HP NGOSS Software

Incident & Problem Management Extension

SOA Integration Guide

Edition: 1.0

July-2010

Legal Notices

Warranty

The information contained herein is subject to change without notice. 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.

License Requirement and U.S. Government 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

Trademark Notices

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

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

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

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

Contents

Preface

This document describes the installation and configuration process for the HP Problem Management-SOA Integration.

Intended Audience

This manual provides information needed for the system integrators to install and set-up SOA to manager SM web services.

Working knowledge of web service and basic system administration on Service is required. Installation of the pre-requisite products may require additional skills.

Unless otherwise specified, all operations and commands described in this guide must be performed by a system administrator logged in with general system privileges, i.e., on Unix as user root or on Windows as system Administrator.

Document Structure

The chapters in this document are structured as followings:

- Chapter 1 provides an overview of this SOA integration
- Chapter 2 provides planning of the integration.
- Chapter 3 provides details of installation and configuration.
- Chapter 4 provides information on how to verify that the installation and configurationis successful (a simple demo is used).
- Chapter 5 provides information on how to remove this integration

References and Associated Documents

Table 1 References and Associated Documents

Abbreviation	Name
[SOA Install Guide]	SOA Installation Guide
[SOA User Guide]	SOA User Guide

Software Versions

The software versions referred to in this document are as follows:

IPM	Operation system
1.1	Server: Windows2003/2008 Client: Windows XP, Vista, Windows 7

Support

Please visit our HP Software Web site at: http://www.hp.com/go/hpsoftwaresupport for contact information, and details about HP Software products, services and support.

- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Chapter 1
Overview

1.1 Purpose

The purpose of this document is to provide information about the installation and configuration tasks on HP NGOSS Incident & Problem Management Extension-SOA Integration version 1.0.0.

1.2 Integration Structure

The HP SM-SOA PE Integration is composed by following components:

- HP Service Oriented Architecture Policy Enforcer 3.10

(hereinafter as HP SOA PE)

SM web service will be implemented in SOA and SOA will be responsible for security and performance management for SM web service.

- HP Service Management 7.11/9.20 (hereinafter as HP SM)

HP NGOSS Incident & Problem Management Extension is a product developed and run on HP SM Server.(hereinafter as IPM)

- TT client(HP or third party Telecom products or software)

TT Client can be different software in different implementations. It will use SM incident web service to create incident in SM. A simple demo is used in this document to do the testing on SOA integration.

The following diagram illustrates HP SM-SOA PE Integration architecture:

The TT request from TT Client processed along the blue arrows.

The TT Update/Close Notification from HP SM processed along the pink arrows.

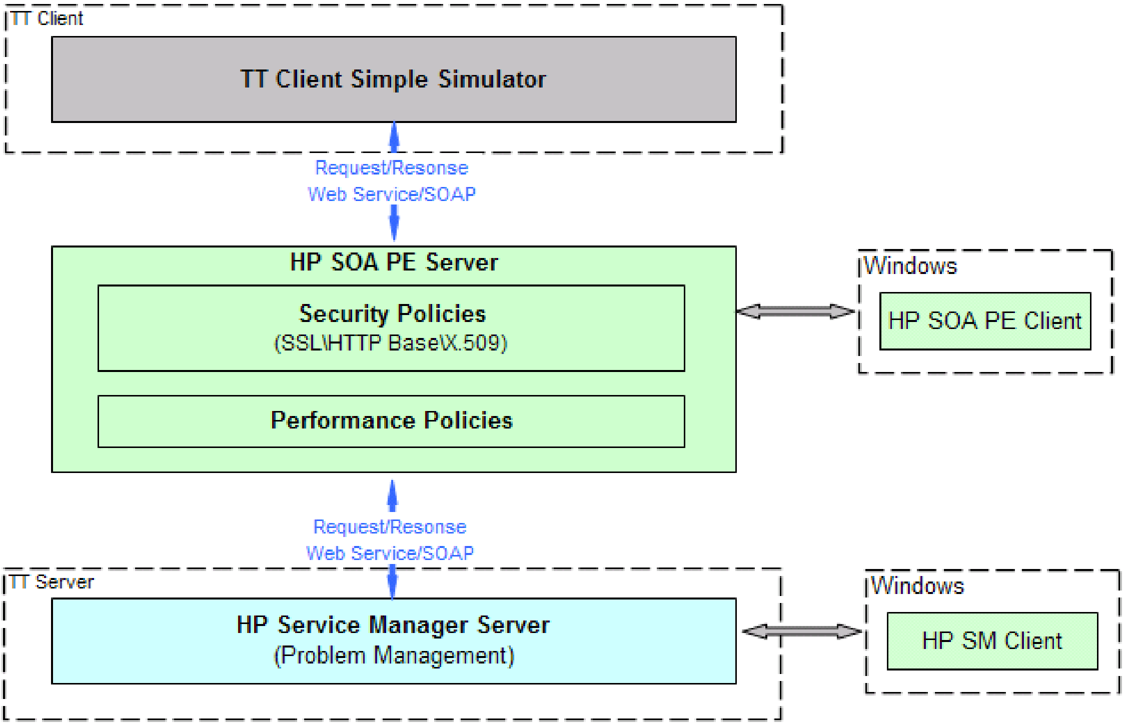


Figure 1 SM-SOA PE Structure Diagram

1.3 Usage Scenario

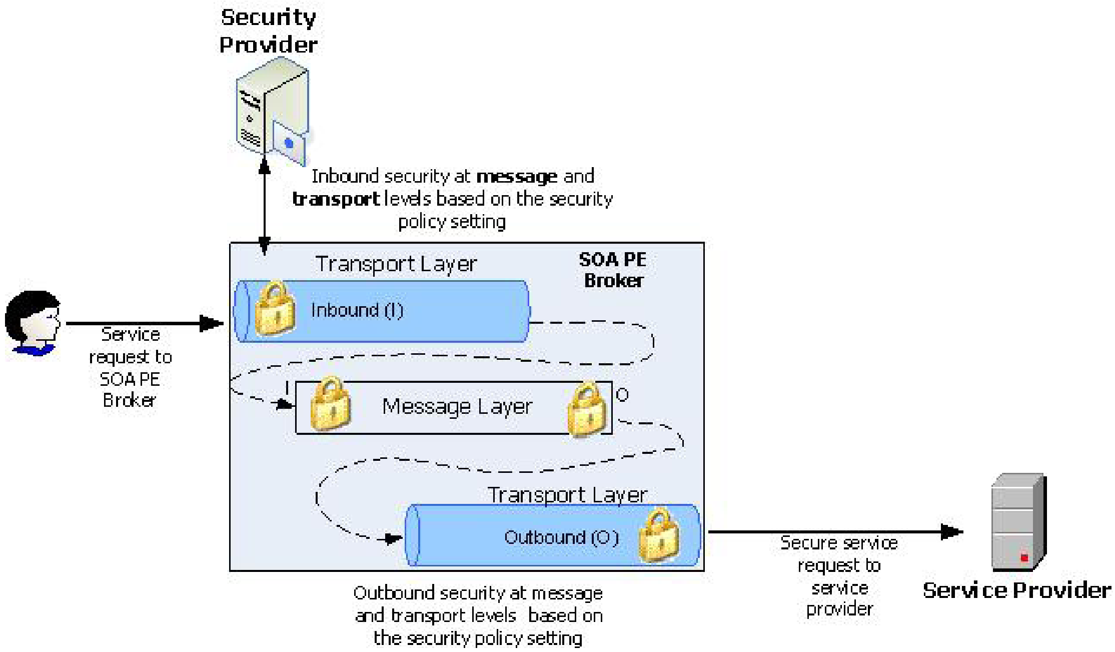
There are two management functions provided by SOA which can be used for SM incident web service in this integration. They are security and performance.

1.3.1 Security Management

SOA PE allows you to implement Web service security at the transport level by providing the Transport Security policy.

The Transport Security policy allows you to implement security at the inbound and outbound levels as discussed in the following sections.

The following diagram illustrates SOA PE security policy:


Security Provider
Inbound security at message and transport levels based on the security policy setting
Transport Layer
SOA PE Broker
Inbound (I)
Service request to SOA PE Broker
I
Message Layer
O
Transport Layer
Outbound (O)
Secure service request to service provider
Service Provider
Outbound security at message and transport levels based on the security policy setting

For this SM Incident web service integration:

1.3.1.1 OutBound HTTP Basic Authentication

Http basic authentication is requried for SM will do basic username and password authentication when incident web service is called.

SOA PE will add http basic authentication in message sent to SM.

1.3.1.2 InBound HTTP Basic Authentication

SOA PE will authenticate inbound message using a username and password.

1.3.1.3 InBound SSL

SOA PE will authenticate inbound message using SSL.

The message transportation between SOA and TT Client will be on SSL. Thus, we can ensure the message security when integration with SM.

1.3.1.4 InBound SSL With Basic Authentication

Like section 1-3-1-3, this will use SSL with basic authentication which is more secure authentication.

1.3.1.5 InBound SSL With X.509

Like section 1-3-1-5, this will use SSL with X.509 to replace basic authentication which is the most secure authentication.

1.3.2 Performance Management

Like security policy, SOA PE also allow you to implement some policies to monitor and control web service. That is performance management.

1.3.2.1 Scheduled Availability

You can use a scheduled availability policy to allow or deny access to a service based on the scheduled availability time period specified for that service.

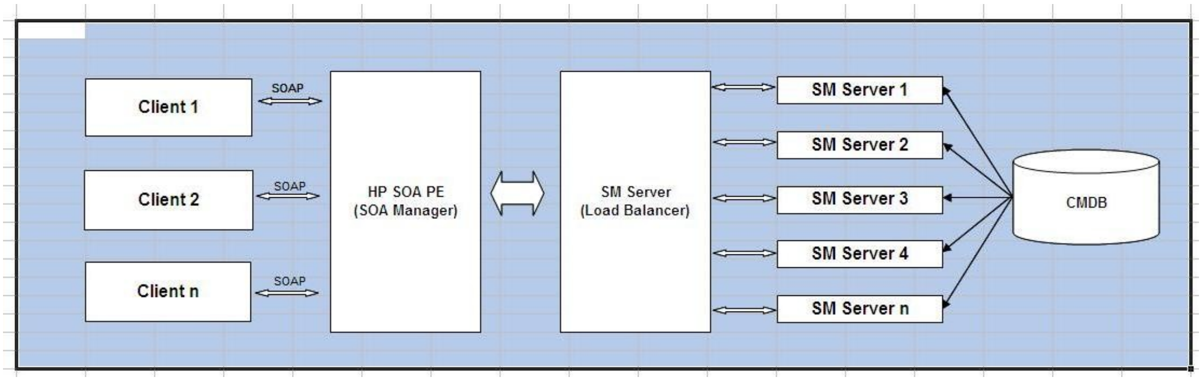
The Intermediary uses this policy to verify the availability of a service at that specific time. If the service is specified to be available, the Intermediary forwards the message from the client to the endpoint (SM). If the service is specified to be unavailable, the Intermediary rejects the message and sends a SOAP fault to the client.

1.3.2.2 Service Protection

You can use a service protection policy to limit access to endpoints being managed using a policy enforcement intermediary. You can use this type of a policy to specify the number of service requests that an intermediary can accept. After the limit specified for the number of service requests that the intermediary can accept is exceeded, SOA PE rejects the subsequent service request messages by sending a SOAP fault which prevents the managed endpoint from crashing or denying service requests. For example, you can specify the number of requests that a managed endpoint can accept in a day, a week, or in a month.

1.3.2.3 Load Balance

Load Balance will de implemented in SM side.



Chapter 2
Planning the Installation

2.1 Pre-requisites

Before installing and configuring the SOA integration with SM, there are some pre-requisites need to be checked.

1. Check the running environment of SOA PE server and Service Manager server.

Category	Hardware	OS version	Software version
SOA PE Server	X86 Server	Windows 2000/XP/Vista/2003/2008	HP SOA PE 3.10
Service Manager	X86 Server	Windows 2000/XP/Vista/2003/2008	HP Service Manager V6.1.x or up to V7.1
	Sun SPARC	Solaris	

2. Check the network connection between Service Manager server and SOA PE server is in normal status.

2.2 Installation Preparation

Following required products must be pre-installed successfully before configuring and executing Data Loading:

Table 2 Installation information list

Category	Description	Item	Sample	Comment
SOA PE Server	The server that SOA PE is running on, which can be windows OS or Unix OS.	Username	admin	
		Password	password	
		IP Address	16.173.245.33	Required when login to web interface
		Web Port	5002	Required when login to web interface
SOA PE Broker	The server that SOA PE Broker is running on. In default, it's the same server as SOA PE Server	Web Port	9032	Used in HTTP
		Secure web port	9033	Used in HTTPS

Table 2 Installation information list

Category	Description	Item	Sample	Comment
Service Manager Server	HP Service Manager Software	Host IP Address	16.173.245.33	
		Webservice port	13080	Ensure no port conflict
		SM User	falcon	Ensure to get the administrator permission
		Password		
		SM Incident web service WSDL URL	http://16.173.245.33:13080/SM/7/IncidentManagement.wsdl	

Chapter 3
Installation and Configuration

Following are the steps for installing and configuring this SOA integration with SM.

3.1 SOA Installation

Please refer to SOA_installation_guide for this installation. This should be done before you continue to do the following installation and configuration.

3.2 Login to SOA PE

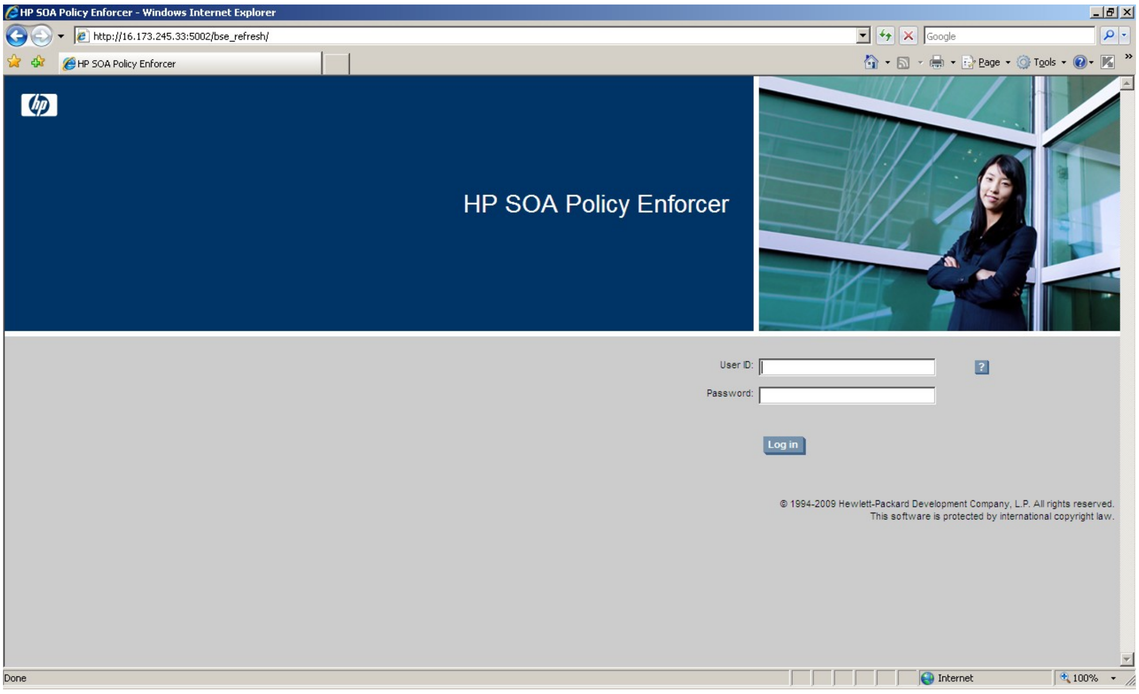
Before you login to SOA PE, you should start SOA PE server and SOA PE broker. In general, you can start through start->All programs->HP Software->SOA Policy Enforcer 3.10->SOA PE Server and SOA PE Broker.

The URL of web management of SOA will be http://<ip_address_server>:<port>/bse_refresh/.

Ip address of server and port should be get according to section 2-2 installation preparation.

The default port is 5002. The default user ID and password is admin and password.

The login interface will be like below one.



© 1994-2009 Hewlett-Packard Development Company, L.P. All rights reserved.
This software is protected by international copyright law.

3.3 SM Web Service Integration

This section provides detail steps for installing and configuring SM Incident web service in SOA.

You can configure other web service like this.

The SM incident web service WSDL URL :

http://16.173.245.33:13080/SM/7/IncidentManagement.wsdl. This is got in section 2-2 installation preparation.

3.3.1 Create an Policy Enforcement Intermediary Group

To create a policy enforcement intermediary group for one SM integration project, follow these steps:

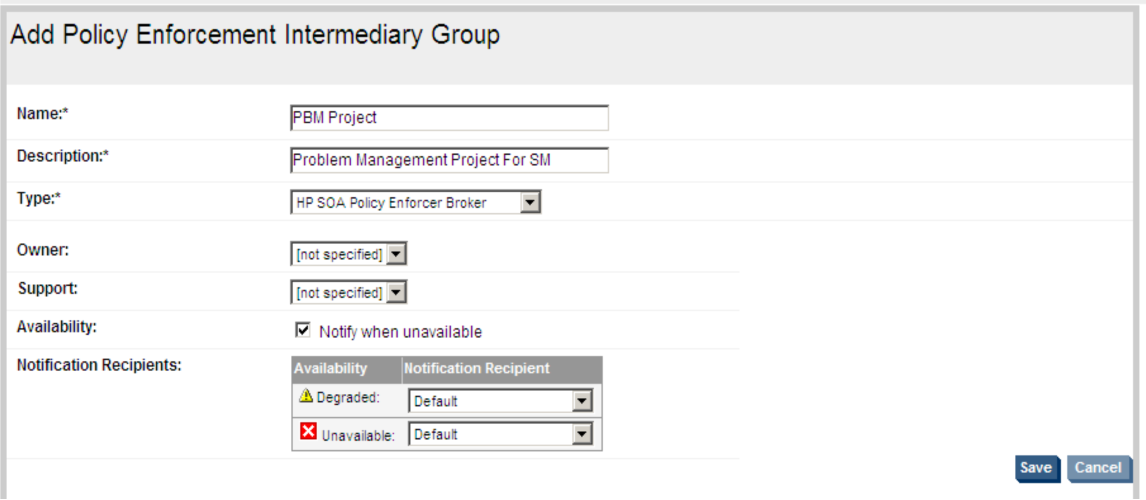
1. From the Actions drop-down menu, click Add Policy Enforcement Intermediary Group. The Add Policy Enforcement Intermediary Group screen opens.

2. Complete the following fields and click save.

Name: You can input project name, like PBM Project.

Description: Input the description about the project or whatever you want.

Below is a sample:



Add Policy Enforcement Intermediary Group

Name:*	PBM Project
Description:*	Problem Management Project For SM
Type:*	HP SOA Policy Enforcer Broker
Owner:	[not specified]
Support:	[not specified]
Availability:	☑ Notify when unavailable
Notification Recipients:	

Availability	Notification Recipient
⚠ Degraded:	Default
☒ Unavailable:	Default

3.3.2 Create an Broker Instance

After the intermediary group is created, you can register a policy enforcement intermediary group for the broker.

1. From the View drop-down menu, click Policy Enforcement Points. The Policy Enforcement Points Summary screen opens.

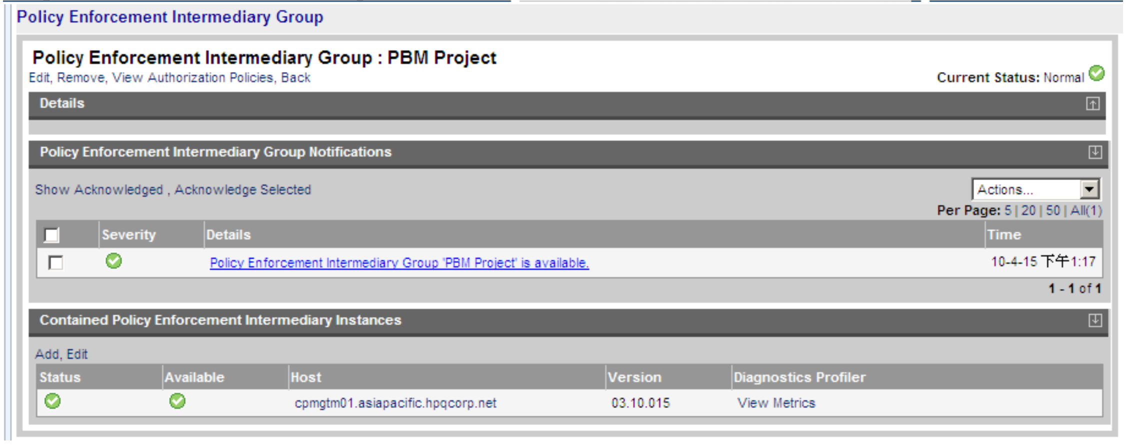
2. Click the policy enforcement intermediary group which is just created in the previous step. The Policy Enforcement Intermediary Group screen opens.

3. Click Add under Contained Policy Enforcement Intermediary Instances. The Add Policy Enforcement Instance screen opens.

4. Input the broker ip address and web port. Click add.

5. The web services contained in the broker will be listed. And click add to finish this creation.

After creation, click Policy Enforcement Points and then click the group. The group screen opens. Refer to below sample:



Policy Enforcement Intermediary Group

Policy Enforcement Intermediary Group : PBM Project

Edit, Remove, View Authorization Policies, Back

Current Status: Normal ✓

Policy Enforcement Intermediary Group Notifications

Show Acknowledged , Acknowledge Selected
Actions...
Per Page: 5 | 20 | 50 | All(1)

□	Severity	Details	Time
□	✓	Policy Enforcement Intermediary Group 'PBM Project' is available.	10-4-15 下午1:17

1 - 1 of 1

Contained Policy Enforcement Intermediary Instances

Status	Available	Host	Version	Diagnostics Profiler
✓	✓	cpmgtm01.asiapacific.hpqcorp.net	03.10.015	View Metrics

3.3.3 Create a Business Service

You can create a business service together with creation on web service.

Or you can create a business service first as the following steps:

1. From the View drop-down menu, Click Business Services. The Business Services screen opens.

2. Click Add. The Add New Business Service screen opens.

3. Input the name of the business service. For example, input Service Manager for this integration. For other fields, you can leave them in default.

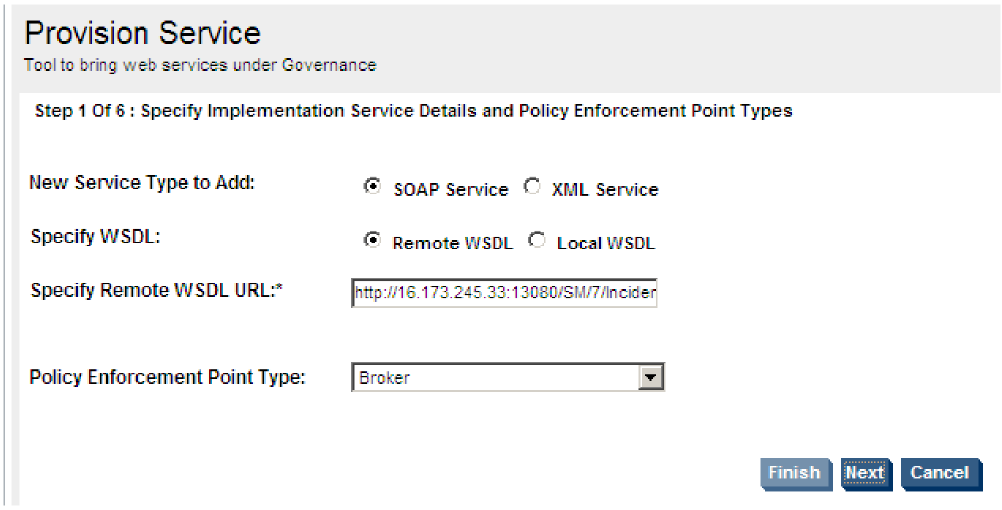
4. Click Add. New Business Service will be added and Business Serives screen displays again.

3.3.4 Create a Web Service

In this step, SM Incident web service will be configured in SOA. The URL of Incident web service WSDL is required according to section 2-2.

1. From the Actions drop-down menu, Click Provison Service. The Provison Service screen opens.

2. Step 1 of 6 : Input SM Incident WSDL URL in Specify Remote WSDL URL. Leave other selections in default.



Provision Service

Tool to bring web services under Governance

Step 1 Of 6 : Specify Implementation Service Details and Policy Enforcement Point Types

New Service Type to Add: ● SOAP Service ○ XML Service

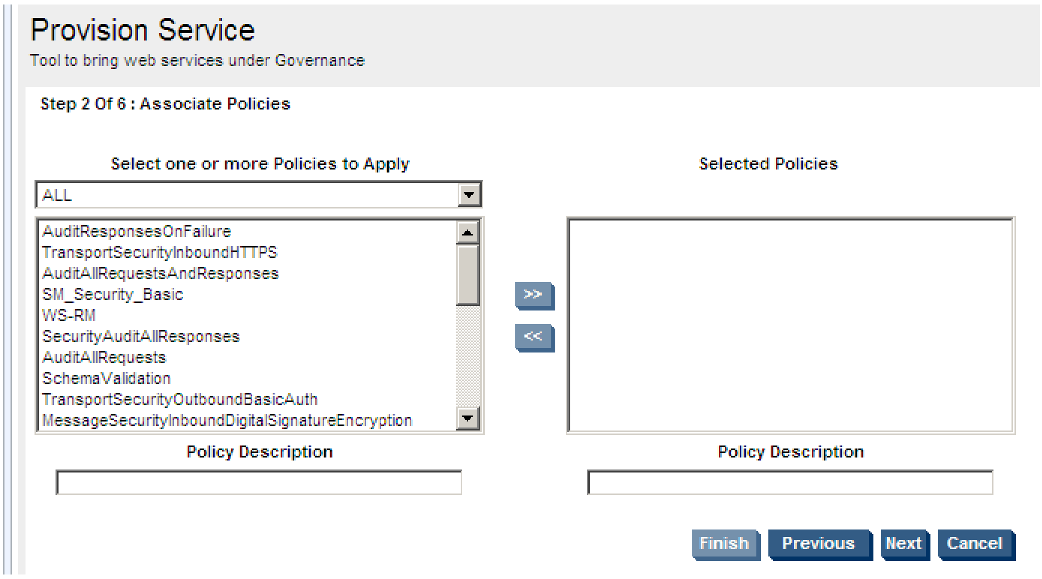
Specify WSDL: ● Remote WSDL ○ Local WSDL

Specify Remote WSDL URL:* http://16.173.245.33:13080/SM/7/Incider

Policy Enforcement Point Type: Broker

3. Click Next, SOA PE will check the URL you input. And if this URL is available, you will be directed to step 2 of 6.

You can associate some policies in this step. You can do it later after web service creation. The configuration on security and performance policies is described in section 3-4.



Provision Service

Tool to bring web services under Governance

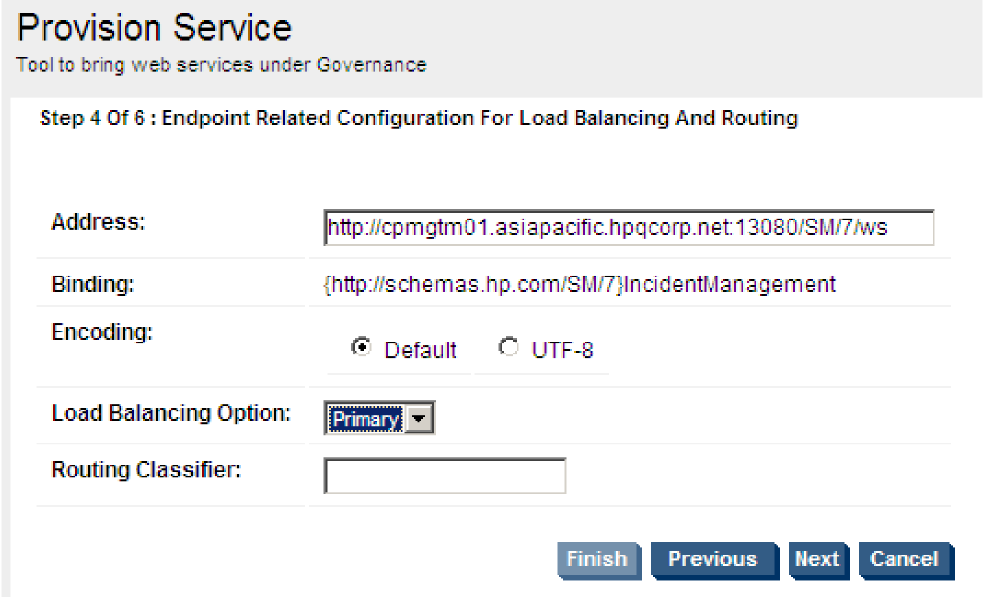
Step 2 Of 6 : Associate Policies

Select one or more Policies to Apply: ALL

AuditResponsesOnFailure
TransportSecurityInboundHTTPS
AuditAllRequestsAndResponses
SM_Security_Basic
WS-RM
SecurityAuditAllResponses
AuditAllRequests
SchemaValidation
TransportSecurityOutboundBasicAuth
MessageSecurityInboundDigitalSignatureEncryption

4. Click Next to step 3 of 6. In this step, you can input http path and name for this web service. You can leave them in default.

5. Click Next to step 4 of 6. Leave them in default.



Provision Service

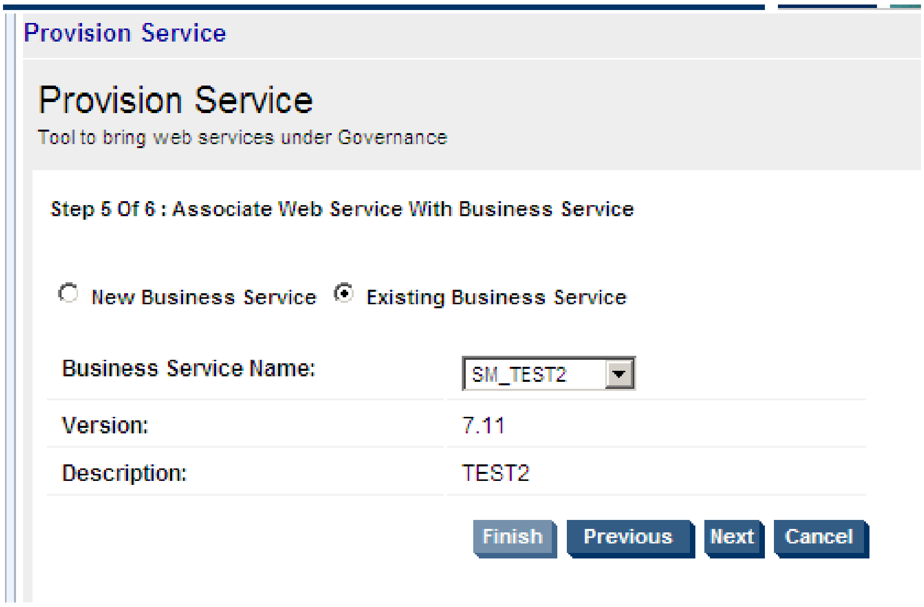
Tool to bring web services under Governance

Step 4 Of 6 : Endpoint Related Configuration For Load Balancing And Routing

Address:	http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws
Binding:	{http://schemas.hp.com/SM/7}IncidentManagement
Encoding:	● Default ○ UTF-8
Load Balancing Option:	Primary
Routing Classifier:	

6. Click Next to step 5 of 6. Associate Web Service With Business Service

You can select existed business service or create new business service here.



Provision Service

Provision Service

Tool to bring web services under Governance

Step 5 Of 6 : Associate Web Service With Business Service

○ New Business Service ● Existing Business Service

Business Service Name:	SM_TEST2
Version:	7.11
Description:	TEST2

7. Click Next to step 6 of 6. You can choose save or deploy only or delpoy and activate here.

8. Click finish to finish this web service configuration.

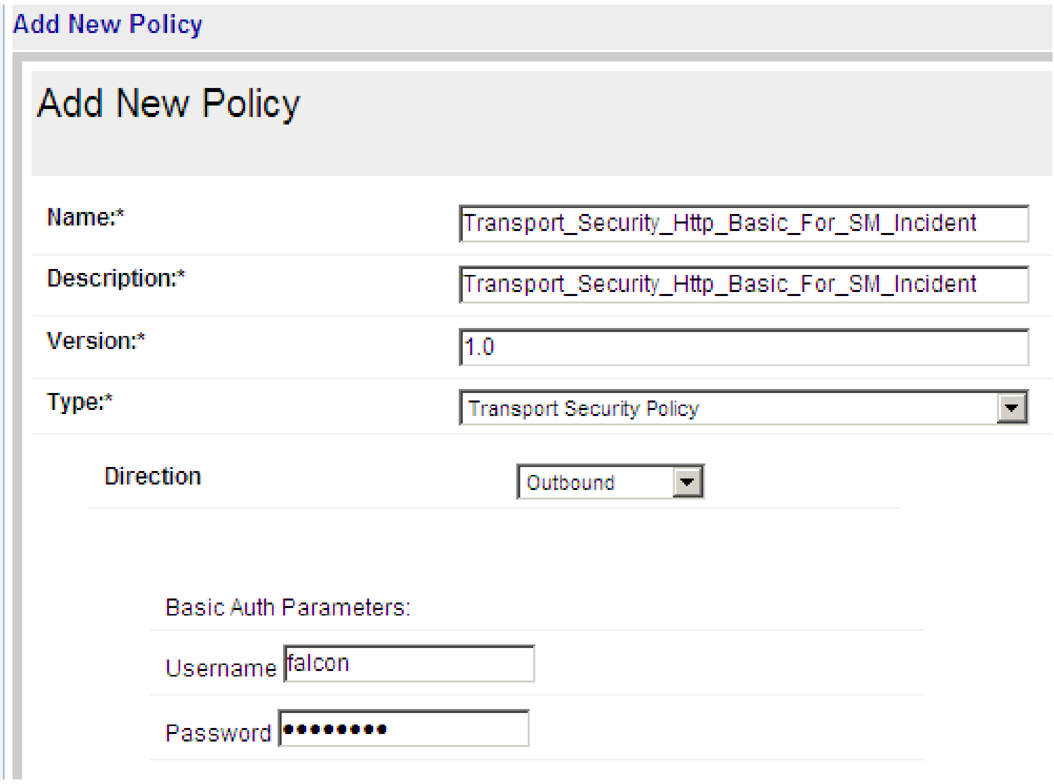
3.4 Security Configuration

3.4.1 Configure OutBound Http Basic authentication Policy

1. From Actions drop-down menu, Click Add policies. The Add New Policy screen opens.

2. Select Transport Security Policy in type, and then select Outbound for direction. Input the name, description and version. For username and password, input the SM username and password. The username and password will be put in http head and authenticated by SM.

Below is an example.


Add New Policy

Add New Policy

Name:*	Transport_Security_Http_Basic_For_SM_Incident
Description:*	Transport_Security_Http_Basic_For_SM_Incident
Version:*	1.0
Type:*	Transport Security Policy
Direction	Outbound

Basic Auth Parameters:

Username	falcon
Password	●●●●●●●●

3. Click Add to finish policy creation.
4.

3.4.2 Configure InBound Http Basic authentication Policy

There has been a pre-configured policy named " TransportSecurityInboundHTTPBasicAuth" which can be used when you do association on web service.

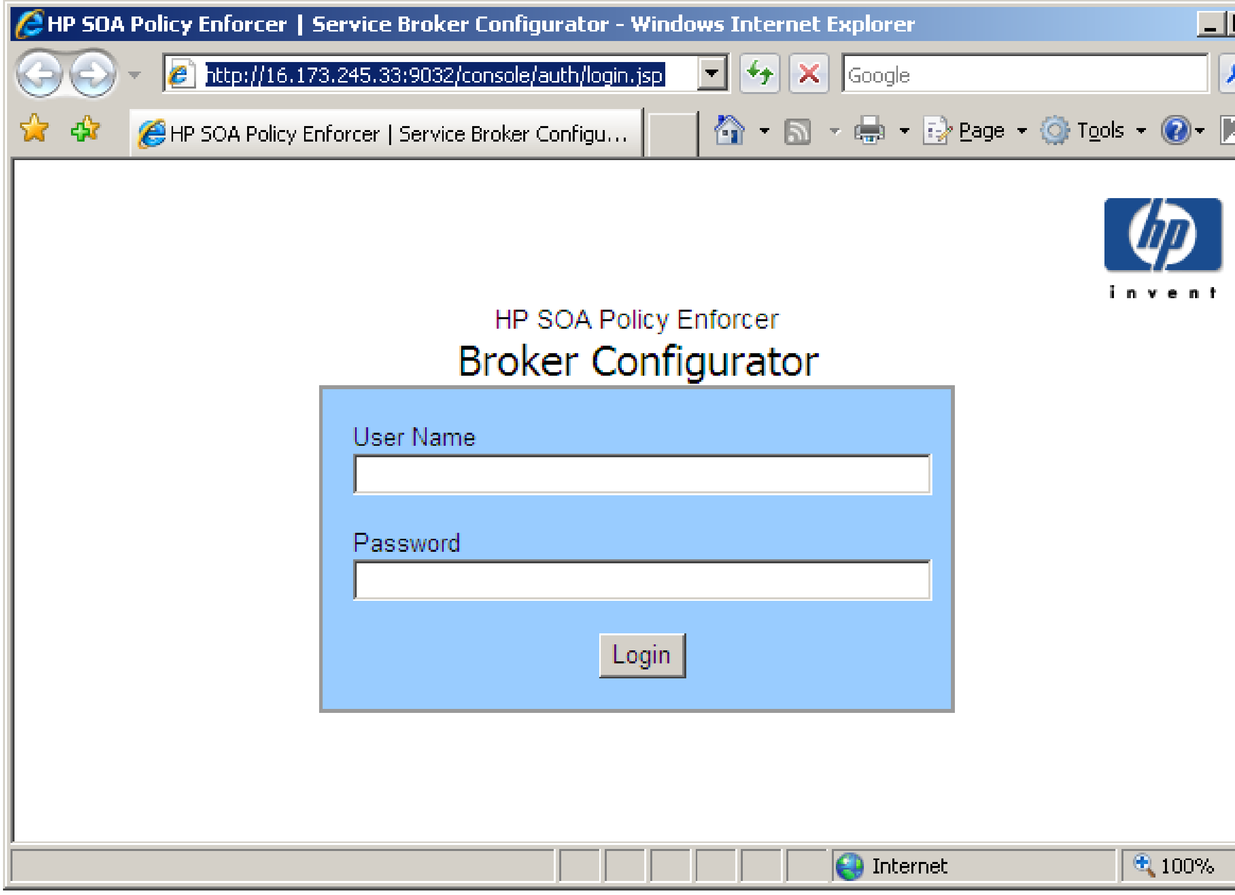
It will use SOA PE login username and password to authenticate inbound message.

So you need to configure http basic authentication as SOA PE login username and password in TT client.

3.4.3 Setting Up SSL in SOA

1. Login to SOA PE Broker. The URL of web login interface should be like http://<ip_server_address>:<port>/console/. The username and password are the same ones which are used to login to SOA PE Server. The default ones are admin/password.

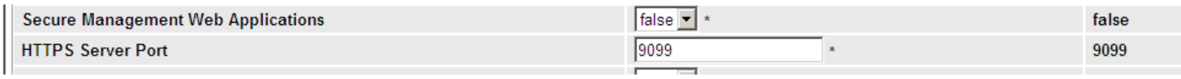
For ip server address and broker port, refer to 2-2 installation preparation. They should be get before this configuration. Below is the web login page:



HP SOA Policy Enforcer | Service Broker Configurator - Windows Internet Explorer
http://16.173.245.33:9032/console/auth/login.jsp
Google
HP SOA Policy Enforcer | Service Broker Configu…
Page
Tools
invent
HP SOA Policy Enforcer
Broker Configurator
User Name
Password
Login
Internet
100%

2. Afer login, click HTTP settings at the right of top menu.

3. Configure HTTPS Server Port and click save. Below is a sample:



Secure Management Web Applications	false *	false
HTTPS Server Port	9099 *	9099

4. Click SSL settings at the right of top menu.

5. Configure all the requried fields. You should have a basic knowledge on SSL, keystore, truststore and java keytool before do this step. You can refer to Appendix A (Creating a Java Key Store) of SOA user guide about how to create keys. The Appendix A of this document guide you how to create a key and certificate by java keytool for testing.

Keystore should be server's keystore. (SOA PE server).

Truststore should be client's truststore. (TT Client server)

6. Click save and restart SOA PE Broker.

3.4.4 Configure InBound SSL Policy

There has been a pre-configured policy named " TransportSecurityInboundHTTPS" which can be used when you do association on web service.

It will request SSL when inbound message comes.

3.4.5 Configure InBound SSL with Basic authentication Policy

There has been a pre-configured policy named ” TransportSecurityInboundHTTPSBasicAuth” which can be used when you do association on web service.

It will request SSL when inbound message comes. And it will use SOA PE login username and password to authenticate inbound message.

So you need to configure http basic authentication as SOA PE login username and password in TT client.

3.4.6 Configure InBound SSL with X.509 Policy

There has been a pre-configured policy named ” TransportSecurityInboundHTTPSX509” which can be used when you do association on web service.

It will request SSL when inbound message comes. And it will authenticate inbound message by X.509 certificate. The X.509 should be configured in section 3-4-3 Setting Up SSL in SOA.

3.4.7 Associate Security Policy

1. From View drop-down menu, Click Web Service. And then click SM IncidentManagement web service. The Web Service Configuration Detail View screen opens.

2. Click configuration tab. From Policies drop-down menu, Click attach/remove polcies. The Select policies to be associated with IncidentManagement Web Service screen opens.

You can select which security policy you want to associate to SM Incident web service to implement different securities.

For SSL, selcect TransportSecurityInboundHTTPS.

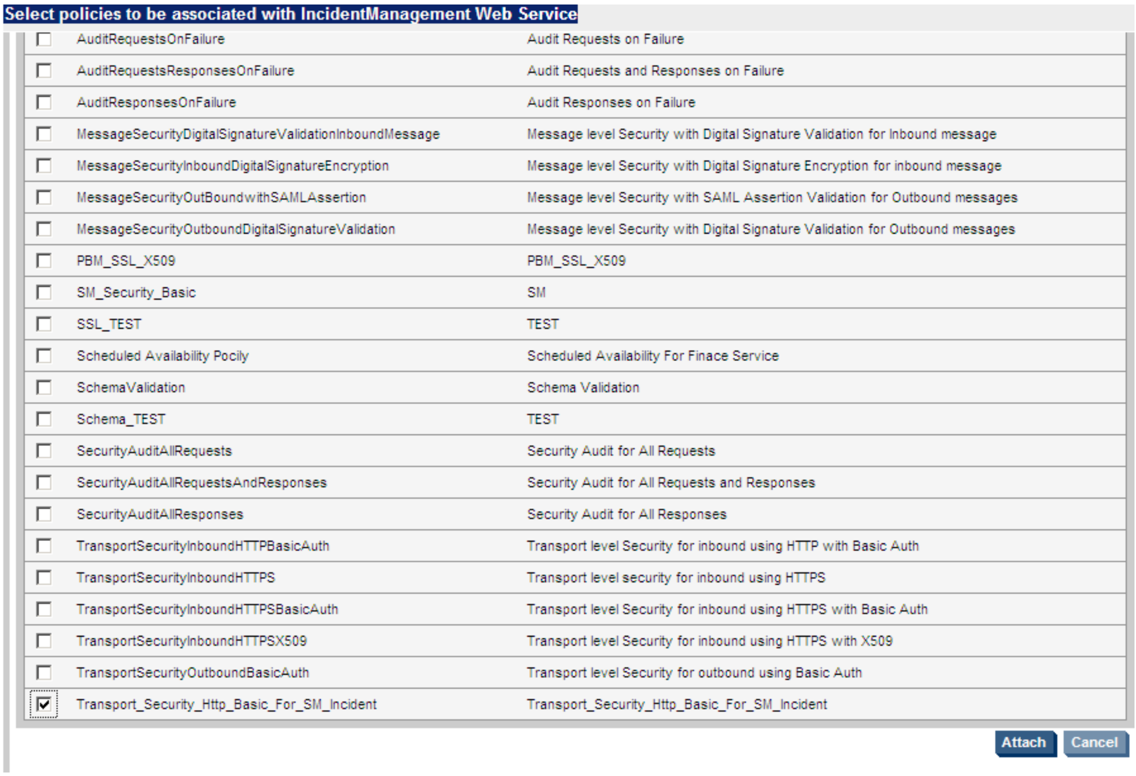
For SSL with basic authentication, select TransportSecurityInboundHTTPSBasicAuth.

For SSL with X.509, select TransportSecurityInboundHTTPSX509.

For Http basic auth, select TransportSecurityInboundHTTPBasicAuth.

Note that you can only select one policy from the above mentioned policies to ensure the security policies are not conflicted.

The screen like this:



Select policies to be associated with IncidentManagement Web Service

□	AuditRequestsOnFailure	Audit Requests on Failure
□	AuditRequestsResponsesOnFailure	Audit Requests and Responses on Failure
□	AuditResponsesOnFailure	Audit Responses on Failure
□	MessageSecurityDigitalSignatureValidationInboundMessage	Message level Security with Digital Signature Validation for Inbound message
□	MessageSecurityInboundDigitalSignatureEncryption	Message level Security with Digital Signature Encryption for inbound message
□	MessageSecurityOutBoundwithSAMLAssertion	Message level Security with SAML Assertion Validation for Outbound messages
□	MessageSecurityOutboundDigitalSignatureValidation	Message level Security with Digital Signature Validation for Outbound messages
□	PBM_SSL_X509	PBM_SSL_X509
□	SM_Security_Basic	SM
□	SSL_TEST	TEST
□	Scheduled Availability Pocily	Scheduled Availability For Finace Service
□	SchemaValidation	Schema Validation
□	Schema_TEST	TEST
□	SecurityAuditAllRequests	Security Audit for All Requests
□	SecurityAuditAllRequestsAndResponses	Security Audit for All Requests and Responses
□	SecurityAuditAllResponses	Security Audit for All Responses
□	TransportSecurityInboundHTTPBasicAuth	Transport level Security for inbound using HTTP with Basic Auth
□	TransportSecurityInboundHTTPS	Transport level security for inbound using HTTPS
□	TransportSecurityInboundHTTPSBasicAuth	Transport level Security for inbound using HTTPS with Basic Auth
□	TransportSecurityInboundHTTPSX509	Transport level Security for inbound using HTTPS with X509
□	TransportSecurityOutboundBasicAuth	Transport level Security for outbound using Basic Auth
☑	Transport_Security_Http_Basic_For_SM_Incident	Transport_Security_Http_Basic_For_SM_Incident

3. Click Attach and click Redeploy to re-activate the web service with new policies.

3.5 Performance Configuration

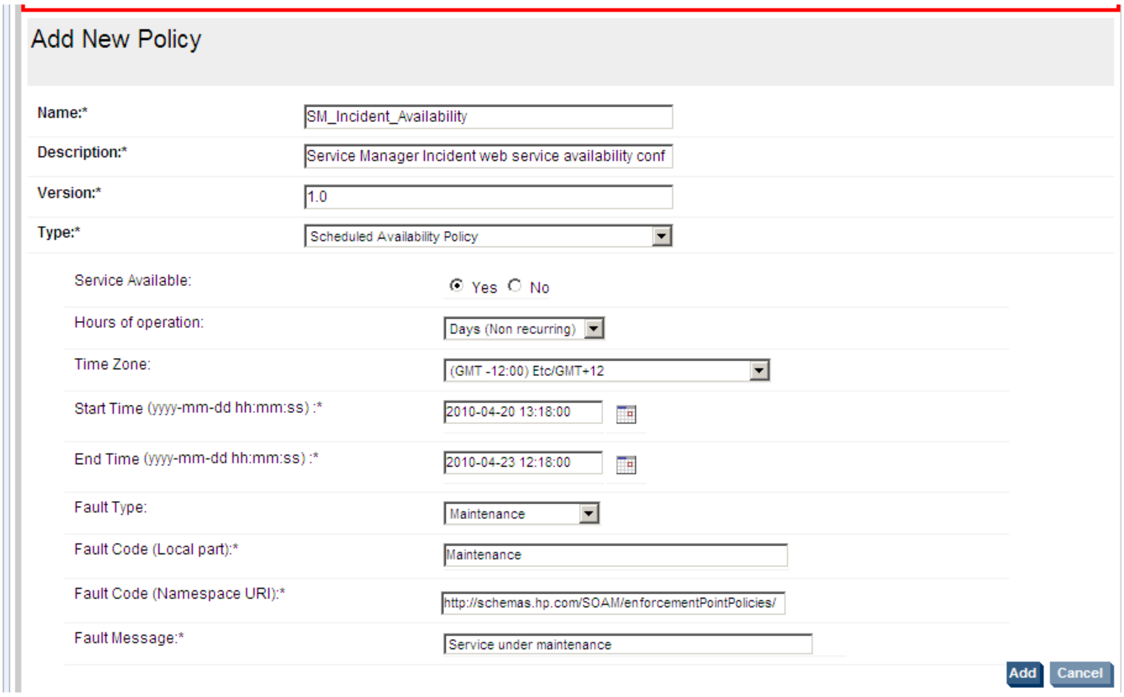
3.5.1 Configure Scheduled Availability Policy

1. From Actions drop-down menu, Click Add policies. The Add New Policy screen opens.

2. Select Scheduled Availability Policy in type, and some options will be displayed at the below area. You can input the time range of availability or unavailability. And also input a name for this policy.

Note that time zone should be the same as your server to make sure the policy works well.

Below is a sample:



Add New Policy

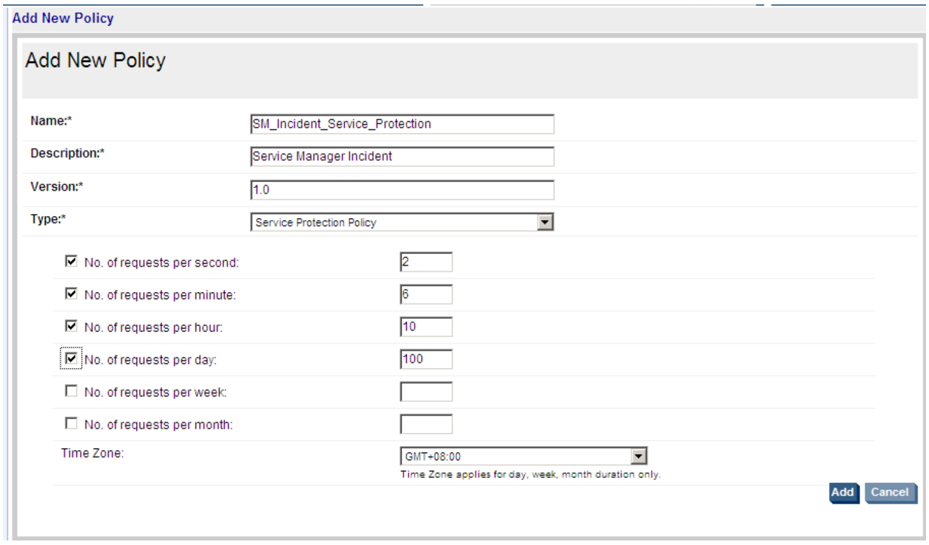
Name:*	SM_Incident_Availability
Description:*	Service Manager Incident web service availability conf
Version:*	1.0
Type:*	Scheduled Availability Policy
Service Available:	● Yes ○ No
Hours of operation:	Days (Non recurring)
Time Zone:	(GMT -12:00) Etc/GMT+12
Start Time (yyyy-mm-dd hh:mm:ss) :*	2010-04-20 13:18:00
End Time (yyyy-mm-dd hh:mm:ss) :*	2010-04-23 12:18:00
Fault Type:	Maintenance
Fault Code (Local part):*	Maintenance
Fault Code (Namespace URI):*	http://schemas.hp.com/SOAM/enforcementPointPolicies/
Fault Message:*	Service under maintenance

3. Click add to finish policy creation.

3.5.2 Configure Service Protection Policy

1. From Actions drop-down menu, Click Add policies. The Add New Policy screen opens.

2. Select Service Protection Policy in Type. Some options will display as the following snapshot, input your requirement.



Add New Policy

Add New Policy

Name:*	SM_Incident_Service_Protection
Description:*	Service Manager Incident
Version:*	1.0
Type:*	Service Protection Policy
☑ No. of requests per second:	2
☑ No. of requests per minute:	6
☑ No. of requests per hour:	10
☑ No. of requests per day:	100
☐ No. of requests per week:	
☐ No. of requests per month:	
Time Zone:	GMT+08:00 Time Zone applies for day, week, month duration only.

3. Click Add to finish policy creation.

3.5.3 Associate Performance Policy

You can refer to section 3-4-7 Associate Security Policy.

Select the policy you just created. As the sample, SM_Incident_Availability is for scheduled availability policy. SM_Incident_Service_Protection is for service protection policy.

3.6 Integration with TT Client

The TT Client can be different software in different situation. As usual, TeMIP is used as TT client. In the next chapter, post install verification, we will use a simple IncidentSample which is provided by SM itself to test this integration.

When you customize your TT Client, you need to configure new WSDL URL which is exposed by SOA instead of using the original SM web service URL.

To get the new WSDL URL, login to SOA PE Broker first. Refer to section 3-4-3 on how to login to SOA PE Broker.

After login, you will see the list of web services configured. Find out SM Incident web service according to column Name, the column Service Interface(WSDL) will display the URL.

Chapter 4
Post Install Verification

4.1 IncidentSample

There is a sample which can create incident through SM web service. It's provided by SM, located in <SM_Install_Path>\ Server\webservices\sample\sm7webservices\Axis2Sample\.

We can use this sample as TT Client to test SOA-SM integration on security and performance.

Read the file readme.txt first to understand that IncidentSample. It's located in this sample path.

4.2 Verify Security Management

According to the previous chapter section 3 to configure SM Incident web service in SOA.

4.2.1 Verify Http Basic authentication

Here are the steps how to verify http basic authentication.

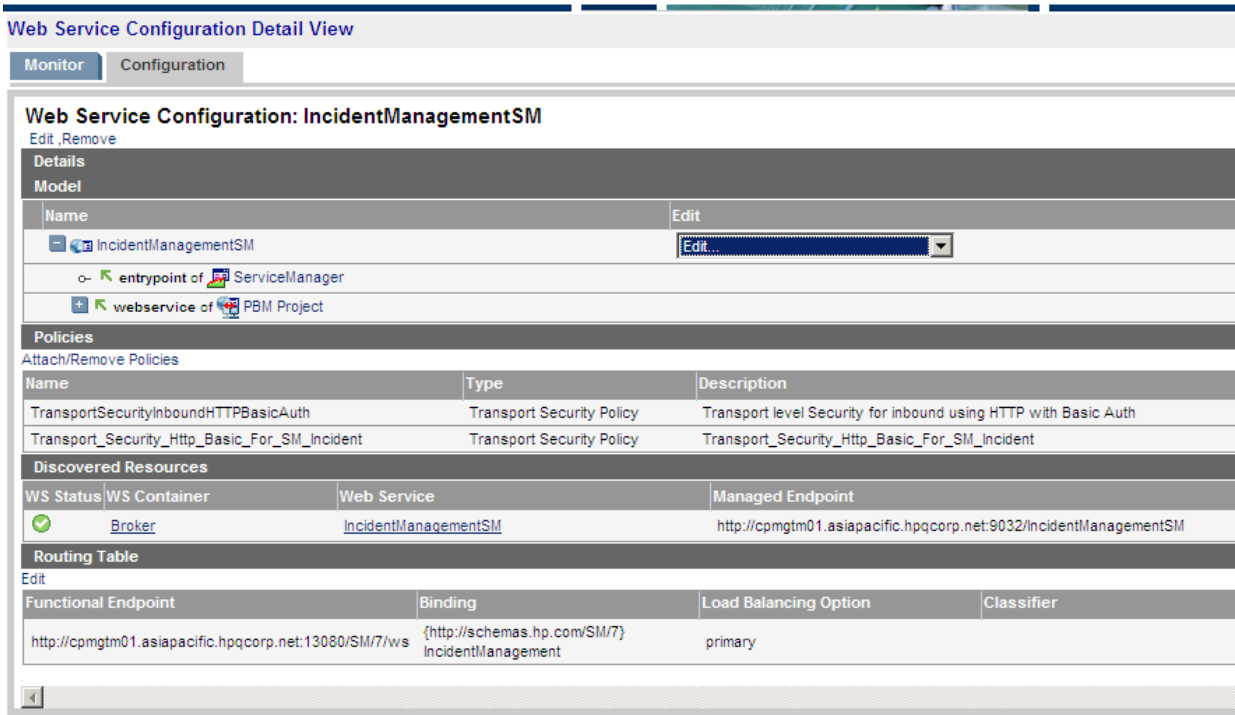
1. We name it as IncidentManagementSM in SOA. Do configuration as 3-3.

2. Then we need to associate two policies, TransportSecurityInboundHTTPBasicAuth and Transport_Security_Http_Basic_For_SM_Incident.

Transport_Security_Http_Basic_For_SM_Incident is a mandatory policy for SM Incident web service because SM will authenticate inbound message by http basic authentication. This policy need to be created. Refer to 3-4-1.

Transport_Security_Http_Basic_For_SM_Incident is a pre-configured policy.

Do association according to section 3-4-7. Below is the result of configuration:



Web Service Configuration Detail View

Web Service Configuration: IncidentManagementSM

Edit ,Remove

Details

Model

Name	Edit
IncidentManagementSM	Edit...
entrypoint of ServiceManager	
webservice of PBM Project	

Policies

Attach/Remove Policies

Name	Type	Description
TransportSecurityInboundHTTPBasicAuth	Transport Security Policy	Transport level Security for inbound using HTTP with Basic Auth
Transport_Security_Http_Basic_For_SM_Incident	Transport Security Policy	Transport_Security_Http_Basic_For_SM_Incident

Discovered Resources

WS Status	WS Container	Web Service	Managed Endpoint
✓	Broker	IncidentManagementSM	http://cpmgtm01.asiapacific.hpqcorp.net:9032/IncidentManagementSM

Routing Table

Edit

Functional Endpoint	Binding	Load Balancing Option	Classifier
http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws	{http://schemas.hp.com/SM/7} IncidentManagement	primary	

3. Then we need to modify IncidentSample to make it connect to SOA to create Incident.

We need to modify the source file “CreateIncidentSample.java” which is located at Axis2Sample\src\com\hp\sm\webservice\sample\incident\ to add http basic authentication.

For Http basic authentication, we have packaged a modified file in our installation package which is named as CreateIncidentSample_http_basic.java. You should do:

1) Modify its content. Find two lines:

basicauth.setUsername("admin");

basicauth.setPassword("password")

Modify the username and password of SOA PE to yours.

2) Rename it as CreateIncidentSample.java.

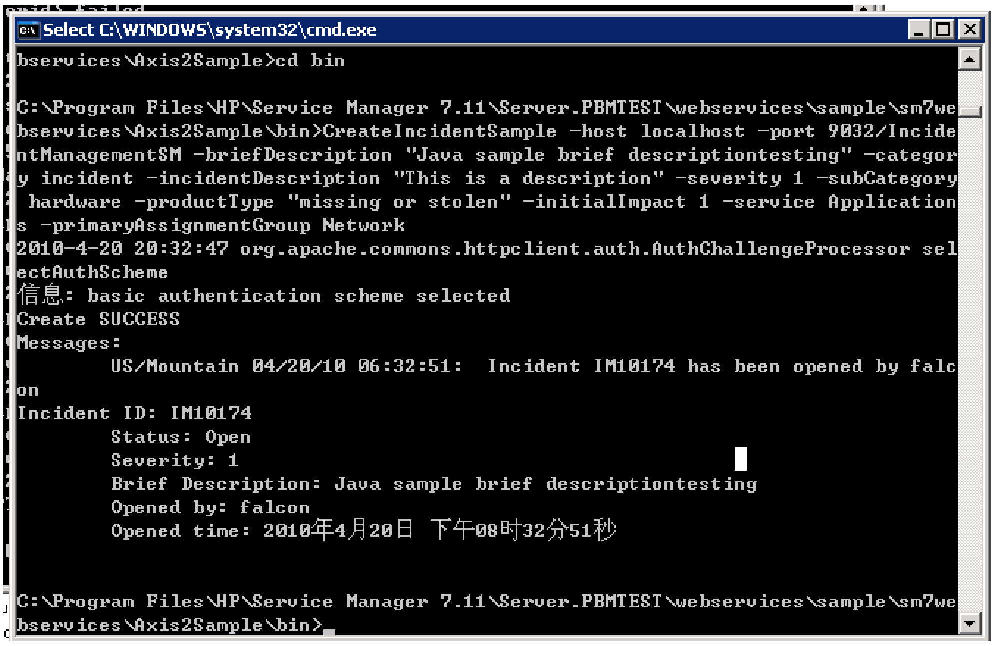
3) replace the original one with it.

4. Compile this IncidentSample. You can refer to readme.txt about how to compile it.

5. After it’s compiled successfully, you have finished all integration configuration for this IncidentSample with SOA. Refer to readme.txt, we need to specify SOA port when you input parameters. For port parameter, specify as “SOA port/Servicename_In_SOA” . For example, “-port 9032/IncidentManagementSM”.

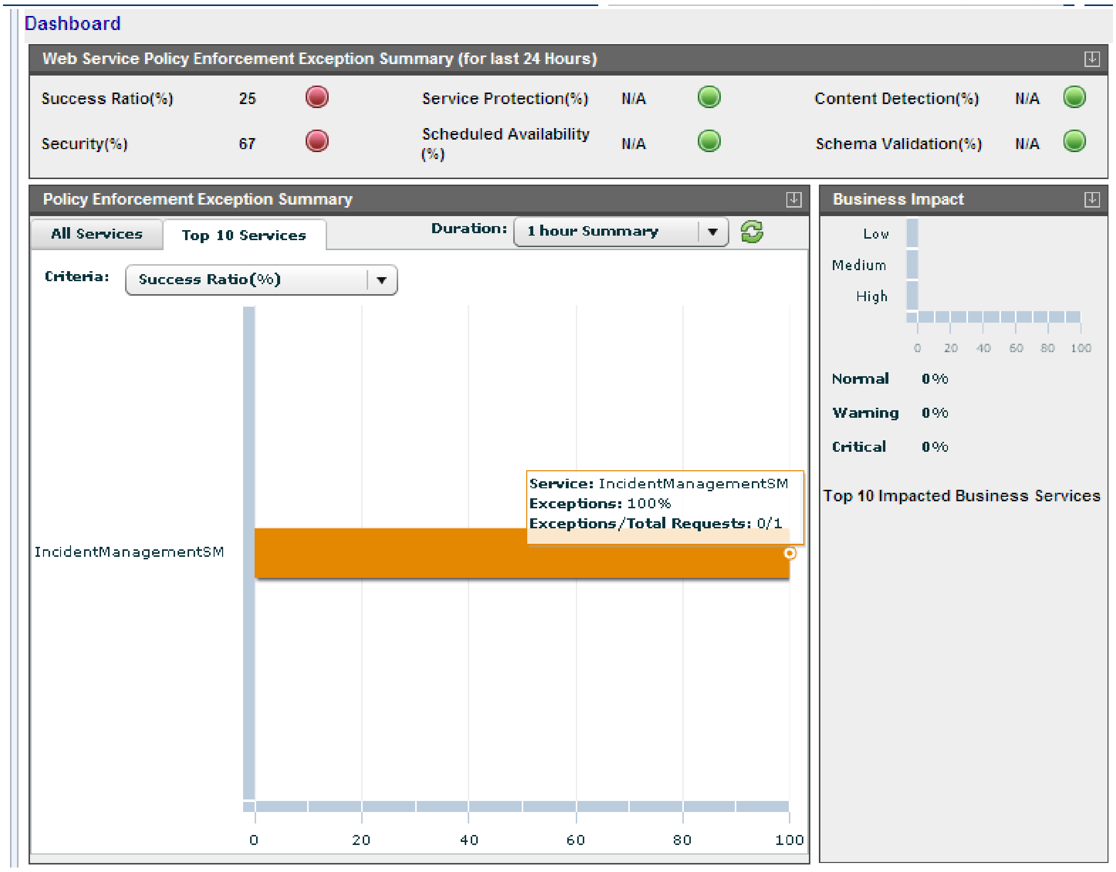
Here is a result of Incident Created Successfully.

Note that basic authentication scheme selected.



```
bservices\Axis2Sample>cd bin

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>CreateIncidentSample -host localhost -port 9032/Incide
ntManagementSM -briefDescription "Java sample brief descriptiontesting" -categor
y incident -incidentDescription "This is a description" -severity 1 -subCategory
 hardware -productType "missing or stolen" -initialImpact 1 -service Application
s -primaryAssignmentGroup Network
2010-4-20 20:32:47 org.apache.commons.httpclient.auth.AuthChallengeProcessor sel
ectAuthScheme
信息: basic authentication scheme selected
Create SUCCESS
Messages:
        US/Mountain 04/20/10 06:32:51:  Incident IM10174 has been opened by falc
on
Incident ID: IM10174
        Status: Open
        Severity: 1
        Brief Description: Java sample brief descriptiontesting
        Opened by: falcon
        Opened time: 2010年4月20日 下午08时32分51秒


C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>_
```

6. And from SOA, you can click dashboard to know that IncidentManagementSM web service is requested successfully.



Dashboard

Web Service Policy Enforcement Exception Summary (for last 24 Hours)

Success Ratio(%)	25	●	Service Protection(%)	N/A	●	Content Detection(%)	N/A	●
Security(%)	67	●	Scheduled Availability (%)	N/A	●	Schema Validation(%)	N/A	●

Policy Enforcement Exception Summary

All Services | Top 10 Services

Duration: 1 hour Summary

Criteria: Success Ratio(%)

Service: IncidentManagementSM
Exceptions: 100%
Exceptions/Total Requests: 0/1

Business Impact

Normal 0%

Warning 0%

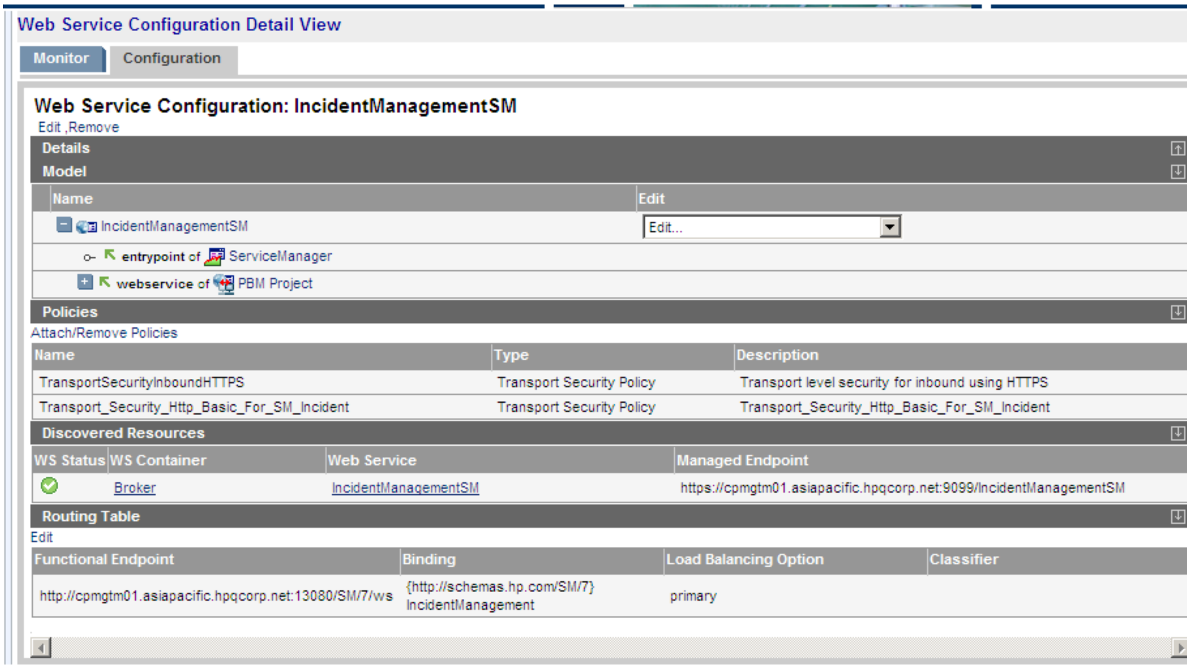
Critical 0%

Top 10 Impacted Business Services

4.2.2 Verify SSL

As SM Incident web service is configured in 4-2-1. We need to associate SSL security policy in SOA and modify IncidentSample to use SSL.

1. Associate SSL security policy. Refer to section 3-4-3, 3-4-4, 3-4-7. After association, SM Incident web service will be like this in SOA:



Web Service Configuration Detail View

Web Service Configuration: IncidentManagementSM

Edit ,Remove

Details

Model

Name	Edit
IncidentManagementSM	Edit...
entrypoint of ServiceManager	
webservice of PBM Project	

Policies

Attach/Remove Policies

Name	Type	Description
TransportSecurityInboundHTTPS	Transport Security Policy	Transport level security for inbound using HTTPS
Transport_Security_Http_Basic_For_SM_Incident	Transport Security Policy	Transport_Security_Http_Basic_For_SM_Incident

Discovered Resources

WS Status	WS Container	Web Service	Managed Endpoint
✓	Broker	IncidentManagementSM	https://cpmgtm01.asiapacific.hpqcorp.net:9099/IncidentManagementSM

Routing Table

Edit

Functional Endpoint	Binding	Load Balancing Option	Classifier
http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws	{http://schemas.hp.com/SM/7} IncidentManagement	primary	

2. Then we need to modify IncidentSample to make it connect to SOA to create Incident.

We need to modify the source files "CreateIncidentSample.java and IncidentManagementServiceUtility.java" which are located at Axis2Sample\src\com\hp\sm\webservice\sample\incident\ to add SSL.

For SSL, we have packaged two modified file in our installation package which is named as CreateIncidentSample_SSL.java and IncidentManagementServiceUtility_SSL.java. You should do:

1) Modify their contents.

For CreateIncidentSample_SSL.java, find two lines:

```
System.setProperty("javax.net.ssl.trustStore", "C:\\key\\soa.trustore");

System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Modify the trustStore and password to yours. Truststore should be the SOA server's truststore.

For IncidentManagementServiceUtility_SSL.java,

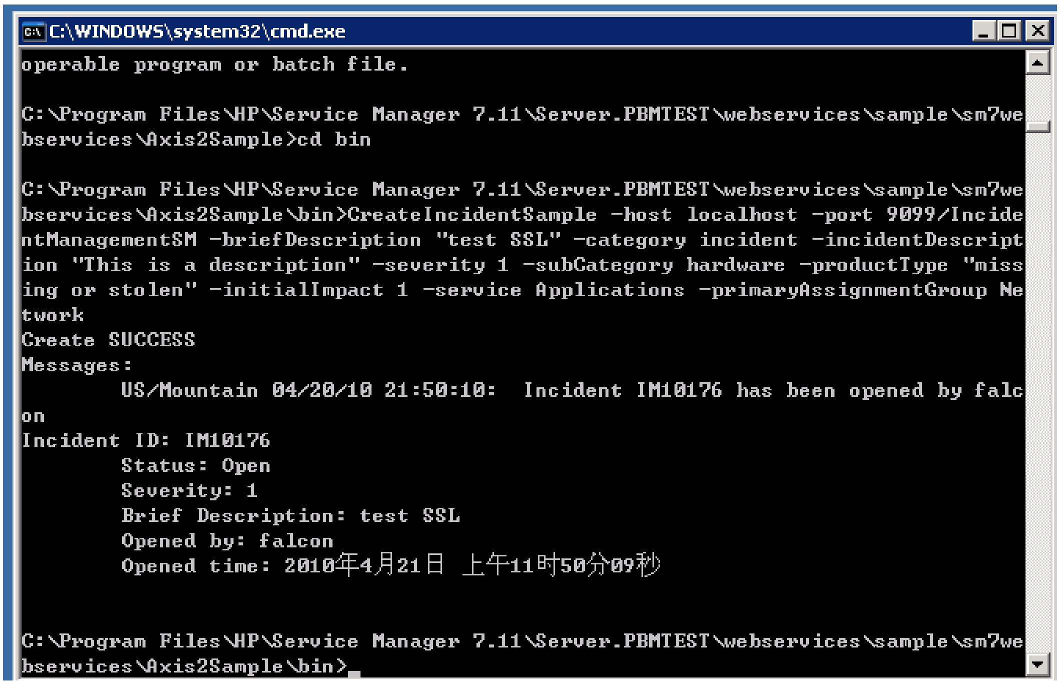
Do not need to modify this file.

2) Rename them as CreateIncidentSample.java and IncidentManagementServiceUtility.java.

3) replace the original one with them.

3. Compile this IncidentSample. You can refer to readme.txt about how to compile it.

4. Then you can create Incident through SSL. For port parameter, specify as “SOA secure port/Servicename_In_SOA”. For example, “-port 9099/IncidentManagementSM”. Below is the result.

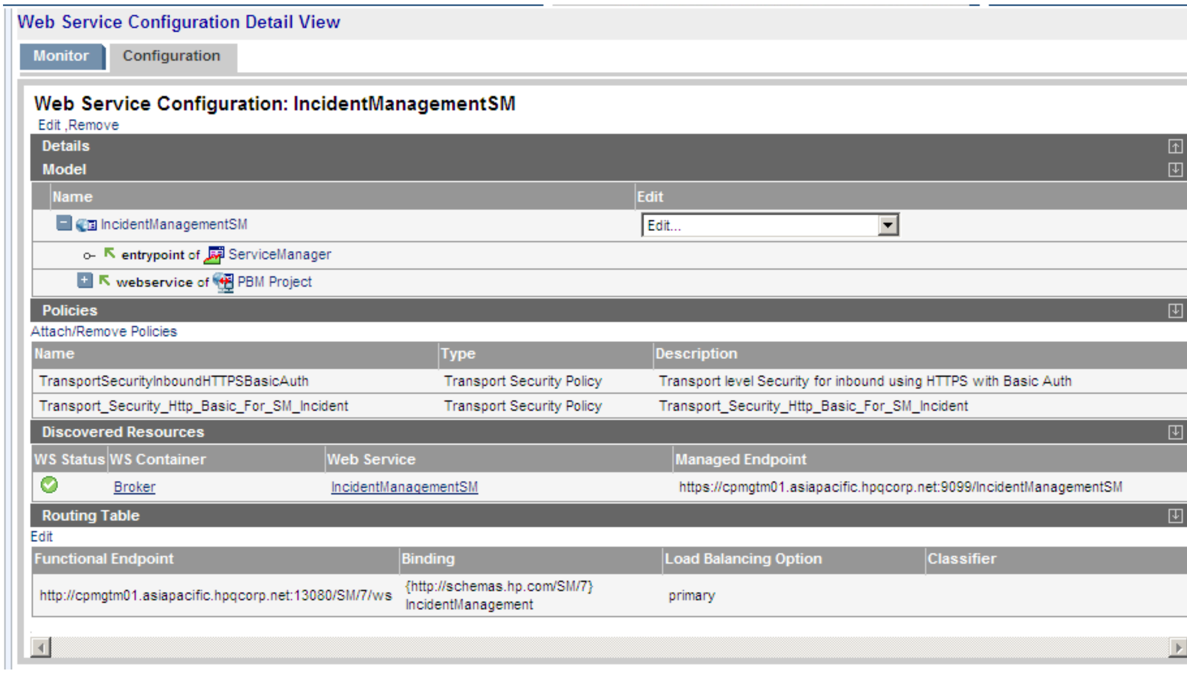


```
operable program or batch file.

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample>cd bin

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>CreateIncidentSample -host localhost -port 9099/Incide
ntManagementSM -briefDescription "test SSL" -category incident -incidentDescript
ion "This is a description" -severity 1 -subCategory hardware -productType "miss
ing or stolen" -initialImpact 1 -service Applications -primaryAssignmentGroup Ne
twork
Create SUCCESS
Messages:
        US/Mountain 04/20/10 21:50:10:  Incident IM10176 has been opened by falc
on
Incident ID: IM10176
        Status: Open
        Severity: 1
        Brief Description: test SSL
        Opened by: falcon
        Opened time: 2010年4月21日 上午11时50分09秒


C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>
```

4.2.3 Verify SSL with Basic authentication

As SM Incident web service is configured in 4-2-1. We need to associate SSL Basic security policy in SOA and modify IncidentSample to use SSL basic.

1. Associate SSL Basic security policy. Refer to section 3-4-3, 3-4-5, 3-4-7. After association, SM Incident web service will be like this in SOA:



Web Service Configuration: IncidentManagementSM

Name	Edit
IncidentManagementSM	Edit...
entrypoint of ServiceManager	
webservice of PBM Project	

Name	Type	Description
TransportSecurityInboundHTTPSBasicAuth	Transport Security Policy	Transport level Security for inbound using HTTPS with Basic Auth
Transport_Security_Http_Basic_For_SM_Incident	Transport Security Policy	Transport_Security_Http_Basic_For_SM_Incident

WS Status	WS Container	Web Service	Managed Endpoint
✓	Broker	IncidentManagementSM	https://cpmgtm01.asiapacific.hpqcorp.net:9099/IncidentManagementSM

Functional Endpoint	Binding	Load Balancing Option	Classifier
http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws	{http://schemas.hp.com/SM/7} IncidentManagement	primary	

2. Then we need to modify IncidentSample to make it connect to SOA to create Incident.

We need to modify the source files “CreateIncidentSample.java and IncidentManagementServiceUtility.java” which are located at Axis2Sample\src\com\hp\sm\webservice\sample\incident\ to add SSL with Basic authentication.

For SSL with basic authentication, we have packaged two modified file in our installation package which is named as CreateIncidentSample_SSL_Basic.java and IncidentManagementServiceUtility_SSL_Basic.java. You should do:

1) Modify their contents.

For CreateIncidentSample_SSL_Basic.java, find four lines:

```
basicauth.setUsername("admin");

basicauth.setPassword("password");

System.setProperty("javax.net.ssl.trustStore", "C:\\key\\soa.trustore");

System.setProperty("javax.net.ssl.trustStorePassword", "password");
```

Modify them to yours. Truststore should be the SOA server’s truststore.

For IncidentManagementServiceUtility_SSL_Basic.java,

Do not need to modify this file.

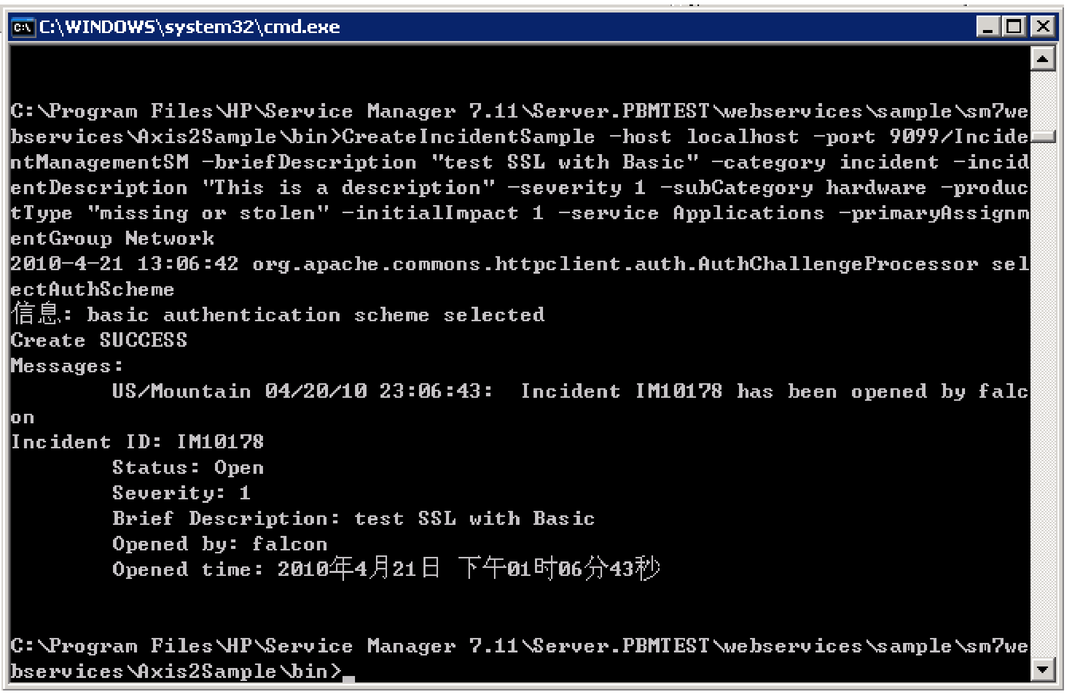
2) Rename them as CreateIncidentSample.java and IncidentManagementServiceUtility.java.

3) replace the original one with them.

3. Compile this IncidentSample. You can refer to readme.txt about how to compile it.

4. Then you can create Incident through SSL with Basic authentication. For port parameter, specify as “SOA secure port/Servicename_In_SOA”. For example, “-port 9099/IncidentManagementSM”.

Below is the result.

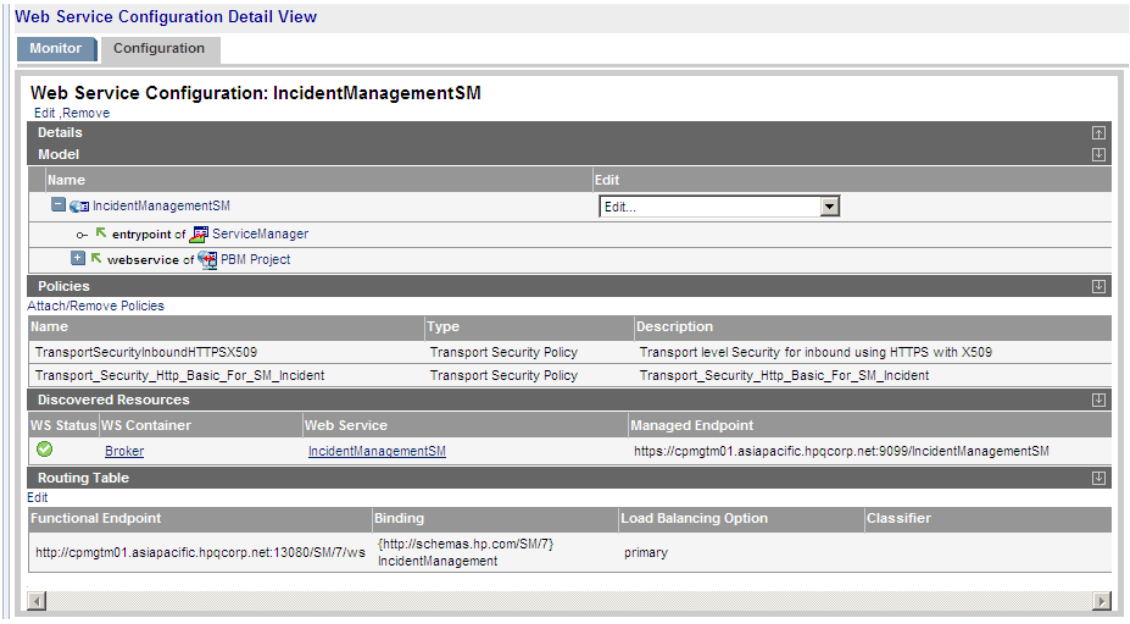


```
C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>CreateIncidentSample -host localhost -port 9099/Incide
ntManagementSM -briefDescription "test SSL with Basic" -category incident -incid
entDescription "This is a description" -severity 1 -subCategory hardware -produc
tType "missing or stolen" -initialImpact 1 -service Applications -primaryAssignm
entGroup Network
2010-4-21 13:06:42 org.apache.commons.httpclient.auth.AuthChallengeProcessor sel
ectAuthScheme
信息: basic authentication scheme selected
Create SUCCESS
Messages:
        US/Mountain 04/20/10 23:06:43:  Incident IM10178 has been opened by falc
on
Incident ID: IM10178
        Status: Open
        Severity: 1
        Brief Description: test SSL with Basic
        Opened by: falcon
        Opened time: 2010年4月21日 下午01时06分43秒


C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>_
```

4.2.4 Verify SSL with X.509

As SM Incident web service is configured in 4-2-1. We need to associate SSL X509 security policy in SOA and modify IncidentSample to use SSL X509.

1. Associate SSL X509 security policy. Refer to section 3-4-3, 3-4-6, 3-4-7. After association, SM Incident web service will be like this in SOA:



Web Service Configuration Detail View

Web Service Configuration: IncidentManagementSM

Edit ,Remove

Details

Model

Name	Edit
IncidentManagementSM	Edit...
entrypoint of ServiceManager	
webservice of PBM Project	

Policies

Attach/Remove Policies

Name	Type	Description
TransportSecurityInboundHTTPSX509	Transport Security Policy	Transport level Security for inbound using HTTPS with X509
Transport_Security_Http_Basic_For_SM_Incident	Transport Security Policy	Transport_Security_Http_Basic_For_SM_Incident

Discovered Resources

WS Status	WS Container	Web Service	Managed Endpoint
✓	Broker	IncidentManagementSM	https://cpmgtm01.asiapacific.hpqcorp.net:9099/IncidentManagementSM

Routing Table

Edit

Functional Endpoint	Binding	Load Balancing Option	Classifier
http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws	{http://schemas.hp.com/SM/7} IncidentManagement	primary	

2. Then we need to modify IncidentSample to make it connect to SOA to create Incident.

We need to modify the source files "CreateIncidentSample.java and IncidentManagementServiceUtility.java" which are located at Axis2Sample\src\com\hp\sm\webservice\sample\incident\ to add SSL with Basic authentication.

For SSL with basic authentication, we have packaged two modified file in our installation package which is named as CreateIncidentSample_SSL_X509.java and IncidentManagementServiceUtility_SSL_X509.java. You should do:

1) Modify their contents.

For CreateIncidentSample_SSL_X509.java, find four lines:

System.setProperty("javax.net.ssl.trustStore", "C:\\key\\soa.trustore");

System.setProperty("javax.net.ssl.trustStorePassword", "password");

System.setProperty("javax.net.ssl.keyStore", "C:\\key\\incident.keystore");

System.setProperty("javax.net.ssl.keyStorePassword", "password");

Modify them to yours. Truststore should be the SOA server's truststore. Keystore should be the TT client's keystore.

For IncidentManagementServiceUtility_SSL_X509.java,

Do not need to modify this file.

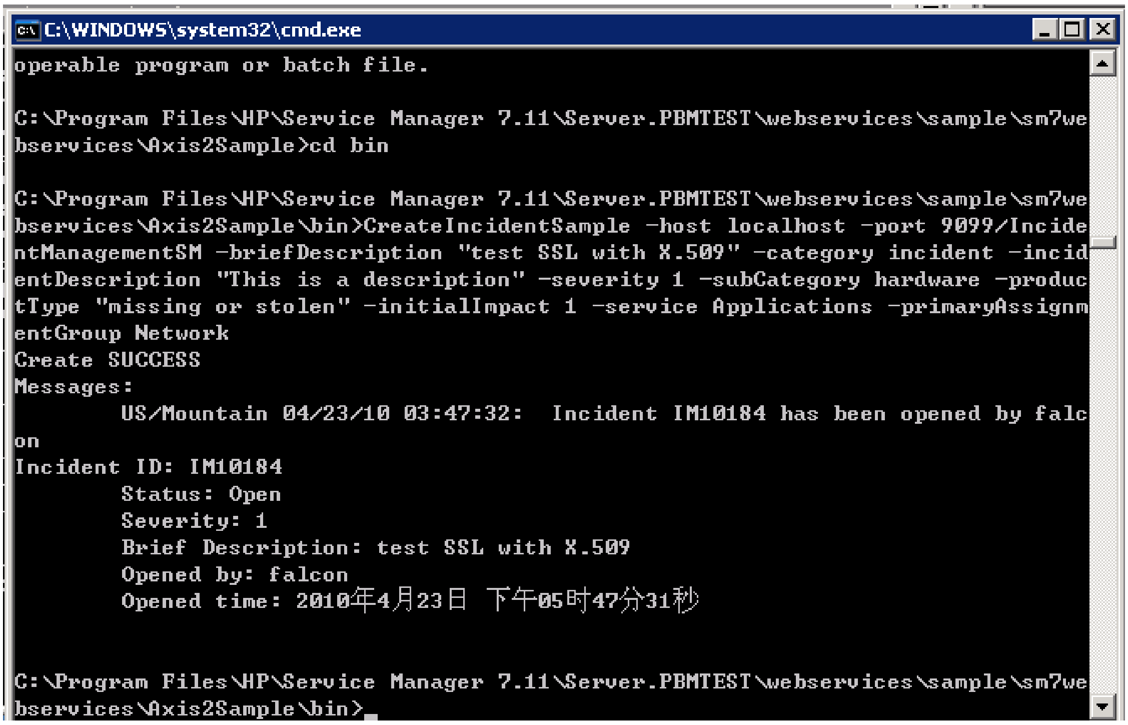
2) Rename them as CreateIncidentSample.java and IncidentManagementServiceUtility.java.

3) replace the original one with them.

3. Compile this IncidentSample. You can refer to readme.txt about how to compile it.

4. Then you can create Incident through SSL. For port parameter, specify as “SOA secure port/Servicename_In_SOA”. For example, “-port 9099/IncidentManagementSM”.

Below is the result.

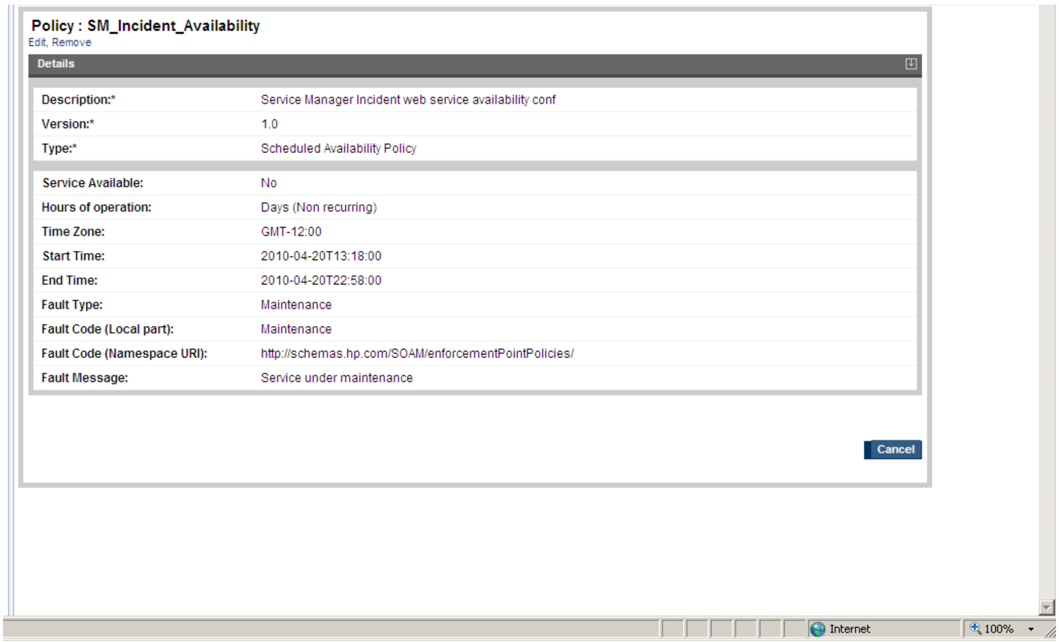


```
operable program or batch file.

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample>cd bin

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>CreateIncidentSample -host localhost -port 9099/Incide
ntManagementSM -briefDescription "test SSL with X.509" -category incident -incid
entDescription "This is a description" -severity 1 -subCategory hardware -produc
tType "missing or stolen" -initialImpact 1 -service Applications -primaryAssignm
entGroup Network
Create SUCCESS
Messages:
        US/Mountain 04/23/10 03:47:32:  Incident IM10184 has been opened by falc
on
Incident ID: IM10184
        Status: Open
        Severity: 1
        Brief Description: test SSL with X.509
        Opened by: falcon
        Opened time: 2010年4月23日 下午05时47分31秒


C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>_
```

4.3 Verify Performance Management

As SM Incident web service is configured in section 4-2. We only need to associate one performance policy to verify it.

We configure a scheduled availability policy named SM_Incident_Avaliability according to section 3-5-1 to make this SM Incident web service unavailability during 13:18 – 22:18.



Policy : SM_Incident_Availability

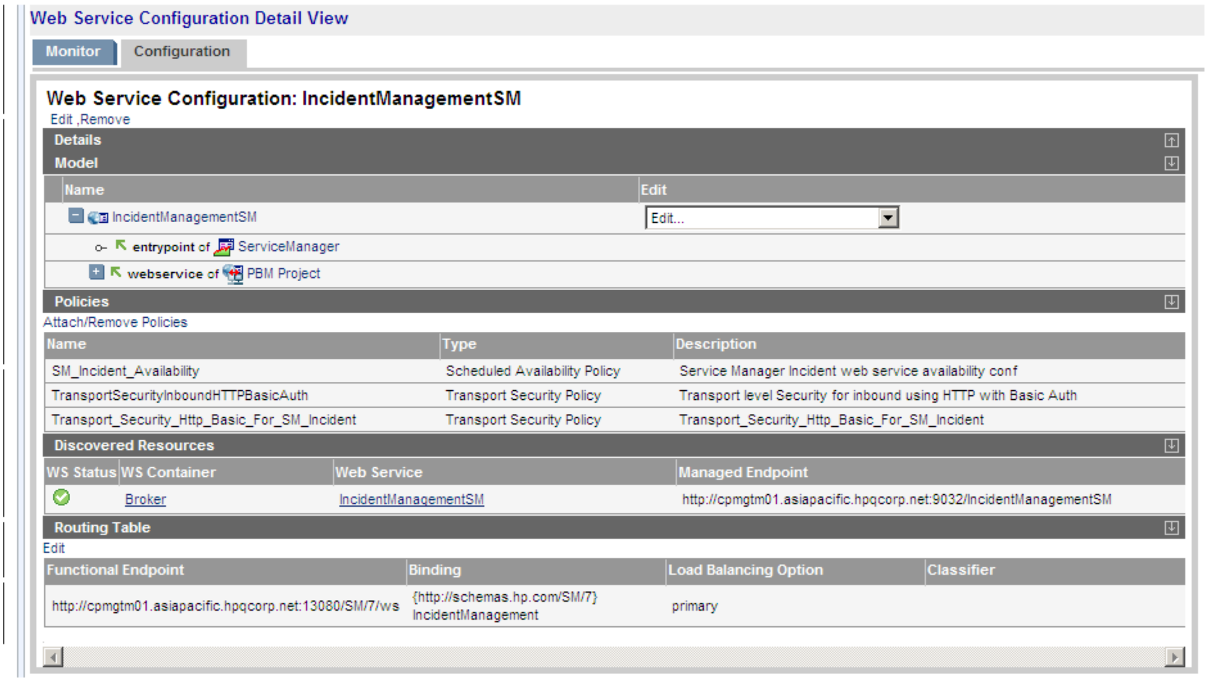
Edit, Remove

Details

Description:*	Service Manager Incident web service availability conf
Version:*	1.0
Type:*	Scheduled Availability Policy
Service Available:	No
Hours of operation:	Days (Non recurring)
Time Zone:	GMT-12:00
Start Time:	2010-04-20T13:18:00
End Time:	2010-04-20T22:58:00
Fault Type:	Maintenance
Fault Code (Local part):	Maintenance
Fault Code (Namespace URI):	http://schemas.hp.com/SOAM/enforcementPointPolicies/
Fault Message:	Service under maintenance

Associate this policy to IncidentManagmentSM according to section 3-5-3.

Like below snapshot:



Web Service Configuration Detail View

Web Service Configuration: IncidentManagementSM

Edit ,Remove

Details

Model

Name	Edit
IncidentManagementSM	Edit...
entrypoint of ServiceManager	
webservice of PBM Project	

Policies

Attach/Remove Policies

Name	Type	Description
SM_Incident_Availability	Scheduled Availability Policy	Service Manager Incident web service availability conf
TransportSecurityInboundHTTPBasicAuth	Transport Security Policy	Transport level Security for inbound using HTTP with Basic Auth
Transport_Security_Http_Basic_For_SM_Incident	Transport Security Policy	Transport_Security_Http_Basic_For_SM_Incident

Discovered Resources

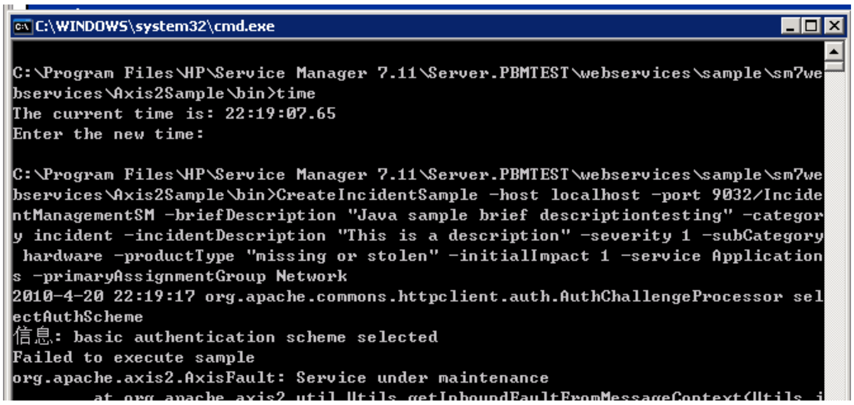
WS Status	WS Container	Web Service	Managed Endpoint
✓	Broker	IncidentManagementSM	http://cpmgtm01.asiapacific.hpqcorp.net:9032/IncidentManagementSM

Routing Table

Edit

Functional Endpoint	Binding	Load Balancing Option	Classifier
http://cpmgtm01.asiapacific.hpqcorp.net:13080/SM/7/ws	{http://schemas.hp.com/SM/7} IncidentManagement	primary	

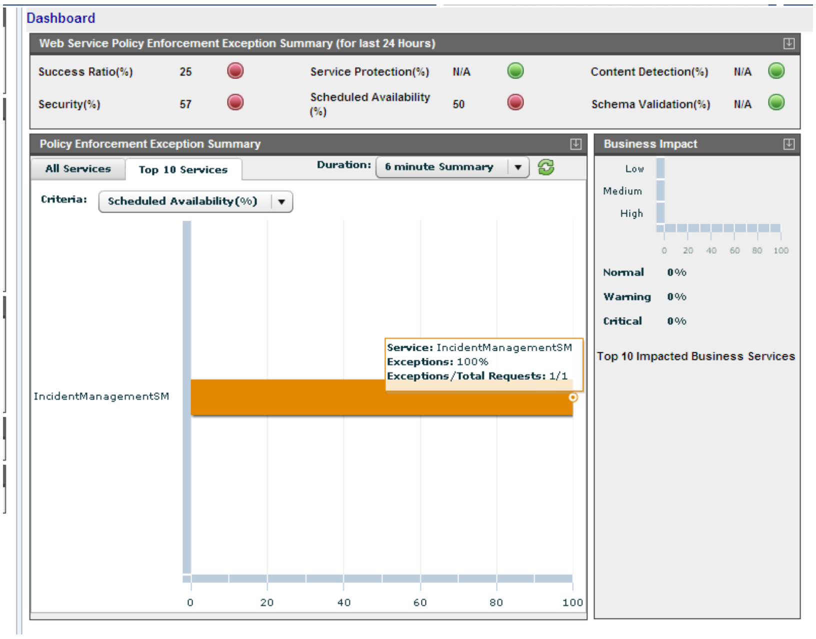
Then we do create Incident using IncidentSample. Below is the result of creation incident failure. You can see “Service under maintaince”.



C:\WINDOWS\system32\cmd.exe

```
C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>time
The current time is: 22:19:07.65
Enter the new time:

C:\Program Files\HP\Service Manager 7.11\Server.PBMTEST\webservices\sample\sm7we
bservices\Axis2Sample\bin>CreateIncidentSample -host localhost -port 9032/Incide
ntManagementSM -briefDescription "Java sample brief descriptiontesting" -categor
y incident -incidentDescription "This is a description" -severity 1 -subCategory
 hardware -productType "missing or stolen" -initialImpact 1 -service Application
s -primaryAssignmentGroup Network
2010-4-20 22:19:17 org.apache.commons.httpclient.auth.AuthChallengeProcessor sel
ectAuthScheme
信息: basic authentication scheme selected
Failed to execute sample
org.apache.axis2.AxisFault: Service under maintenance
        at org.apache.axis2.util.Utils.getInboundFaultFromMessageContext(Utils.j
```

And from SOA, you can click dashboard. You can know that scheduled availability policy takes into effect.



Dashboard

Web Service Policy Enforcement Exception Summary (for last 24 Hours)

Success Ratio(%)	25	●	Service Protection(%)	N/A	●	Content Detection(%)	N/A	●
Security(%)	57	●	Scheduled Availability (%)	50	●	Schema Validation(%)	N/A	●

Policy Enforcement Exception Summary

All Services | Top 10 Services

Duration: 6 minute Summary

Criteria: Scheduled Availability(%)

Service: IncidentManagementSM
Exceptions: 100%
Exceptions/Total Requests: 1/1

Normal 0%

Warning 0%

Critical 0%

Top 10 Impacted Business Services

Chapter 5
Remove Integration

5.1 Remove security or performance policy

1. Click web service
2. Click SM Incident web service
3. Click Attach/Remove Policies to remove policies from web service.

5.2 Remove SM web service

1. Click web service
2. Click SM Incident web service
3. Click Configuration Tab
4. Click Remove

Chapter 6
Appendix A Create Key through java keytool

In SOA, you need to specify keystore and truststore. It should be the server keystore and client truststore.

The below steps guide you how generate a keystore and truststore for one system. You need to generate keystore and truststore for server and client both. When you only want SSL or SSL with basic authentication, only server’s keystore and truststore are required. When you want SSL with X509, client and server’s keystore and truststore are all required.

Steps how to generate keystore and truststore on one computer:

1.keytool -genkey -alias soassl -keystore localhost.keystore

Note: name must be full computer name

2.keytool -export -alias soassl -file mycert.cer -keystore localhost.keystore

3.keytool -import -alias soassl -file mycert.cer -keystore localhost.truststore

```
Enter keystore password:  password

Owner: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown

Issuer: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown

Serial number: 4bc45019

Valid from: Tue Apr 13 19:06:01 CST 2010 until: Mon Jul 12 19:06:01 CST 2010

Certificate fingerprints:

         MD5:  CE:39:74:C4:56:5D:3C:6E:30:C7:5C:48:39:46:36:EA

         SHA1:  65:E9:2C:23:EA:97:E5:D9:D4:6C:2C:BB:A3:E8:C4:7B:2A:B4:D4:8E

Trust this certificate? [no]:  yes

Certificate was added to keystore
```