HPSP VPN Technology Extension

Delivery Guide

Release v7.0

Legal Notices

Table of Contents

In This Guide

This document explains installation and administration processes for the HPSP VPN Technology Extension.

Audience

The audience for this guide is the Solutions Integrator (SI). The SI has a combination of some or all of the following capabilities:

Understands and has a solid working knowledge of:

- UNIX® commands
- Windows® system administration

Understands networking concepts and language

Is able to program in Java™ and XML

Understands security issues

Understands the customer's problem domain

Conventions

The following typographical conventions are used in this guide.

Font	What the Font Represents	Example
Italic	Book or manual titles, and man page names	Refer to the *HP Subscription Repository* and the *Javadocs* man page for more information.
	Provides emphasis	You *must* follow these steps.
	Specifies a variable that you must supply when entering a command	Run the command: `javac` *<sourceFiles>*
	Parameters to a method	The *assigned_criteria* parameter returns an ACSE response.
Bold	New terms	The **distinguishing attribute** of this class...
Computer	Text and items on the computer screen	The system replies: `Press Enter`
	Command names	Use the `javac` command ...
	Method names	The `get_all_replies()` method does the following...
	File and directory names	Edit the file $Installation_dir/config/conf.xml
	Process names	Check to see if `system` is running.
	Window/dialog box names	In the `Test and Track` dialog...
	XML tag references	Use the `<DBTable>` tag to...
Computer Bold	Text that you must type	At the prompt, type: **`ls -l`**
Keycap	Keyboard keys	Press **Return**.
[Button]	Buttons on the user interface	Click `[Delete]`. Click the `[Apply]` button.
Menu Items	A menu name followed by a colon (:) means that you select the menu, then the item. When the item is followed by an arrow (->), a cascading menu follows	Select Locate:Objects->by Comment.

Abbreviations

HPSP: HP Service Provisioner
HPSP VPN TE: HP Service Provisioner Technology Extension
HP TV: HP Trueview resource inventory
HPSA VPN: HPSA VPN activation solution
HP SR: Subscription Repository

1 Introduction

1.1 L3 VPN Services

The current version of the HPSP VPN TE covers the L3 VPN Services. An L3 VPN is an IP based network delivering private network services over the CSP infrastructure.

Figure 1: High level view

Internally, it uses layer 3 VRF (VPN/virtual routing and forwarding) to segment routing tables for each "customer" using the service. Protocol BGP is required in the CSP.

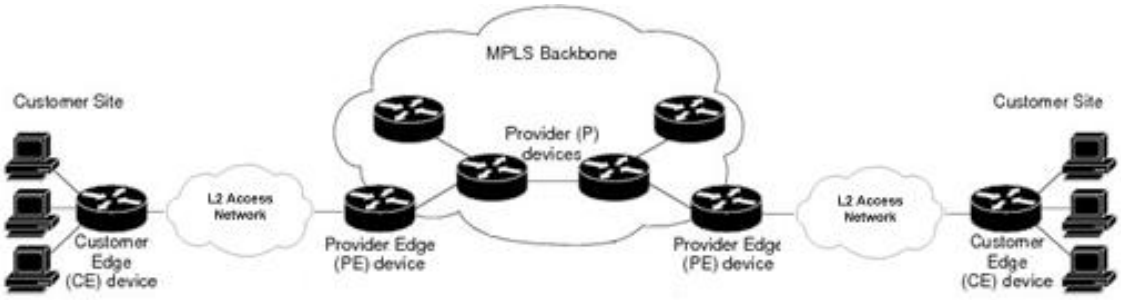


Figure 2: Technical view

1.2 The HPSP VPN TE Solution

The HPSP Technologies Extensions provide, on top of the HPSP, the modules needed to cover the provisioning process for a concrete technology/business domain, in this case, the L3 VPNs.

1.2.1 Functionality covered

The functionality covered by the solution is:

- Management of L3 VPN services, including:
  - Selection of the VPN topology to apply:
    - Full Mesh
    - Hub & Spoke
  - Selection of the Class of Service to apply and rate limit available per site
  - Configuration of the connectivity between the CE and correspondent PE, including the following protocols:
    - RIP
    - BGP
    - OSPF
    - Static Routes
  - Configuration and provisioning of the L2 access network (vlan path between the CE and the PE), including:
    - L2 direct connections
    - L2 ring networks
    - L2 star networks
  - Provisioning of the PE including the VRF configuration.
  - Monitor the installation task of the CE equipment
  - Remote configuration of the CE equipment
- The available models of equipments that can be managed by the solution are the ones covered by the HPSA VPN solution.

1.2.2 Architecture

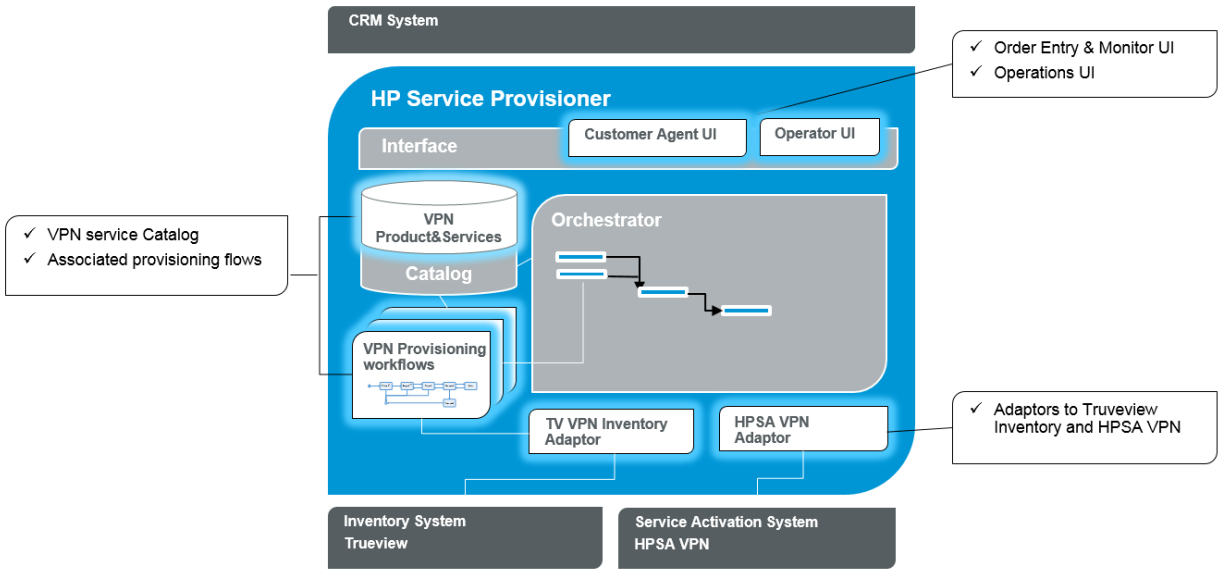


Figure 3: HPSP VPN TE Architecture

Modules included in the solution:

Module	**Description**
VPN Service Catalog	Product and Service Catalog for the L3 VPN services, including the decomposition of the customer services in technical services.
Associated provisioning workflows	Workflows in charge of managing the provisioning process, associated to the technical services in the catalog.
TV VPN Inventory Adaptor	Out-of-the-box adaptor to interact with HP TV, in charge of the network resource inventory.
HPSA VPN Adaptor	Out-of-the-box adaptor to interact with HPSA VPN, in charge of the service activation.
Customer Agent UI	Order entry and service monitor functionality. Integrated into the HP OSS Console platform.
Operator UI	Manual task management and technical monitoring. Integrated into the HPSP default UI.

2 Installation & Configuration

This part of the guide will try to summarize the installation process of the Technology Extension solution, specifying also the rest of components it requires to work properly.

2.1 Prerequisites

This chapter describes the list of steps to install and configure the different solutions integrated by the application.

Please consult the documentation of each solution for details on how to install the different components.

2.1.1 HPSA

The following actions are required to properly install and configure the HPSA solution.

2.1.1.1 Installation

Install the HPSA v7.0.

2.1.1.2 Configuration

Deploy the 'CRM Model' solution on top of the HPSA.

2.1.2 HPSA VPN Solution

The following actions are required to properly install and configure the HPSA VPN solution.

2.1.2.1 Installation

Install the HPSA VPN v7.0.

2.1.2.2 Configuration

In order to configure the HPSA VPN ready for the HPSP VPN TE solution, execute the script 'resetVPNAdaptativeMode' located in $HP\OpenView\ServiceActivator\solutions\SAVPN\etc\config

2.1.3 HP Service Provisioner

The following actions are required to properly install and configure the HP Service Provisioner solution.

2.1.3.1 Installation

Deploy the HP Service Provisioner v7.0 solution on top of the installed HPSA.

2.1.3.2 Configuration

No configurations are required.

2.1.4 OSS Console

The following actions are required to properly install and configure the HP OSS Console solution.

2.1.4.1 Installation

Install the OSS Console v2.0

2.1.4.2 Configuration

No configurations are required.

2.2 HPSP VPN TE Installation

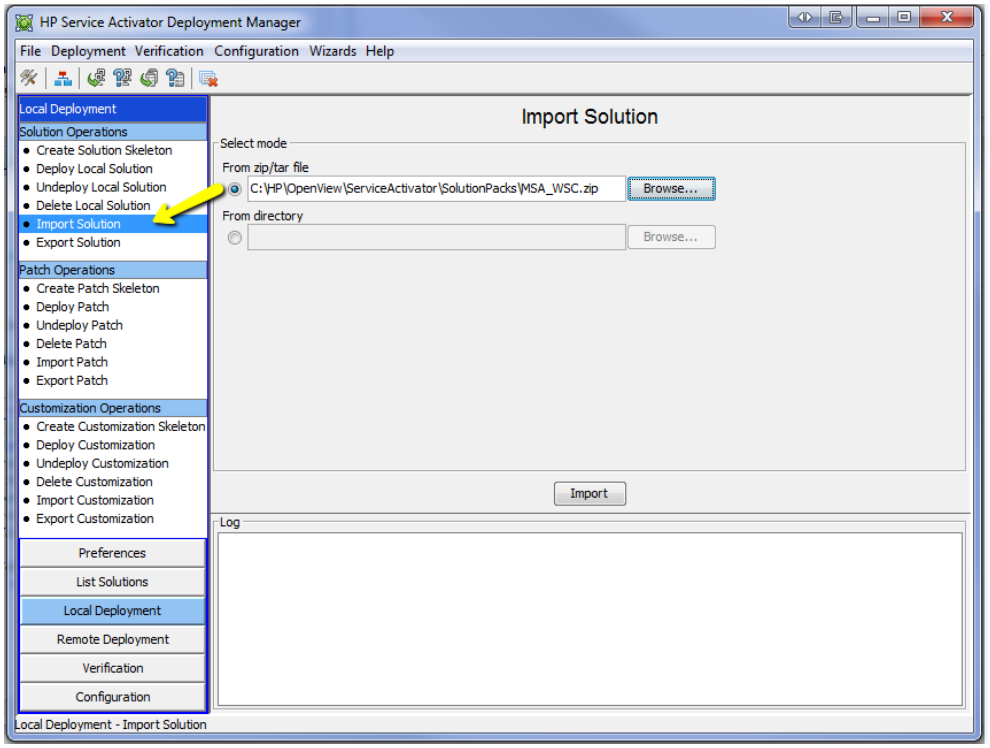
Once the prerequisites have been followed, the HPSP VPN TE installation process can start.

2.2.1 Web service connectivity module

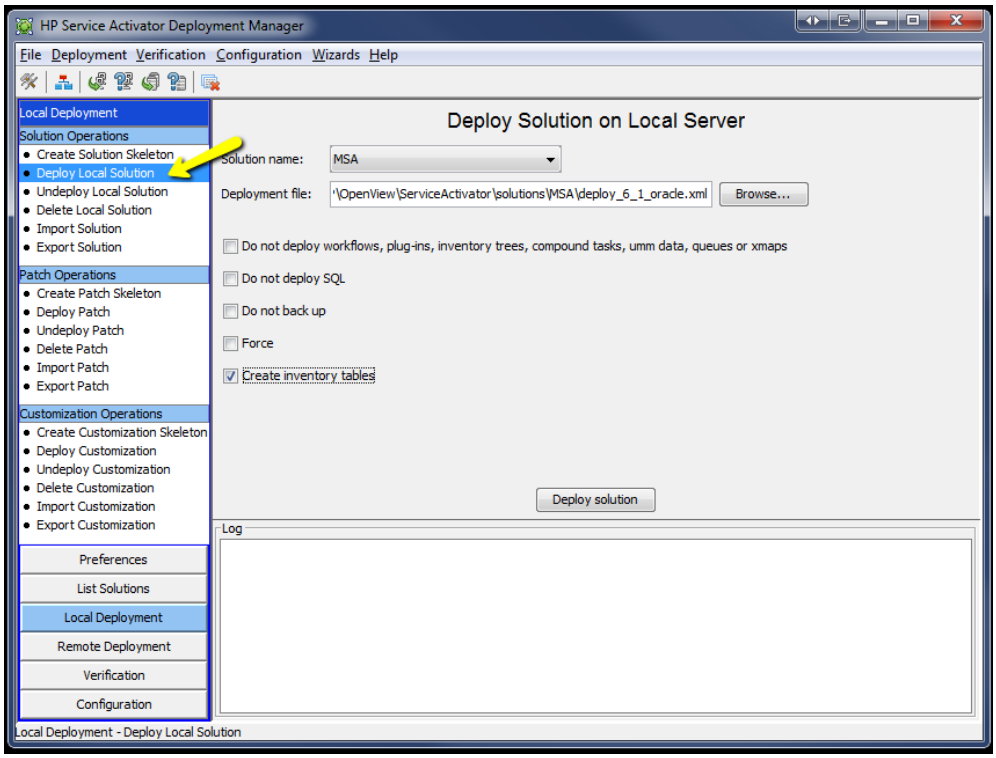
This module is required for the solution to interact with the TV platform via web service.

The first step is to install the patch 'HPSA Extension Pack v7.0' on top of the installed HPSA. Once installed, the following module has to be deployed:

Go to Local Deployment -> Import solution and select the MSA_WSC.zip located in the directory 'binaries' of the ISO file. Click on import.



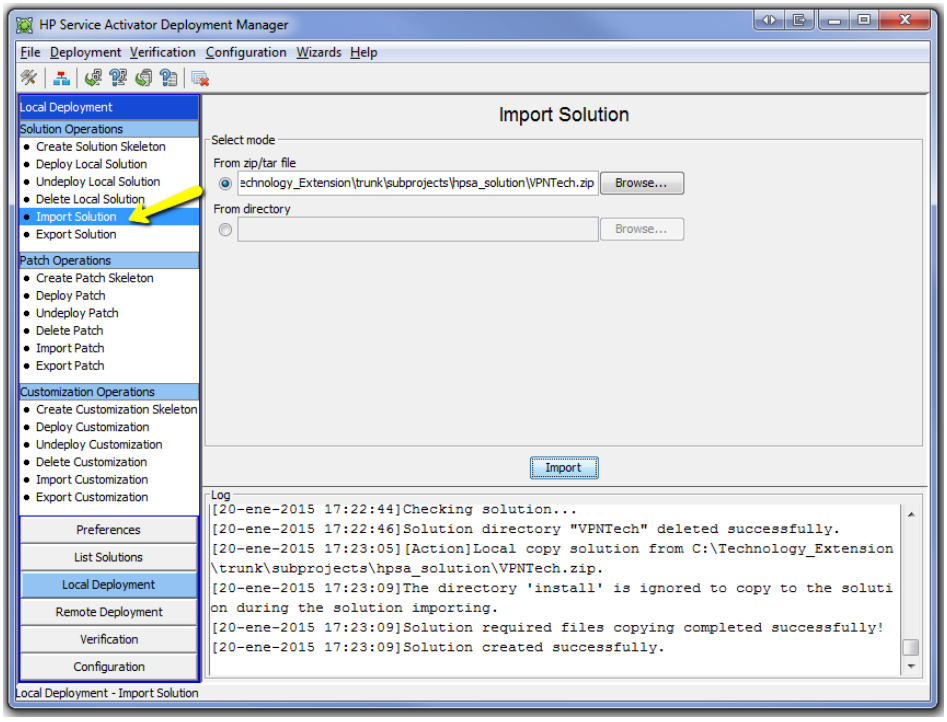
Go to Local Deployment -> Deploy local solution and select the imported solution. Then select the appropriate deployment file. Check the option “Create inventory tables” and click on Deploy solution.



2.2.2 HPSP VPN TE Core

Deploy the HPSP VPN TE solution included in the ISO:

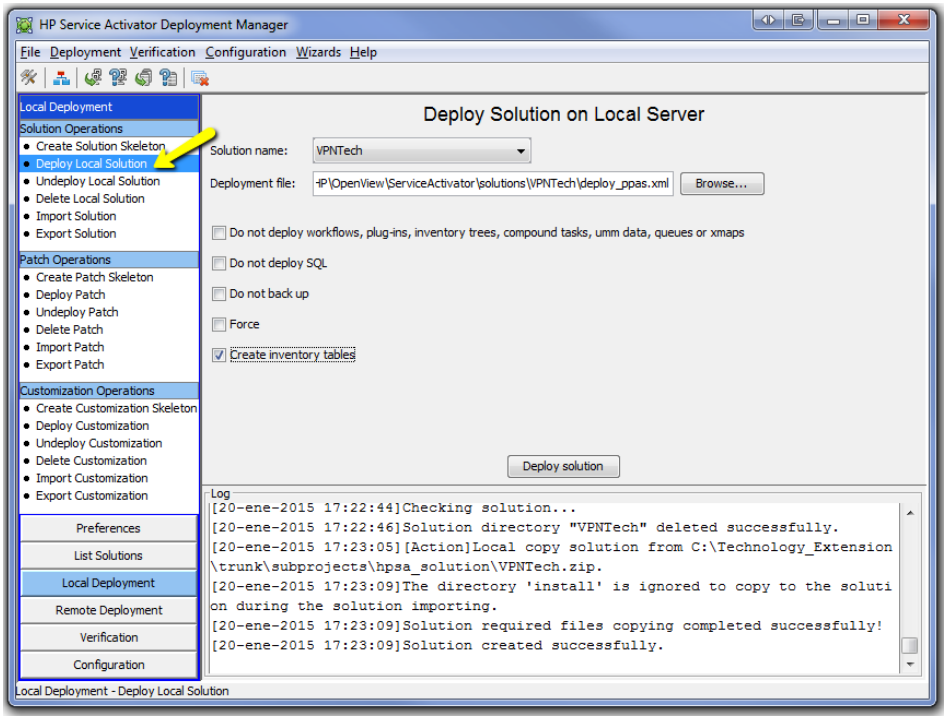
Go to Local Deployment -> Import solution and select the VPNTech.zip located in the directory 'binaries' of the ISO file. Click on import.



A manual interaction is required at this point. Access the file 'populate_poc_data_xxx.sql' (where xxx represents the installed data base) located in '$HP\OpenView\ServiceActivator\solutions\VPNTech\etc\sql', open it and replace the values <tvuser>, <tvpassword>, <host:port> with the appropriate values to connect to TV Inventory. Save it.

-- **Replace the fields in bold letter with the appropiate TV connectivity values**
INSERT INTO WSC_ENDPOINT (ENDPOINTID, TARGETEQUIPMENT, USERNAME, PASSWORD, URL, WSCSERVICEID, NETWORKELEMENTID, ISPARENT__) VALUES (WSC_ENDPOINT_SEQ.nextVal, 'TV', **tvuser**, **tvpassword**, 'http://**host**:**port**/tnp-ws/services', (SELECT WSCSERVICEID FROM WSC_SERVICE WHERE SERVICENAME='TV'), (SELECT NETWORKELEMENTID FROM CR_NETWORKELEMENT WHERE NAME='TV'), '0');

Then, go to Local Deployment -> Deploy local solution and select the imported solution. Then select the appropriate deployment file. Check the option "Create inventory tables" and click on Deploy solution.



2.2.3 HPSP VPN TE UI

Put the file 'GUI_VPN_Technology_Extension_v7.0.0.zip' included in the 'binaries' directory of the ISO file, in the 'dist' directory of the HP OSS Console. Please consult the HP OSS Console documentation on more details on how to deploy solutions on top.

2.3 Configuration

This chapter describe the steps needed to configure the solution once the installation process has been done.

2.3.1 HPSP Microworkflow configuration

Edit the `mwfm.xml` located at `$HP\OpenView\ServiceActivator\etc\config` to match this configuration:

- Add or uncomment this line:

```
<Generate-Service-ID>true</Generate-Service-ID>
```

- Uncomment authenticator module:

```
<Module>
    <Name>authenticator</Name>
    <Class-Name>
        com.hp.ov.activator.mwfm.engine.module.umm.DatabaseAdvancedAuthModule
    </Class-Name>
    <Param name="mwfm remote url" value="//localhost:2000/wfm"></Param>
    <Param name="expiry days" value="90"></Param>
    <Param name="expiry_alert_days" value="10"></Param>
    <Param name="reuse_interval" value="3"></Param>
    <Param name="password_validation" value="true"></Param>
</Module>
```

- Configure the socket sender module:

```
<Module>
       <Name>crm_portal_sync</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.SocketSenderModule</Class-Name>
       <Param name="host"  value="localhost"/>
       <Param name="port"  value="5099"/>
       <Param name="fault tolerant"  value="true"/>
       <Param name="read_message_from_db" value="true"/>
</Module>

<Module>
       <Name>som_sender_module</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.SocketSenderModule</Class-Name>
       <Param value="localhost" name="host"/>
       <Param value="4099" name="port"/>
       <Param value="true" name="fault tolerant"/>
       <Param value="true" name="read_message_from_db"/>
</Module>
```

- Add the JMS listener and sender module, changing the user/password if necessary:

```
<Module>
       <Name>jms_listener_queue</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSListenerModule</Class-Name>
       <Param name="workflow"  value="Example_Controller"/>
       <Param name="jndi url"  value="remote://primary:4447"/>
       <Param name="jndi initial context factory"
              value="org.jboss.naming.remote.client.InitialContextFactory"/>
       <Param name="connection_factory_name"  value="ConnectionFactory"/>
       <Param name="jms_trans_mode"  value="queue"/>
       <Param name="jms_destination"  value="HPSAQueue"/>
       <Param name="username" value="hpsa"/>
       <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
       <Param name="header" value="true"/>
       <Param name="dtd" value="exchange.dtd"/>
       <Param name="dtd_root_tag" value="msg"/>
       <Param name="min threads" value="1"/>
       <Param name="max threads" value="3"/>
       <Param name="max queue length" value="50"/>
       <Param name="write message to" value="db"/>
</Module>

<Module>
       <Name>jms sender queue</Name>
       <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSSenderModule</Class-Name>
       <Param name="jndi_url"  value="remote://primary:4447"/>
       <Param name="jndi_initial_context_factory"
              value="org.jboss.naming.remote.client.InitialContextFactory"/>
       <Param name="connection factory name"  value="ConnectionFactory"/>
       <Param name="jms destination"  value="HPSAQueue"/>
       <Param name="username" value="hpsa"/>
       <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
</Module>
```

- Configure the conflict module:

```
<Module>
       <Name>SchedulerJobExecuter</Name>
       <Class-Name>com.hp.ov.activator.vpn.module.scheduler.JobExecuter</Class-Name>
       <Param name="db module" value="db"/>
</Module>

<Module>
       <Name>sosa_async_responser</Name>
       <Class-Name>com.hp.spain.engine.module.sosa.SosaAsyncResponserImpl</Class-Name>
       <Param name="errors async persistence file"
       value="C:/HP/OpenView/ServiceActivator/var/tmp/errors_async_responser.dat"/>
       <Param name="write_in_queue" value="false"/>
```

```
        <Param name="sosa async queue"  value="sosa async queue"/>
</Module>

<Module>
        <Name>conflict_module</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.ConflictModule</Class-Name>
        <Param name="poll interval"  value="10000"/>
</Module>
```

- Add the following modules, reviewing that the user/password fields match your own configuration:

```
<Module>
        <Name>SOFAModuleTV</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.SOFAModule</Class-Name>
        <!-- Adapter package -->
        <Param name="implementation package"
        value="com.hp.ov.activator.mwfm.engine.module.sofa.inventory.tv"/>
        <!-- RMI Port -->
        <Param name="rmi_service_port" value="9998"></Param>
        <!-- Maximum interval to wait for a ws request in seconds-->
        <Param name="max ext waiting response" value="60"></Param><!-- default value is 60-->
        <!-- WS Parameters-->
        <Param name="wsc module name" value="wsc"></Param>
        <Param name="target_equipment" value="TV"></Param>
        <Param name="service_name" value="TV"></Param>
</Module>

<Module>
        <Name>SOFAModuleSAVPN</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.SOFAModule</Class-Name>
        <!-- Adapter package -->
        <Param name="implementation package"
                value="com.hp.ov.activator.mwfm.engine.module.sofa.activation.savpn"/>
        <Param name="rmi service port" value="9997"></Param>
        <Param name="mwfm remote url" value="//localhost:2000/wfm"></Param>
        <Param name="mwfm_remote_user" value="hpsa"></Param>
        <Param name="mwfm_remote_password" value="s5/HIIXk9NIZdrwnw6tSmA=="></Param>
        <!-- Socket listener parameters -->
        <Param name="wait latency" value="1000"></Param><!-- default value is 1000 -->
        <Param name="max ext waiting response" value="60"></Param><!-- default value is 60 -->
        <Param name="listener_port" value="5099"></Param>
        <Param name="terminal_codes" value="200;500;501;306;307;201;402;401"></Param>
        <Param name="ok codes" value="200;210"></Param>
        <Param name="database module" value="db"></Param>
</Module>

<Module>
        <Name>wsc</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.sofa.WSCModuleVPNTech</Class-Name>
        <Param name="database module" value="db"/>
        <Param name="retry count" value="1"/>
        <Param name="retry_interval" value="20"/>
</Module>
```

```
                                <!-- SOM Config modules -->
<Module>
        <Name>som_jms_listener_queue</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSListenerModule</Class-Name>
        <Param name="workflow"  value="Example Controller"/>
        <Param name="jndi_url"  value="remote://primary:4447"/>
        <Param name="jndi_initial_context_factory"
                value="org.jboss.naming.remote.client.InitialContextFactory"/>
        <Param name="connection factory name"  value="ConnectionFactory"/>
        <Param name="jms_trans_mode"  value="queue"/>
        <Param name="jms_destination"  value="HPSAQueue"/>
```

```
        <Param name="username" value="hpsa"/>
        <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
        <Param name="header" value="true"/>
        <Param name="dtd" value="exchange.dtd"/>
        <Param name="dtd_root_tag" value="msg"/>
        <Param name="min threads" value="1"/>
        <Param name="max threads" value="3"/>
        <Param name="max queue length" value="50"/>
        <Param name="write_message_to" value="db"/>
</Module>

<Module>
        <Name>som_jms_sender_queue</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.JMSSenderModule</Class-Name>
        <Param name="jndi_url"  value="remote://primary:4447"/>
        <Param name="jndi_initial_context_factory"
               value="org.jboss.naming.remote.client.InitialContextFactory"/>
        <Param name="connection factory name"  value="ConnectionFactory"/>
        <Param name="jms_destination"  value="HPSAQueue"/>
        <Param name="username" value="hpsa"/>
        <Param name="password" value="s5/HIIXk9NIZdrwnw6tSmA=="/>
</Module>

<Module>
        <Name>ServiceOrderManagement</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.som.SRModule</Class-Name>
        <Param name="username" value="sruser"/>
        <Param name="password" value="sruser"/>
        <Param name="encrypted password" value="false"/>
        <Param name="ws url" value=" http://localhost:8180/subscriptionrepository/operations"/>
        <Param name="retry_count"  value="3"/>
        <Param name="retry_interval"  value="10000"/>
        <Param name="min_threads" value="1"/>
        <Param name="max_threads" value="3"/>
</Module>

<Module>
        <Name>trueview</Name>
        <Class-Name>com.hp.ov.activator.mwfm.engine.module.TrueviewModule</Class-Name>
        <Param name="username" value="admin"/>
        <Param name="password" value="admin1001"/>
        <Param name="encrypted_password" value="false"/>
        <Param name="ws_url" value="http://portov4.gre.hp.com:8011/tnp-ws/services"/>
        <Param name="retry_count"  value="3"/>
        <Param name="retry_interval"  value="10000"/>
        <Param name="min threads" value="1"/>
        <Param name="max_threads" value="3"/>
</Module>
```

2.3.2 Import the VPN Catalog

To import the VPN catalog, the HPSP must be running. Then, go to `$HP\OpenView\ServiceActivator\bin` and execute the next command, specifying the path to the catalog file (the file called `catalogVPNTE.xml` located in `$HP\OpenView\ServiceActivator\solutions\VPNTech\docs`)

```
SOMData -import -user hpsa -password hpsa -filePath
C:\HP\OpenView\ServiceActivator\solutions\VPNTech\docs\catalogVPNTE.xml
```

2.4 Start and Stop the solution

The HPSP VPN TE is deployed as a solution on top of the HPSP. For information on stopping and starting the HPSP, refer to the HPSP Installation Guide.

2.5 Putting the solution to work

2.5.1 CSP Network configuration

The Technology Extension solution requires some previous population of the TV Inventory System in order to work:

2.5.1.1 CSP Core Network

At least on available BGP Network has to be configured. The BGP Network contains the PE and P equipments that will compose the CSP Network. This network requires the following configuration:

- The CSP has to be defined as a valid customer in TV
- All the BGP components (PE and P equipments) will be associated to this customer, as it is the owner of the core network.
- All the equipments will be well configured in the TV Inventory including a valid location.
- All the connections and IP links have to be configured, connecting the equipments (following the CSP network design).
- The IP links have to be added to the already created BGP network.
- Some UDAs (user defined attributes) have been added to the standard TV configuration in order to complete the basic information of the network elements. The PE equipments require the configuration of the following UDAs:

Module	**Description**
Role	Fixed value: "PE"
Default Network	Identifier of the BGP Network
Username	User name to access the equipment remotely via Telnet/SSH
Password	User name to access the equipment remotely via Telnet/SSH
Username enable	User enable to access the equipment remotely via Telnet/SSH. Optional
Password enable	Password enable to access the equipment remotely via Telnet/SSH. Optional
Management IP	IP to access the equipment remotely via Telnet/SSH

Management IF	Name of the interface to be accessed remotely. Optional, only informative.
Element Type	Element type of the equipment. Compatible with the field 'Element type' of network elements in the HPSA VPN solution*
OS Version	OS Version of the equipment. Compatible with the field 'OS Version' of network elements in the HPSA VPN solution*
Vendor	Vendor of the equipment. Compatible with the field 'Vendor' of network elements in the HPSA VPN solution*

*Consult the HPSA VPN documentation to know the available network element models

Once configured, the BGP network has to be in active state.

2.5.1.2 L2 Access Networks

The access networks are Ethernet networks that will connect the CE equipments to the CSP core network.

Each access network is composed of Access and Aggregation switches. The Aggregation switches transport the traffic of the customers to the PEs. The configuration of each Ethernet network requires the following configuration:

- All the equipments (Access switches and Aggregation switches) will be well configured in the TV Inventory including a valid location.
- All the equipments will be associated to the CSP customer, as it is the owner of the network.
- All the connections (facilities and Ethernet links) have to be configured, connecting the equipments (following the CSP network design).
- The Ethernet connections have to be added to the already created Ethernet network (including the connections between the aggregation switches and the PEs)
- An Ethernet circuit has to be defined connecting each access switch to the PE (this circuit will go through the access network in order to reach the core network). This circuit will be used to calculate the physical path to reach the core network.
- Some UDAs (user defined attributes) have been added to the standard TV configuration in order to complete the basic information of the network elements. These equipments require the configuration of the following UDAs:

Module	**Description**
Role	Fixed value: "ACCSWITCH" for access switches and "AGGSWITCH" for aggregation switches.

Default Network	Identifier of the Ethernet network
Access Circuit	Identifier of the access circuit to reach the core network.
Username	User name to access the equipment remotely via Telnet/SSH
Password	User name to access the equipment remotely via Telnet/SSH
Username enable	User enable to access the equipment remotely via Telnet/SSH. Optional
Password enable	Password enable to access the equipment remotely via Telnet/SSH. Optional
Management IP	IP to access the equipment remotely via Telnet/SSH
Management IF	Name of the interface to be accessed remotely. Optional, only informative.
Element Type	Element type of the equipment. Compatible with the field 'Element type' of network elements in the HPSA VPN solution*
OS Version	OS Version of the equipment. Compatible with the field 'OS Version' of network elements in the HPSA VPN solution*
Vendor	Vendor of the equipment. Compatible with the field 'Vendor' of network elements in the HPSA VPN solution*

*Consult the HPSA VPN documentation to know the available network element models

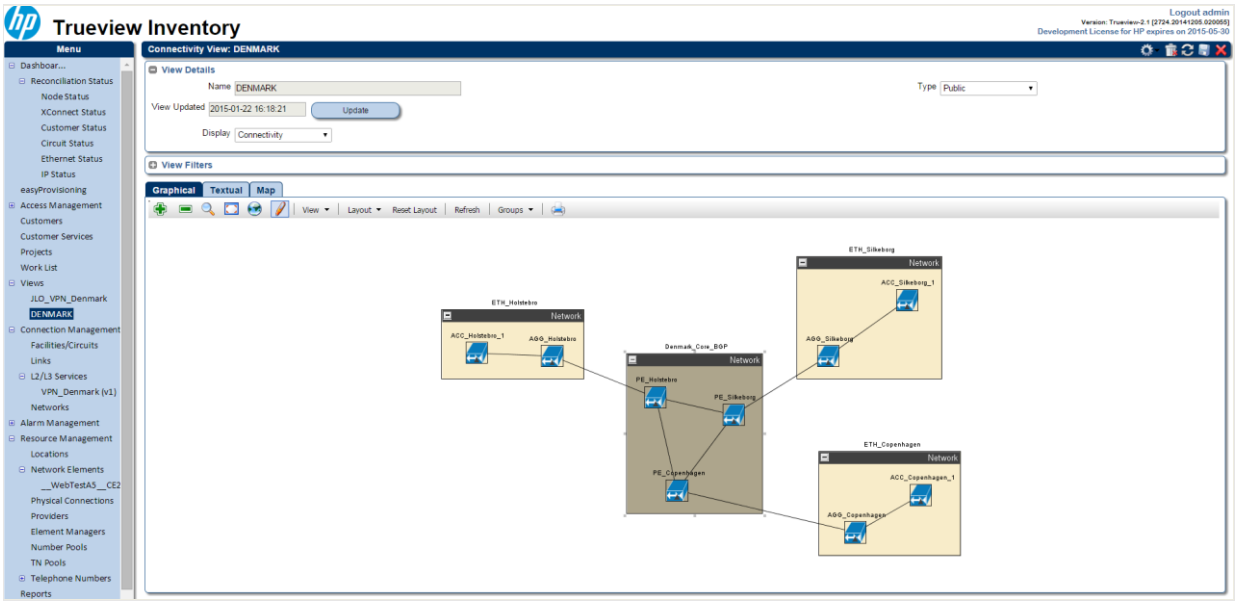
Once configured, the Ethernet network has to be in active state.

2.5.1.3 IP Pool

An IP pool has to be created in TV. This IP pool will be used to obtain the available IPs in order to provisioning the L3 connectivity between the customers (and core network). IP pools in TV are defined as number pools. The HPSP solution, by default, will use an IP pool called 'Simple-VPN-Pool'. This pool has to be created and configured in the Inventory with the appropriate IP ranges.

2.5.1.4 Preview

This is an example of a view in the TV Inventory, containing a BGP core network and three access networks located in different areas:



2.5.2 Access the HPSP VPN TE UI

Once the Inventory has been configured, the solution can be accessed and customer VPN services created and managed. Access the solution in this URL:

http://<hostname>:<port>

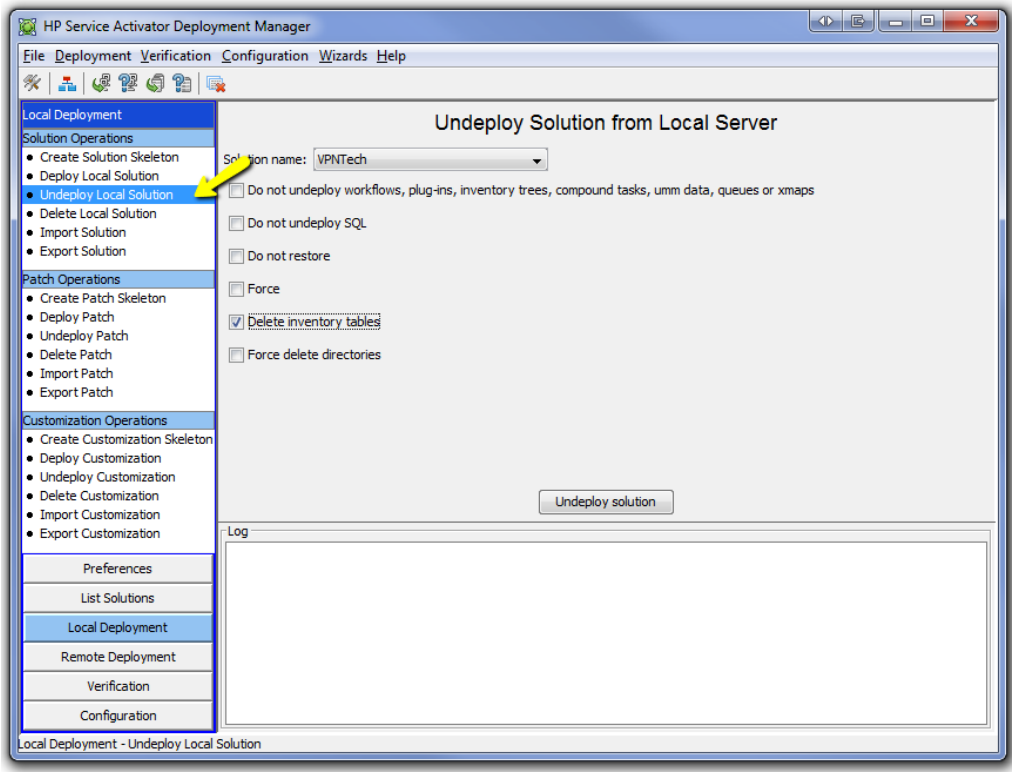
Where <host>:<port> are the host and port (typically 3000) on which the OSS Console has been deployed.

Please consult the HPSP VPN TE User's Guide for details on how to use the tool.

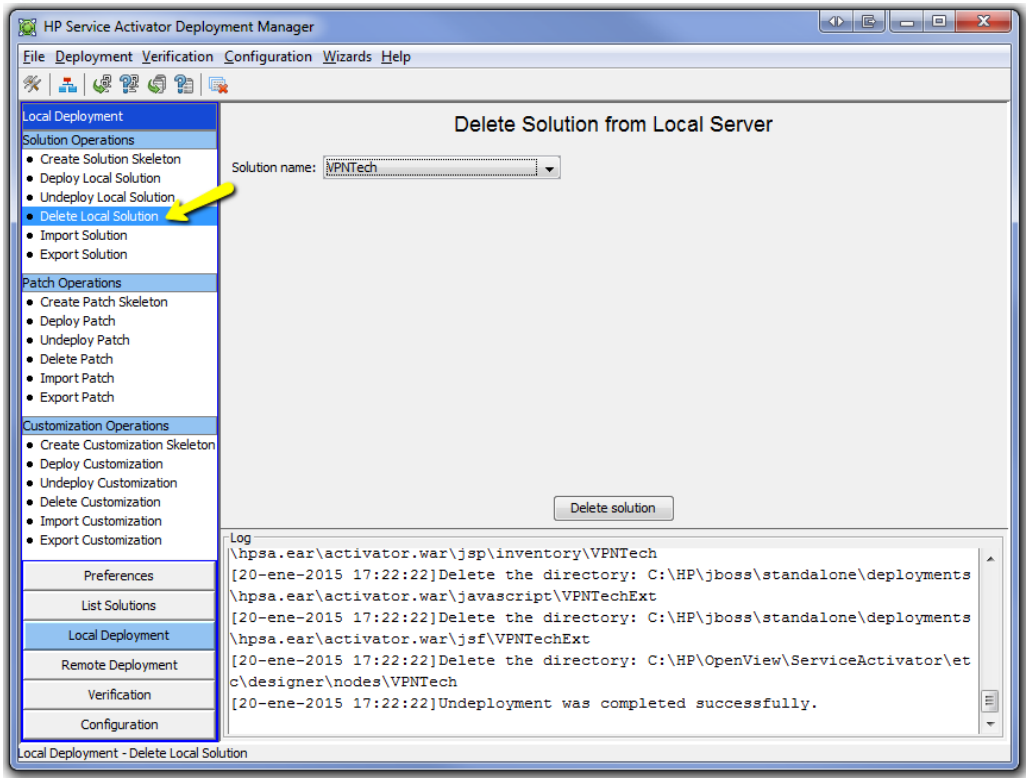
2.6 Uninstall the solution

Undeploy the HPSP VPN TE solution.

Go to Local Deployment -> Undeploy local solution, and select the 'VPNTech' solution. Check the option 'Delete inventory tables'. Click on Undeploy the solution.



Go to Local Deployment -> Delete local solution, and select the VPNTech solution. Click on Delete solution.



Please consult the guides of the different solutions included in the requirement list in order to uninstall the whole environment.

3 Appendix I: Customize the solution

3.1 UI Customization

The HPSP VPN TE UI is deployed on top of the HP OSS Console solution. Visual customizations are available out-of-the-box with this solution. Please consult the HP OSS Console documentation for more details about how to customize the look&feel of the solution.

3.2 Logic Customization

It's strongly recommended to use the services included in the HPSP VPN TE Catalog as they are. If a modification/extension of the logic is required, create your own products combining the existing services or use the pre-workflow and post-workflow functionality included in the HPSP, this way, the users can develop their own workflows and assign them to the CFSs and Products in the Catalog without changing the basic functionality and ensuring the backward compatibility for next versions.