`.

Table 2 Database tables required for exchange service

Table	Field	Description
systemguid	systemguid	Unique system web service GUID
tasklist	ovhdid	ID of incident that triggered the action
	action	Action for the incident (state transitions of status diagram). Can be ProcessIncident, AddInfo, AcceptIncidentProcessing, RejectIncidentSolution, VerifyIncidentSolution, or CloseIncident.
	startTimestamp	Creation timestamp of entry.
	enqueueTimestamp	Timestamp for ordering of tasks. Initial value is startTimestamp.
	earliestReadyTimestamp	Timestamp that specifies the earliest time when this entry can be processed. Empty means immediately. Task becomes ready only after this time.
	state	Task state. Can be 1=READY or 2=INPROCESS (task is processed already).
	tries	Number of attempts to complete this task.
	guid	GUID of the task to delete the correct entry in database.
	sapid	Name of external help desk instance that incident is exchanged with.

Table 2 Database tables required for exchange service (cont'd)

runtimedat a	incidentguid	GUID of exchanged incident
	ovhdincidentid	ID of incident in helpdesk managed by web service
	exthdincidentid	ID of incident in the external helpdesk
	requesterguid	System GUID of requester helpdesk for that incident
	providerguid	System GUID of provider helpdesk for that incident
	metadata	Incident state in statement diagram and role the ServiceDesk has for this incident (Requester or Provider). Stored in the same format used for the Hidden_Meta_Data field in ServiceDesk (such as Requester:RequesterProcessing, Provider:SolutionProvided).
	infologid	Reference to multiple entries in runtimedata_infolog.
	attachmentid	Reference to multiple entries in runtimedata_attachments.
	lastchange	Timestamp of last change of entry.
runtimedat a_infolog	infologid	Key referenced from runtimedata.
	infologblock	Number of infolog block sent already.
runtimedat a_attachm ents	attachmentid	Key referenced from runtimedata.
	filename	Filename of an attachment for incident.
	attachmentguid	GUID for attachment (also known by external helpdesk) to delete attachment.

Tools

There are several configuration tools in the installation \bin directory. Tool scripts are available for Windows (.bat) and Unix (.sh):

- `encryptPasswords` encrypts the passwords in the configuration file. All properties ending with `.password` must be configured with this tool. Use `-global` or `<instance key>` as a parameter.
 - `global`
Encrypt a password in the global properties file (`ovictex.properties`). For example:
`encryptPasswords.bat -global`
 - `<instance key>`
Encrypt a password in the configuration file of a specific instance. For example:
`encryptPasswords.bat exthd`
- `setup` is the setup script for Tomcat start/stop. For Tomcat

- Start: Setup startup
- Shutdown: Setup shutdown
- Start with debug mode: Setup debug startup
- checker checks the configuration in `ovictex.properties` and Service Manager configuration (see [Verifying Configuration](#) on page 21 for more information) .

Field Mapping Configuration

Incident exchange web service exchanges incident data as XML documents between Service Manager and the external HelpDesk SAP Solution Manager. Incident exchange transforms the incident data in Service Manager to an XML message for SAP Solution Manager, and transforms Solution Manager data to an XML message for Service Manager. The transformation maps the field name in Service Manager to XML elements in Solution Manager while taking into account the following:

- Field names in Service Manager are usually different from the message element name.
- Service Manager field data type can differ from the message element data type.
- Not all message elements have corresponding data fields in Service Manager. Such fields are usually combined into a single log field called `Journal`.
- Some fields also require value mapping. For example, the possible values for the `Priority` field in Service Manager are **1 - Critical, 2 - High, 3 - Average, 4 - Low**. The Solution Manager Priority can be **5, 4, 3, 2, 1**. These values must be specified in the `FieldValueMapping` configuration.
- Service Manager can assign customized fields to an Incident. These fields can be mapped to message elements.

A declarative field mapping file defines the mapping outlined above and

- Enables the exchange of incident data between two helpdesks with reduced code size (the same code can handle any number of fields)
- Improves flexibility (mapping can be changed without changing code)
- Improves extensibility and customizability (a deployment-specific mapping can be added without changing code)
- Used to map incident data with an external helpdesk other than Solution Manager

Types of Mapping

The mapping file supports field mapping and field value mapping. Field mapping is simple (XML message element is a single value) or composite (multiple values such as an array).

Structure of FieldMapping XML file

The field mapping configuration is related to the `ICT_SERVICE_DESK_API` WSDL scheme defined by SAP Solution Manager. The mapping consists of field mapping and value mapping.

Field mapping includes:

- `IctHead`

- IctIncidentAttachment
- IctIncidentSapNotes
- IctIncidentSolutions
- IctIncidentUrls
- IctIncidentStatement
- IctIncidentAdditionalInfo

The following is a mapping file example:

```
<FieldMapping ExtHDFField="IctHead/AgentId" >
  <OutOvHDFField>Assignee</OutOvHDFField>
  <OutDataType>Person</OutDataType>
  <InOvHDFField>Assignee</InOvHDFField>
  <InDataType>Person</InDataType>
</FieldMapping>
```

In the above example:

- Element IctHead/AgentId of SAP Solution Manager (sub-element AgentId of top level element IctHead) maps to the field Assignee exposed by the Service Manager IncidentManagement Web Service.
- Data types for the IN and OUT exchange modes are specified in the InDataType and OutDataType tags.
- Person type indicates that the Exchange must convert incoming data (to/from the Service Manager) to/from an internal Person type that corresponds with the IctIncidentPerson type of the SAP SolutionManager web service.
- InDataType and OutDataType tags declare types on the Service Manager side.

Composite Field Mapping

Composite field mapping maps a message element to a OvHD field depending upon the value of a sub-element (key) of the element ExtHDKeyField (OvHD and ExtHD are old terms; in this document, OvHD correspond to HP Service Manager and ExtHD correspond to SAP Solution Manager). A different value for the key defines mapping to a different Service Manager field. The following is a composite field mapping example.

```
<CompositeFieldMapping ExtHDFField="IctIncidentStatement"
  ExtHDKeyField="IctIncidentStatement/TextType">
<!-- For exchanging information log -->
<FieldMapping ExtHDFField="IctIncidentStatement/Text" >
  <InDataType>InformationLog</InDataType>
  <OutDataType>InformationLog</OutDataType>
  <KeyFieldOutVal>SU99</KeyFieldOutVal>
  <KeyFieldInVal>SU99</KeyFieldInVal>
</FieldMapping>
<!-- for exchanging Solution Provided -->
<FieldMapping ExtHDFField="IctIncidentStatement/Text">
  <OutOvHDFField>Solution</OutOvHDFField>
  <InOvHDFField>Solution</InOvHDFField>
  <KeyFieldOutVal>SU99</KeyFieldOutVal>
  <KeyFieldInVal>SU01</KeyFieldInVal>
</FieldMapping>
<!-- for exchanging CustomText01 (as example) -->
```

```

<FieldMapping ExtHDField="IctIncidentStatement/Text" >
  <InOvHDField>CustomText01</InOvHDField>
  <OutOvHDField>CustomText01</OutOvHDField>
  <KeyFieldOutVal>SU99</KeyFieldOutVal>
  <KeyFieldInVal>SU77</KeyFieldInVal>
</FieldMapping>
<!-- For sending custom fields from OVHD to external HD create an entry as
the example below. Replace the place holder strings as per your
configuration -->
<!--
  <FieldMapping ExtHDField="IctIncidentStatement/Text" >
    <OutOvHDField>USER_VISIBLE_FIELDNAME_FOR_THAT_CUSTOM_FIELD
    </OutOvHDField>
    <KeyFieldOutVal>TEXT_TYPE_AS_DEFINED_BY_USER_FOR_THIS_FIELD
    </KeyFieldOutVal>
  </FieldMapping>
-->
</CompositeFieldMapping>

```

Element `IctIncidentStatement/Text` is mapped to the information log if the key element `IctIncidentStatement/TextType` is **SU99** or to Resolution field if the key element is **SU01** (for an incoming message).

This is used when a message has multiple occurrences of the same element that have different sub-element values. The sub-element is referred to as the key field. In the example above the `IctIncidentStatement/TextType` element is the key field. For a composite field mapping, every instance of `FieldMapping` has a unique `KeyFieldInVal`.

Field Value Mapping

Field value mapping maps the values of a message element to the corresponding value of an OvHD field. The following is an example.

```

<FieldValueMapping Id="IctHead/Priority">
  <ValueMapping OvHDValue="4" ExtHDValue="5"/>
  <ValueMapping OvHDValue="4" ExtHDValue="4"/>
  <ValueMapping OvHDValue="3" ExtHDValue="3"/>
  <ValueMapping OvHDValue="2" ExtHDValue="2"/>
  <ValueMapping OvHDValue="1" ExtHDValue="1"/>
</FieldValueMapping>

```



Since both helpdesks priority lists can be configured, check the actual values in the field value mapping.

Field Mapping Schema

The RelaxNG Compact Schema of the mapping file is shown below.

```

default namespace =
  "http://schemas.hp.com/openview/incidentExchange/mapping"
start =
  element IncidentExchMapping {
    attribute targetNamespace { xsd:anyURI },
    element FieldMappings {
      (FieldMapping

```

```

        | element CompositeFieldMapping {
            attribute ExtHDField { string },
            attribute ExtHDKeyField { string },
            FieldMapping+
        })+
    } &
    element ValueMappings {
        element FieldValueMapping {
            attribute Id { string },
            element ValueMapping {
                attribute ExtHDValue { string },
                attribute OvHDValue { string }
            }+
        }
    }
}
FieldMapping =
    element FieldMapping {
        ## field accessor in XML document using XPath like notation. Example:
        ## ExtHDField="IctHead/AgentId"
        attribute ExtHDField { string },
        attribute ValueMappingId { string }?,
        (element InOvHDField { string } &
        (element DefaultOutOvHDField { string }
        | element OutOvHDField { string }))? &
        element InDataType { "InformationLog" | "Priority" | "Date" |
        "Attachment" | "OvCISearchKey" }? &
        element OutDataType { "Person" | "Priority" | "Date" | "Attachment" |
        "OvCISearchKey" }? &
        element KeyFieldOutVal { string }? &
        element KeyFieldInVal { string }? )
    }

```

The schema elements are described in the following table.

Table 3 Schema element functionality

Schema element	Function
IncidentExchMapping	Top-level element of the mapping schema.
FieldMappings	Container element for all FieldMapping and CompositeFieldMapping elements.
ValueMappings	Container element for FieldValueMapping elements.
FieldMapping	Maps a message element to an OvHD field and includes type information for storing to and loading from OvHD. Optionally contains a reference to a FieldValueMapping element through attribute ValueMappingId. The value of this attribute must match the value of attribute Id in a FieldValueMapping element. When this reference is present, the information in the FieldValueMapping must be used to map field value.

Table 3 Schema element functionality (cont'd)

Schema element	Function
CompositeFieldMapping	Maps a message element to a OvHD field depending upon the value of a sub-element (key) of the element. A different key value defines mapping to a different OvHD field. The keyFieldInVal must be unique for each individual field mapping within a composite field mapping.
ValueMapping	Maps the OvHD value of a message element to an ExtHD value.
ExtHDField	Field accessor in XML message document in XPATH like expression that identifies a specific field of exchanged incident information.
InOvHDField	Indicates the OvHD field name where information received from the external helpdesk is written for a specific ExtHDField.
OutOvHDField	Indicates the OvHD field name whose value is sent to the external helpdesk for a specific ExtHDField.
DefaultOutOvHDField	If this element appears in a field mapping then the value of this element is taken as the default value sent to the external helpdesk for a specific ExtHDField. For example, if a mapping DefaultOutOvHDField is specified as DefaultUserId and OutDataType is specified as Person, the default user ID will be sent to the external helpdesk for a specific ExtHDField.
InDataType	Datatype for storing the field value to OvHD.
OutDataType	Datatype for loading the field value from OvHD.
InDataType and OutDataType	Specifies the method to call for reading/writing information from/to the incident using the OvHDAccess layer. InDataType and OutDataType are optional elements. If not specified, then the field types are assumed to be String. Otherwise the following data types can be specified: <ul style="list-style-type: none"> • Priority: Priority of an incident • Date: A date field • Attachment: Refers to an attachment • Person: Indicates that the information is a person detail.
OvCISearchKey	Indicates the information is used as a search key for CI in OvHD.
InformationLog	Applicable only for InDataType. Indicates the information should be appended to the Information Log.
KeyFieldInVal	Value stored in OvHD for the element used as the key field.
KeyFieldOutVal	Value sent to ExtHD for the element used as the key field.

Default Field Mapping File and Customization

Prerequisites

SMSSMEX operates with Service Manager based on the extended IncidentManagement Web Service and supports only the fields listed below (exposed in the Service Manager IncidentManagement WS).

Table 4 SMSSMEX supported fields

Field	Type	Field	Type
IncidentID	Text	Subcategory	Text
Category	Text	SLAAgreementID	Decimal
OpenTime	Datetime	PlannedEnd	Datetime
OpenedBy	Text	SiteCategory	Text
PriorityCode	Text	ProductType	Text
Severity	Text	ProblemType	Text
UpdatedTime	Datetime	ResolutionFixType	Text
PrimaryAssignment Group	Text	UserPriority	Text
ClosedTime	Datetime	Solution	Text
ClosedBy	Text	InitialImpact	Text
ClosureCode	Text	CustomText01	Text
ConfigurationItem	Text	CustomText02	Text
Location	Text	CustomText03	Text
IncidentDescription		CustomText04	Text
Resolution	Resolution	CustomText05	Text
Assignee	Text(OperatorID)	CustomText06	Text
Contact	Text(ContactID)	CustomText07	Text
JournalUpdates		CustomText08	Text
AlertStatus	Text	CustomText09	Text
ContactLastName	Text	CustomText10	Text
ContactFirstName	Text	SapSid	Text
Company	Text	SapClient	Text
Title	Text	SapInstallationNumber	Text

Table 4 SMSSMEX supported fields (cont'd)

TicketOwner	Text	HiddenMetaData	Text
UpdatedBy	Text	IsIncidentExchange	Boolean
IMTicketStatus	Text	attachments	Attachments

Adding Fields to fieldMapping.xml

The default field mapping file (provided with the incident exchange web service) does not include all fields from the web service and can be extended. Any additional field mapping can be included in section `IctIncidentStatement`. The following is an example:

```
<FieldMapping ExtHDField="IctIncidentStatement/Text">
  <OutOvHDField>SC_WS_FIELDNAME</OutOvHDField>
  <KeyFieldOutVal>SOLMAN_FIELD_TYPE </KeyFieldOutVal>
</FieldMapping>
<FieldMapping ExtHDField="IctIncidentStatement/Text">
  <OutOvHDField>CustomText09</OutOvHDField>
  <KeyFieldOutVal>SU99 </KeyFieldOutVal>
</FieldMapping>
```

In the above example, the custom field defined in Service Manager is sent to the external HD, so `KeyFieldOutVal` is defined at the external helpdesk. No `InOvHDField` or `KeyFieldInVal` is specified since the example only sends to the external helpdesk.

IN/OUT data exchange requires definition of IN and OUT:

```
<FieldMapping ExtHDField="IctIncidentStatement/Text">
  <OutOvHDField>SC_WS_FIELDNAME1</OutOvHDField>
  <InOvHDField>SC_WS_FIELDNAME2</InOvHDField>
  <KeyFieldOutVal> SOLMAN_FIELD_TYPE1 </KeyFieldOutVal>
  <KeyFieldInVal> SOLMAN_FIELD_TYPE2 </KeyFieldInVal>
</FieldMapping>
```

In this example if the values of `SC_WS_FIELDNAME1` and `C_WS_FIELDNAME2` are the same, then the `OvHD` field is overwritten when information is sent from external helpdesk (1:1 field synchronization). For example:

```
<FieldMapping ExtHDField="IctIncidentStatement/Text">
  <OutOvHDField>CustomText09</OutOvHDField>
  <InOvHDField>CustomText09</InOvHDField>
  <KeyFieldOutVal> SU01</KeyFieldOutVal>
  <KeyFieldInVal>SU01</KeyFieldInVal>
</FieldMapping>
```

In the following example, `CustomText08` updates field `ZZ08` in SAP Solution Manager, but `ZZ08` updates `CustomText09` in Service Manager (does not overwrite `CustomText08`).

```
<FieldMapping ExtHDField="IctIncidentStatement/Text">
  <OutOvHDField>CustomText08</OutOvHDField>
  <InOvHDField>CustomText09</InOvHDField>
  <KeyFieldOutVal> ZZ08</KeyFieldOutVal>
  <KeyFieldInVal>ZZ08</KeyFieldInVal>
</FieldMapping>
```

Additional Information

Section `IctIncidentAdditionalInfo` defines synchronization of CIs between SAP Solution Manager and Service Manager and defines the method for sending SAP Attributes from SAP Solution Manager.



The first part of the mapping describes CI mapping handling and must not be changed.

```
<FieldMapping ExtHDField="IctIncidentAdditionalInfo/AddInfoValue" >
  <OutDataType>OvCISearchKey</OutDataType>
  <InDataType>OvCISearchKey</InDataType>
  <KeyFieldOutVal>SAPSystemID</KeyFieldOutVal>
  <KeyFieldInVal>SAPSystemID</KeyFieldInVal>
</FieldMapping>
<FieldMapping ExtHDField="IctIncidentAdditionalInfo/AddInfoValue" >
  <OutDataType>OvCISearchKey</OutDataType>
  <InDataType>OvCISearchKey</InDataType>
  <KeyFieldOutVal>SAPSystemClient</KeyFieldOutVal>
  <KeyFieldInVal>SAPSystemClient</KeyFieldInVal>
</FieldMapping>
<FieldMapping ExtHDField="IctIncidentAdditionalInfo/AddInfoValue" >
  <OutDataType>OvCISearchKey</OutDataType>
  <InDataType>OvCISearchKey</InDataType>
  <KeyFieldOutVal>SAPInstNo</KeyFieldOutVal>
  <KeyFieldInVal>SAPInstNo</KeyFieldInVal>
</FieldMapping>
```

The following two attributes are used only when Solution Manager forwards an Incident to SAP Solution Manager.

```
<FieldMapping ExtHDField="IctIncidentAdditionalInfo/AddInfoValue" >
  <InDataType>InformationLog</InDataType>
  <KeyFieldInVal>SAPIncidentID</KeyFieldInVal>
</FieldMapping>
<FieldMapping ExtHDField="IctIncidentAdditionalInfo/AddInfoValue"
  ValueMappingId="IctIncidentAdditionalInfo/AddInfoValue
  /SAPIncidentStatus" >
  <InDataType>InformationLog</InDataType>
  <KeyFieldInVal>SAPIncidentStatus</KeyFieldInVal>
</FieldMapping>
```

The only attributes that do not have read-only status in the SAP Solution Manager are CI attributes, allowing IN-mode mapping (from SAP Solution Manager to Service Manager). The following table defines the available attributes:

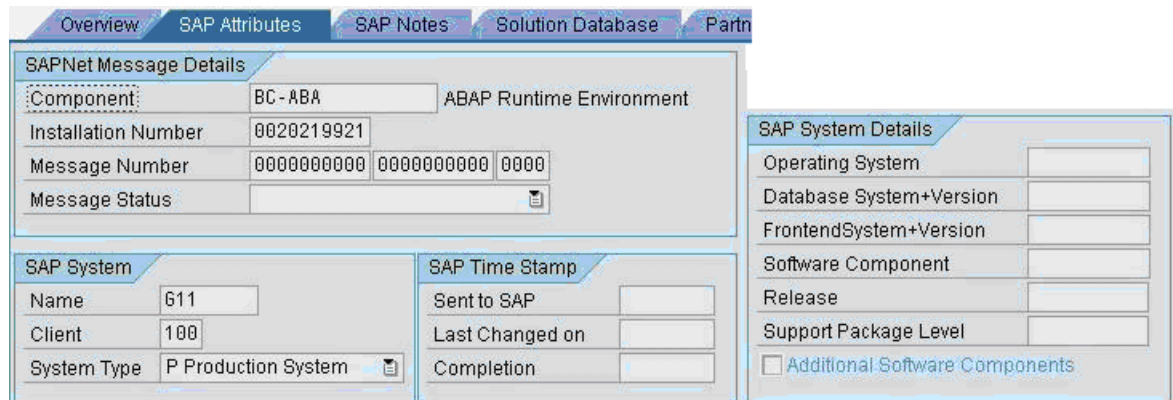
Table 5 Attribute Types of the SAP Solution Manager

AttributeType	Description
SAPComponent	SAP Component (e.g. SV-SMG-SUP)
SAPSystemID	SAP System ID
SAPSystemClient	Client of SAP System
SAPCategory	Category of the Incident
SAPSystemType	SAP System Type

Table 5 Attribute Types of the SAP Solution Manager

SAPInstNo	SAP Installation Number
SAPSubject	Subject of the Incident
SAPOperatingSystem	Operating System of SAP System
SAPDatabase	Database of SAP System
SAPFrontend	Frontendsystem and Version
SAPSoftwareComponent	Software Component
SAPSoftwareComponentRelease	Software Component Release
SAPSoftwareComponentPatch	Software Component Patch
SAPIncidentID	ID of the Incident at SAP (when forwarded to SAP)
SAPIncidentStatus	Status of the Incident at SAP (when forwarded to SAP)

In the SAP GUI most attributes are in the SAP Attributes tab.



The following example writes all incoming additional values of type SAPDatabase to the Journal in Service Manager:

```
<FieldMapping ExtHDFfield="IctIncidentAdditionalInfo/AddInfoValue" >
  <InDataType>InformationLog</InDataType>
  <KeyFieldInVal>SAPDatabase</KeyFieldInVal>
</FieldMapping>
```

The following example updates field CustomText03.

```
<FieldMapping ExtHDFfield="IctIncidentAdditionalInfo/AddInfoValue" >
  <InOvHDFfield>CustomText03</InOvHDFfield>
  <KeyFieldInVal>SAPDatabase</KeyFieldInVal>
</FieldMapping>
```

Changeable Mappings

The following mappings can be modified.

Table 6 Changeable mappings

Mapping	Description
IctHead/AgentID IctHead/ReporterID IctIncidentAttachment/PersonId IctIncidentStatement/PersonId	OutOvHDField/InOvHDField field name can be modified if the replacement field contains the ID of a Contact joined with a contact table that is exposed via ConfigurationManagement Web Service (defined in the default configuration). The AssigneeName field contains the operator name of Service Manager instead of the contacts name.
IctHead/ShortDescription	OutOvHDField/InOvHDField can be modified with any text field from Service Manager.
IctHead/RequestedEnd	Can be modified with any datetime field in the Service Manager.



Required Mappings: The following mappings are required and must not be changed.

- IctHead/Priority (the value mapping for this field mapping can be changed)
- IctIncidentSapNotes/item
- IctIncidentSolutions/item
- IctIncidentUrls/item
- IctIncidentAdditionalInfo/AddInfoValue (first 3 mappings)

Person Synchronization Details

SAP Solution Manager to Service Manager

Persons sent from SAP Service Manager can be mapped to person fields in Service Manager. When Person details are received, the corresponding contact record is found in Service Manager by querying the Configuration Management Web Service. The resolved contact ID must be set in the mapped field. The exchange web service describes persons with the following fields:

- Sex
- First name
- Last name
- Telephone
- Mobile phone
- Fax
- Email

Fields that are used to find persons in Service Manager:

- Email
- First name
- Last name

Persons are searched by all three fields. If no matching person is found in Service Manager or duplicates are found, then a notification is added to the Journal. For example, an empty email causes the following message in response to Journal updates:

```
Warning! Contact can not be found. Firstname,Lastname,Email fields should
not be empty. Invalid contact: FirstName: "Nicholas" LastName: "Brown"
Phone number: "(770) 954-4588" Fax number: "(770) 954-4590" ...
```

SMSSMEX does not create Persons or Contacts. An operator-type lookup is enforced only for the AssigneeName field.

Mapping from Service Manager to SAP Solution Manager is performed in the same way. The ID of the Person field in the Service Manager is used to make an additional call to Configuration Management WS to get all details about the Person. The collected data is forwarded to the Solution Manager. In SAP Solution Manager the ID of the Person is checked. If the ID is

- Known: Solution Manager assigns an existing record to the Incident.
- Not known: Solution Manager tries to resolve a Person via the email field. If this is not possible, a new Person is created.

SMSSMEX Version

To find out the version of the SMSSMEX service in Tomcat, do one of the following:

- Open `<SMSSMEX_installDir>\tomcat\webapps\ovictex\WEB-INF\lib\ovictex.war` with a zip tool. The war file MANIFEST.MF file contains the version information.
- Go to the Status page.

B Installing and Configuring SAPCRYLIB

To install SAPCRYLIB (see <https://service.sap.com/sap/support/notes/510007>) do the following:

- 1 Download SAPCRYLIB from the website “SAP Download Area - SAP Cryptographic Software” at https://websmp101.sap-ag.de/~form/handler?_APP=00200682500000000917&_EVENT=DISPLAY.

- 2 Use `sapcar.exe` to extract the SAR file:

```
sapcar -xvf sarfile_name
```

- 3 Copy the extra files to `\usr\sap\[Instance folder]\DVEBMGS00\exe`.
- 4 In transaction `/nrz10` in the Profile field, select the profile with `prof.type` of “Instance profile”.
- 5 Select **Extended maintenance** in Edit Profile.
- 6 Click **Change**.
- 7 Add the following parameters:

```
ssf/name          = SAPSECULIB
ssf/ssfapi_lib    = $(DIR_EXECUTABLE)\sapcrypto.dll
```

- 8 Restart the system.
- 9 Go to transaction `/nsmicm`.
- 10 Select the menu entry **GOTO** and select **Services** or press **SHIFT+F1**.
- 11 If the **HTTPS** port is not listed, then configure the profile. Add or change the following parameter:

```
icm/server_port_2 PROT=HTTPS,PORT=[SSL Port]
```
- 12 In transaction `/nsmicm` select from the **Administration** → **ICM** → **Restart** → **Yes** to restart ICM.

C Logging

The following describes the location of log files.

- Windows: If you start SMSSMEX from
 - **setup -startup**
%SMSSMEX_HOME%/logs/smssmex.log.<date>
 - Tomcat
%SMSSMEX_HOME%/tomcat/logs/smssmex.log.<date>
- Unix: If you start SMSSMEX from
 - **setup.sh -startup**
%SMSSMEX_HOME%/logs/smssmex.log.<date>
 - Tomcat
%SMSSMEX_HOME%/tomcat/logs/smssmex.log.<date>

D Deploying Button Icons

SMSSMEX enhances the functionality of Service Manager by adding some buttons in incident form to trigger message exchange related actions. The icons for the buttons are provided additionally in the release package (under `<SMSSMEX1.10 Release Package>\icons` folder). You can deploy them to the Service Manager Client manually.

Service Manager has two client applications: Windows Client and Web Client. For each of the clients, the icons should be deployed separately.

Windows Client

Copy button icons from `<SMSSMEX1.10 Release Package>\icons` folder to `<Client_Home>\plugins\com.hp.ov.sm.client.eclipse.user_9.xx\src\resources\icons\obj16`

For more information, see *Service Manager Installation Guide*.

Web Client

Copy the button icons from `<SMSSMEX1.10 Release Package>\icons` folder to `<WebApps_Root>\webtier-<version>\images\obj16` directory.

E SAP System Landscape Directory Registration

System Landscape Directory is the central information repository for your system landscape (Software Catalogue). It contains information about all installable and installed components in a system landscape. This section describes how to register this integration into System Landscape Directory.



The SAP System Landscape Directory Registration is a new feature in SMSSMEX v1.02. However, this feature is optional. If you do not deploy the SAP System Landscape Directory, the functionality of SMSSMEX v1.10 patch 2 will not be affected.

Prerequisites

Service Landscape Directory is running.

Registering System Landscape Directory

- 1 Browse to the *<SMSSMEX1.10 Release Package>* and copy the SLDReg folder to your computer.
- 2 Open the SLDReg folder. Modify the `HPSMISystem.properties` file according to the parameter descriptions in the file. For example, update the `ComputerName` variable to the host name which is running SMSSMEX.

```
ComputerName = <your computer name>
```

- 3 Run the following command to compile XML file:

```
java -cp SLDReg.jar com.hp.sm.sld.XMLGenerator
```

After execution, `HPSMI.xml` is generated.

- 4 Run the following command to register System Landscape Directory:

```
java -cp SLDReg.jar com.hp.sm.sld.Register <SLD_HOST> <SLD_HTTPPORT>  
<UserName> <Password>
```

In this command:

- `<SLD_HOST>` is the host name of the Service Landscape Directory server.
- `<SLD_HTTPPORT>` is the http port of the service landscape directory service.
- `<UserName>` is the name that you use to log in to the server.
- `<Password>` is the password that you use to log in to the server.

