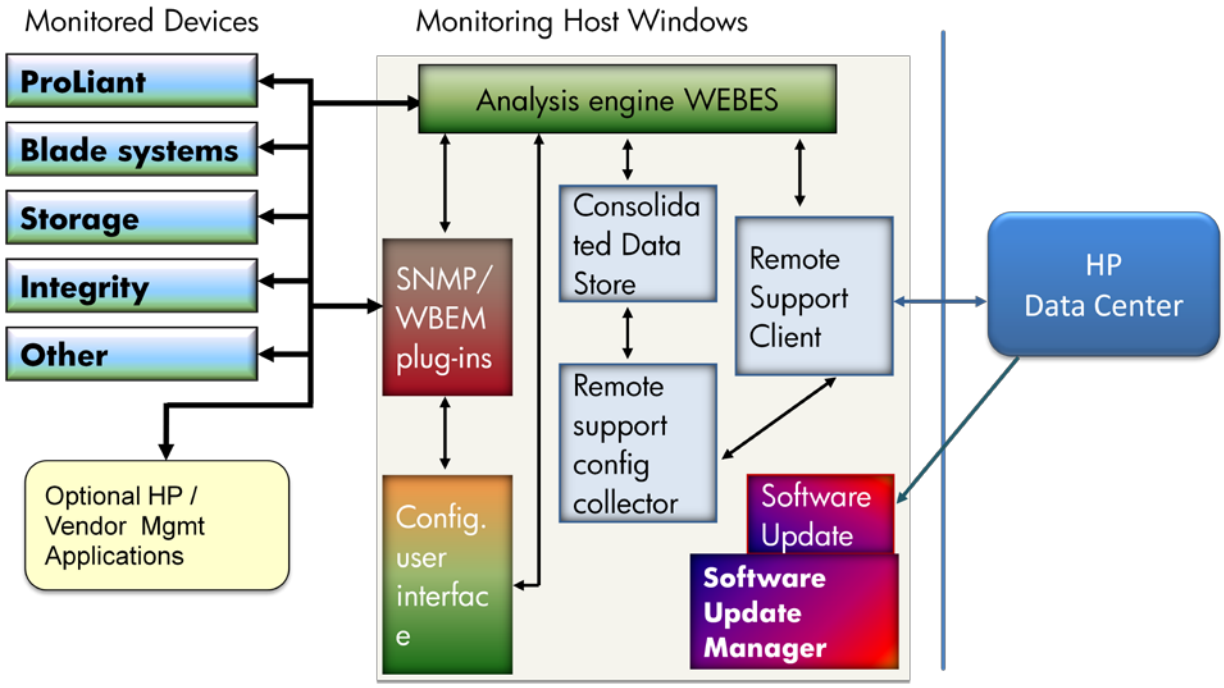
HP Insight Remote Support Standard

Handout for
Installation, Configuration, Trouble Shooting Tips

15-Feb-2011



This document describes the installation and basic configuration of Insight Remote Support. This handout is intended to be used in conjunction with the HP IRS Standard Quick Start Guide and the further IRS Standard documentation.

To keep this document up to date, please send your experiences to the author. Thanks.

Author: Werner Christoffel
werner.christoffel@hp.com

TABLE OF CONTENTS

1 Scope

May help to
- prepare to install and basic configure IRS Standard
- install and configure the remote support modules of IRS Standard
- configure the managed devices, that they are ready for remote support
- prepare configuration collections of the managed devices
- some trouble shooting tips
- have a supplement available to the official documentation

- This handout refers on the following IRS Versions A.05.30 to A.05.60

1.1 IRS Resources

- IRS Standard Documentation
- IRS Standard Software download (kit with all IRSS components)
- HP Insight Management WBEM Provider Information
- PSP Kit download (Proliant Support Pack)
- WEBES Documentation
- Remote Support workshop (installation demo movies) public accessible

Which managed devices are supported is listed up in the release notes.

1.2 IRS Standard References

Check ALWAYS for the latest version of these manuals, please.
The public accessible manuals are
- HP Insight Remote Support Frequently Asked Questions
- HP Insight Remote Support Quick Start Guide
- A.05.xx Insight Remote Support Release Notes
- HP RSSWM Configuration, Usage and Troubleshooting Guide for IRS

HP Internal documents:
- AMC User Guide (Data Centre Application Manager Console User Guide)

2 Prerequisites Checks

2.1 System Requirements for IRS

- Any 32 bit or 64 bit ProLiant or HP Blade server with
  - 2.8GHz CPU (recommended CPUs with 1MB or more cache total)
  - 2 GB or more physical memory (for IRSS)
  - 36 GB or more local, free disk space (for the OS and IRSS)
- **Important:** Support is provided for a static virtual machine environment only.
- Microsoft Windows server 2003 Standard and Enterprise (SP2 highly recommended)
  Microsoft Windows 2003 R2
  Microsoft Windows server 2008 Standard and Enterprise
  Microsoft Windows server 2008 R2 with IRS A.5.50 and WEBES V6.1 and newer
  Important: Windows 2008 Server Core is NOT supported.
- Fixe IP address
- SNMP service and trap service must be active
- Microsoft .NET Framework 2.0 or higher
  (necessary for Microsoft SQL Server 2005 and RSSWM)
  Important: .NET Framework 4.0 does NOT include the functionality of .NET 2.0. Therefore you must install a version previously than .NET 4.0.
- Windows Installer V3.1 (necessary for WEBES)
  downloadable from http://support.microsoft.com/kb/893803
- SUN Java Runtime Kit V 1.6.xx or higher
  (necessary for the WEBES User Interface)
- Is also supported to be installed on a Command View (SMS) server
  Important: do NOT install IRS onto a System Management Appliance (SMA)
- Minimum Version of Command View EVA, supported by IRS:
  - 7.01 for EVA arrays (if IRS is on a separate system)
  - 8.01 for EVA-LE arrays

  You can verify if the system meets the requirements under
  "**Start**" > "Programs" > "Accessories" > "System Tools" > "System Information"

2.2 Remote access to HP

For more details refer to the latest version of the manual IRS Security Overview, please.

Important: Redundant data center settings.
Round Robin may have to be configured on the customer's DNS servers.

IP Address	Server Name (alias)	Protocol	Service
15.192.8.184 15.216.12.26 15.217.96.178	services.isee.hp.com	HTTPS	IRS Content Server - Remote Support Data Center

15.193.0.152 15.192.17.238 15.201.40.168	rsswm.policy.hp.com	TCP over SSL	IRS Software Policy Server (Radia)
15.193.0.153 15.192.17.239 15.201.40.169	rsswm.software.hp.com	HTTPS	IRS Software Download Server (Radia)

Important: Depending on the service needs the HP Server Names (alias) may not constantly be reachable all the time via all of the listed IP addresses. Therefore the IRS server must use DNS resolution instead of the hosts.

- It is recommended to configure the alias names in the firewall, because the IP addresses may change.

Quick check:

- telnet rsswm.policy.hp.com 443 <- blinking cursor, exit by typing 2 words
- https://rsswm.software.hp.com:443/site <- RSSWM is operating correctly
  or
  https://rsswm.software.hp.com/proc/rps/stats <- some statistic figures
- https://services.isee.hp.com/version/index.html <- Version number

Testing each individual instance:

- *Remote Support Data Center* (services.isee.hp.com)
  https://rsdc-pro1-services.austin.hp.com/version/index.html
  https://rsdc-pro2-services.austin.hp.com/version/index.html
  https://rsdc-itg1-services.atlanta.hp.com/version/index.html
  Could also be tested with the command `telnet`

- *RSSWM*
  https://rsswm-software1.atlanta.hp.com/site
  https://rsswm-software2.atlanta.hp.com/site
  https://rsswm-software.houston.hp.com/site
  Could also be tested with the command `telnet`

  telnet rsswm-policy1.atlanta.hp.com 443
  telnet rsswm-policy2.atlanta.hp.com 443
  telnet rsswm-policy.houston.hp.com 443

IRS Supported transportations:

- Connection directly to the HP backend via the Internet or via Proxy conforming to the HTTP/1.0 specification
- tcp (https) port 443 outbound with established back

IRS NOT supported transportations:

- NTLM authentication (also known as Integrated Windows Authentication).
- Kerberos authentication
- Proxies using proxy auto-configuration scripts

Important: The Insight Remote Support Client configuration may fail if a customer's firewall or security software filters network communication between the monitored client and the HP Support Center. For example, some firewall software, such as WatchGuard firewall, filters some HTTP protocols by default. It may block http redirection, http download of compressed files, etc. In those cases, change the firewall settings so that it does not block ANY HTTP communication between the CMS and the HP Support Center. Verify that it passes any HTTP 1.0 standard protocol between the CMS and the HP Support Center, so that it meets the communication requirement (tcp 443 outbound with established back).

RSSWM on the Hosting Device communicates over HTTPS/443. Likewise, the Remote Support Client component also communicates over HTTPS/443 to submit incidents to and retrieve entitlement information from the HP Support Center. HTTPS provides encryption for confidentiality of software configuration data collected from the Hosting Device and transferred to HP.

2.3 SNMP community names

Recommended to define community names for the SNMP communication (examples)

- "trap" > rspsnmp
- "read only" > rspsnmp (optional for the moment)
- "read create" > rsp-snmp (optional for the moment)

2.4 Default User Profile

Important: For RSSM installation a user account with "administrators" rights is necessary.

- Any user with "administrators" rights can be used
- May be the same as for Command View

2.5 Necessary kits for IRS

- ProLiant support pack (PSP) actual version recommended
- Insight Remote Support Standard kit (kit with all necessary RS packages)
- Microsoft .NET Frameworks 2.0 SP1 or higher
- SUN Java 1.6.xx or higher recommended

2.6 Remote Desktop Access

To prevent unpredictable results start Remote Desktop always with console mode.

- "Start" > "Run…" > mstsc /console for Windows XP SP2 and earlier
- "Start" > "Run…" > mstsc /admin for Windows XP SP3 and newer

(figure out the suitable one by "Start" > "Run…" > mstsc /admin)

Important: The initialization and registration of Remote Support Software Manager (RSSWM) can only be performed by a user who is logged onto the Hosting Device via the system console or a console-mode RDC Session.

2.7 Windows 2008 add SNMP and .NET Framework

These products can be activated in the following way:

- select "Start" > "Settings" > "Control Panel"
- select "Programs and Features"
- click on "Turn Windows features" on or off
- click on "Features"
- click onto "Add Features"
- select the services SNMP and .NET Framework

Note: IRSS will install .NET Framework 2.0 automatically if it's not installed yet. Windows 2008 has version 3.0 built in. This version covers also the 2.0 functionality.

2.8 Windows 2008 local firewall settings

Per default most of the remote access methods are blocked by the Windows 2008 firewall. Example: If you fail to access WEBES or the SMH on this system using another computer in the local network, the remote access can be opened for these applications.

This could be done by

- " Start" > "Programs" > "Administrative Tools" > "Windows Firewall
- "with Advanced Security"
- Select "Inbound Rules"
- click on "New Rule..."
- add new rule with its application ports

Important: Always make modifications ONLY with the customer's agreement.

2.9 Some Resources Consumption Data

Examples of a ProLiant G3 Server with 2GB of physical Memory

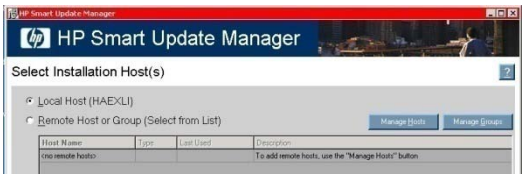
Program	Memory Consumption
Java.exe	30'000 kB
DESTAService.exe	560'000 kB
ELMC WCCproxy	2,000 kB
CAAgents	3'500 kB
Uc.exe	20'000 kB
PostgreSQL (DB for WEBES)	100'000 kB
Radxxx.exe	1'000 kB

2.10 PSP - ProLiant Support Pack Installation

Note: IRS Standard does not need a System Management Homepage that it's running as expected. It's recommended to install an actual and supported version of a PSP when IRSS will be installed on a physical System, that the IRS server can also be monitored.

Example to install the PSP:

- Create a directory like `C:\PSP`
- Unpack the PSP kit into this directory
- Start the installation by `C:\PSP\setup.exe`



Important: On a virtual system only the System Management Homepage can be installed. For all other modules of the PSP the prerequisites do NOT exist.
If you installing IRSS onto a virtual platform, it is highly recommended to configure this ESX or ESXi platform into IRSS to monitor this physical device.

2.11 Check for remote access to HP

Now check if you have access to the HP Remote Support backend.

3 Install IRSS

3.1 Used Application Ports

Remark: This port list covers basically the application ports, which are being used from the components on the CMS themselves, that they can communicate which each other locally.

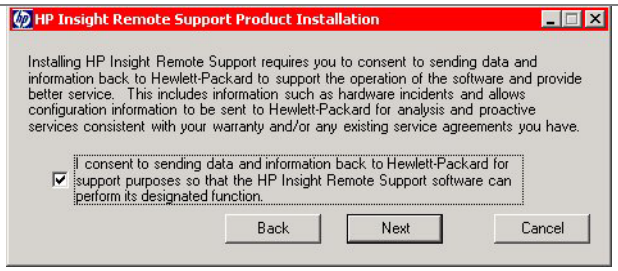
-	ICMP (ping)		IRSS	→ MS	discover function by HP-SIM, UDN
-	SMTP	25	IRSS	→ Mail	Local WEBES mail to local SMTP server
-	SNMP	161	IRSS	→ MS	communication IRS to the MS
-	SNMP Trap	162	MS	→ IRSS	service incident to WEBES
-	HTTP	2301	IRSS	→ MS	start/enter SMH when it is in standby mode
-	HTTPS	2381	IRSS	→ MS	enter the SMH
-	WBEM	5989	IRSS	→ MS	default WBEM CIMOM port
-	WBEM WMI	6989	IRSS	→ MS	WMI port (Pegasus WMI Mapper)
-	HTTPS	7906	MS	→ IRSS	WSEA user interface access
		7906	IRSS	← → IRSS	
-	WCCproxy	7920	IRSS	← → IRSS	communication RSC and other WCCProxy(ies)
-	WCCproxy	7920	MS	← → IRSS	service incident to WEBES
-		7950	IRSS	← → IRSS	PostgreSQL – WEBES

3.2 Installation of IRSS

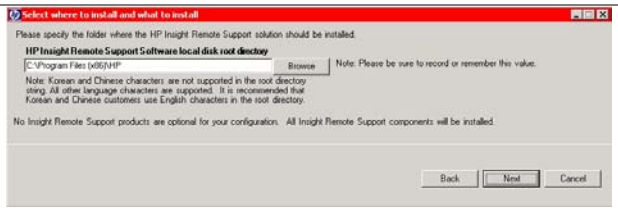
Depending on the used version of the kit the sequence may be different.
The Remote Support Software Manager (RSSWM) User Interface requires administrator privileges on the Windows operating system.

Download the kit form the software depot
Start the installation by double clicking to **`rs_stdxxxxxx.exe`** .
(This kit can also be used to upgrade previous installations. It does also upgrade the RSSWM.)

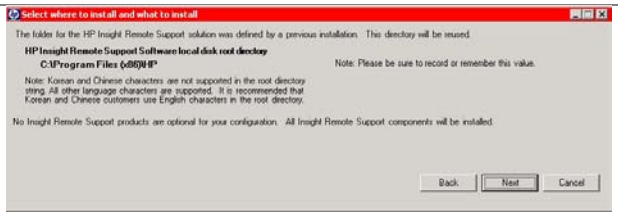
First you have to agree to the license conditions.



You must agree to this statement.

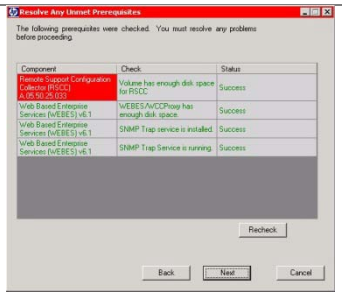


The installation location can be defined here, if it's a first time installation.



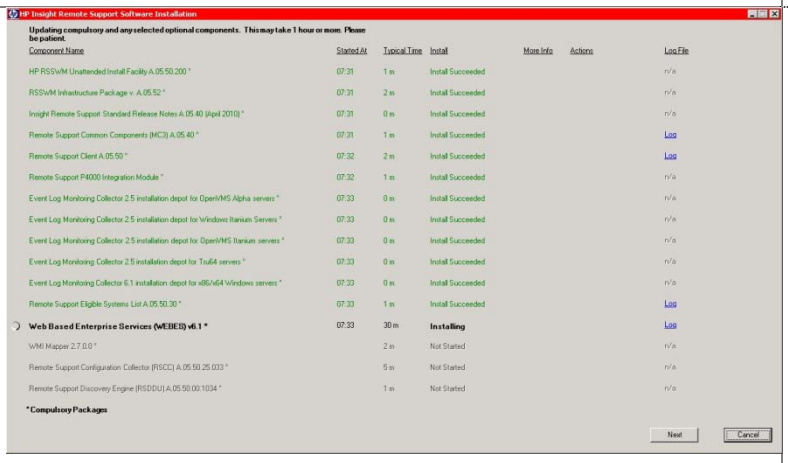
The default installation location is recommended.

If you're upgrading, this data path cannot be modified.



All prerequisites must be met before you can continue.

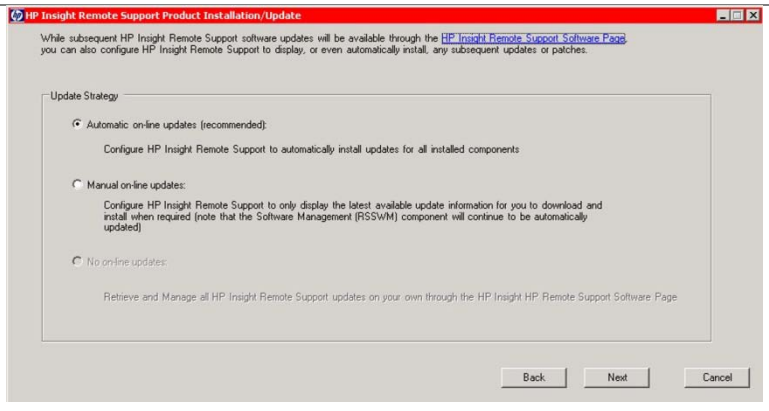
(You can set up the missing SNMP service without exiting the IRS installation.)



All compulsory and additionally selected kits will now be installed.

You may read the log files to find a possible reason, why the installation failed.

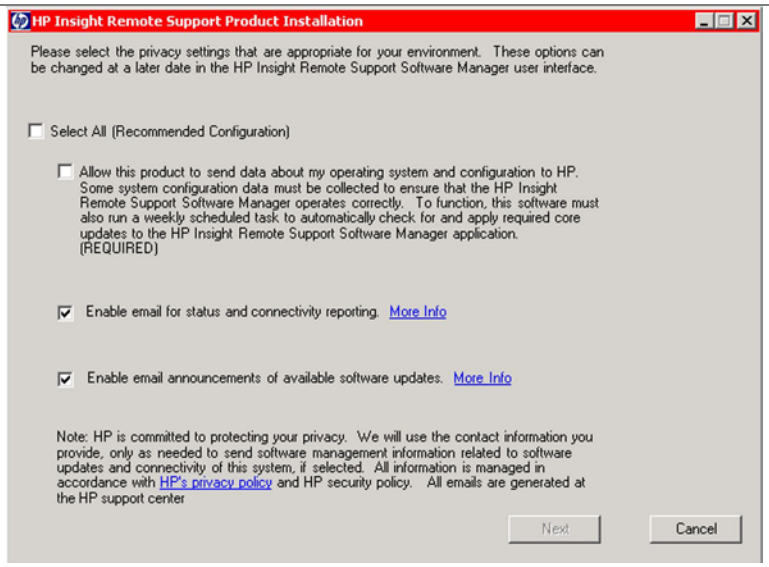
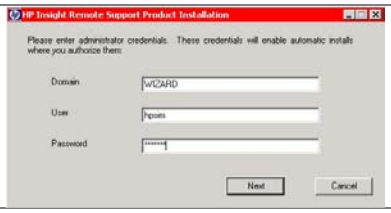
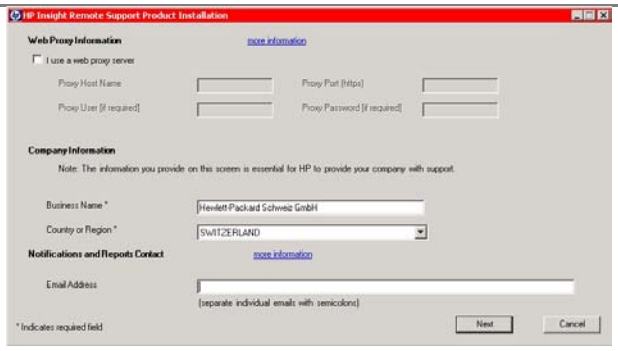
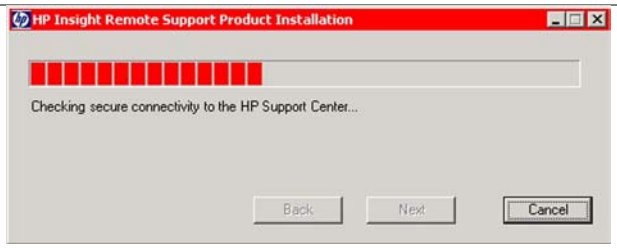
A "retry" button may appear if a package has failed to be installed correctly; very helpful.



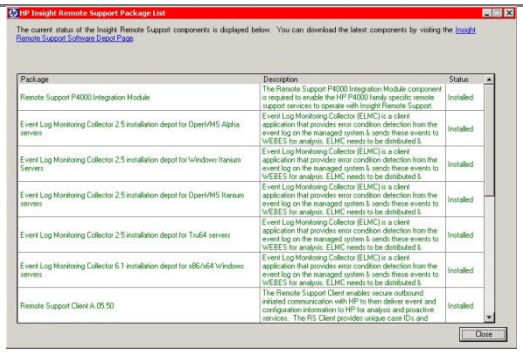
Select the update modus and the kit source. Typically: Automatic update.

This can be modified anytime.

No on-line update can be chosen only with the first time installation.

	Here "Select All" During the next steps some fields can still be kept empty.
	Enter the user credentials, which allow automatic installs where you allow it. (User must have local administrator rights.)
	Enter the proxy information here, if necessary, for the remote access to HP. The correct company name is highly recommended. Select the country where IRS is being installed. This notification is about RSSWM status.
	This connectivity test must be successful. (If the connectivity test fails, the settings on the proxy may be a reason.)

IRS installation successful. You can open the status list of the installed packages.



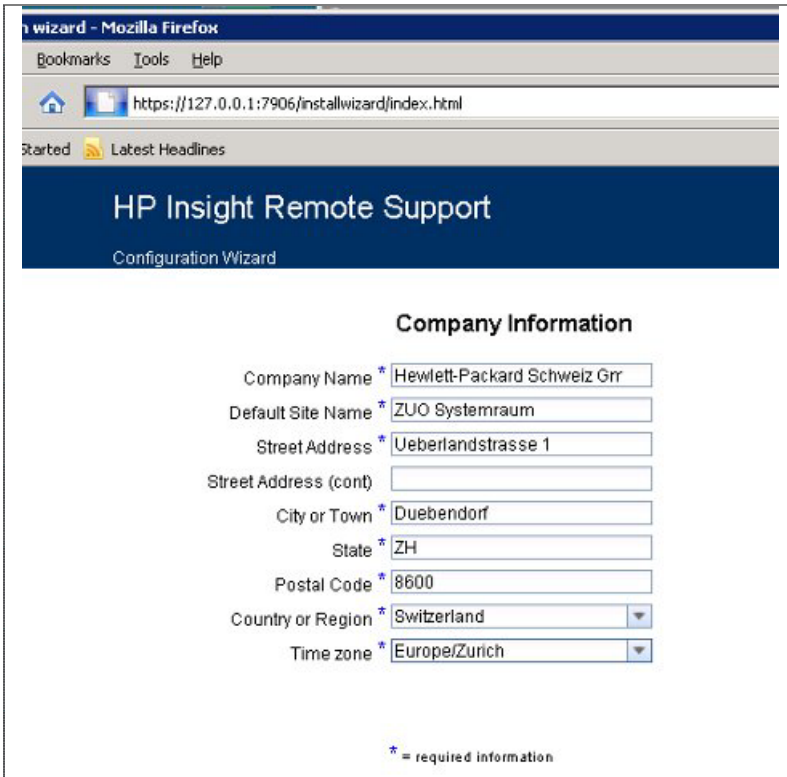
Example of such a status list.

This info box may be helpful later on too.

The IRSS basic configuration will start right now.

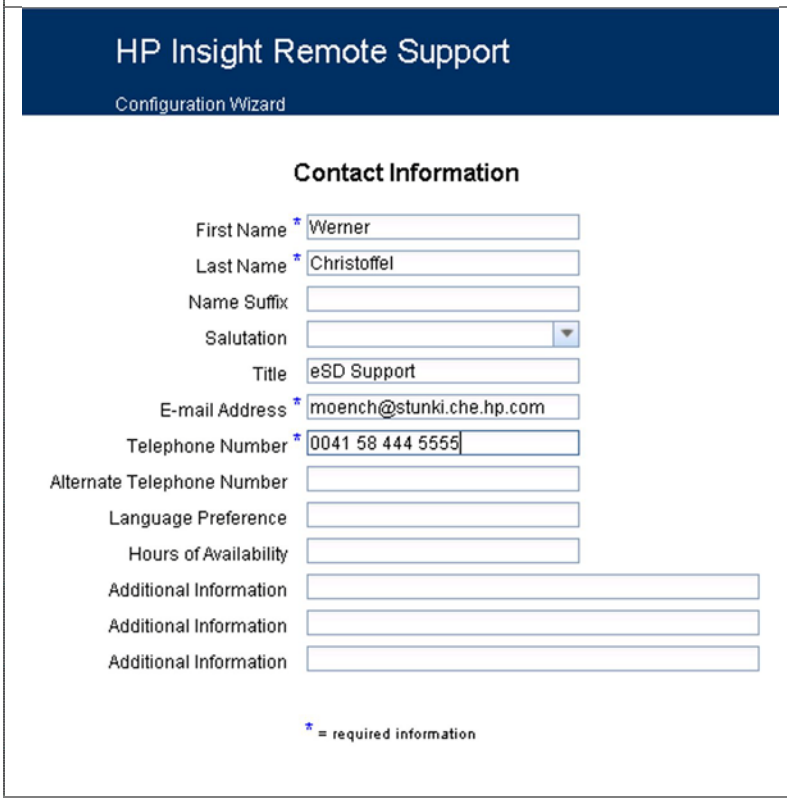
You must scroll down the text and accept to the license agreement to be able to configure and enable the remote support.

Next you can choose if HP may collect some information about the IRS server.

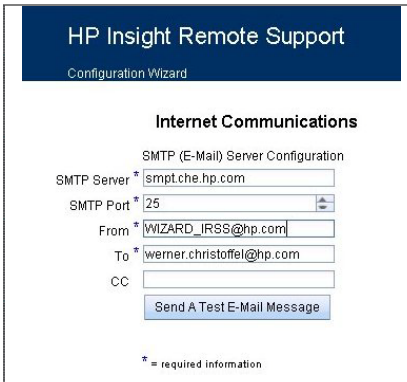


These are primary location information, which HP is using in case a problem incident has been sent to HP's call system.

Additional address information can be added, if a managed device is physically located in a different place.

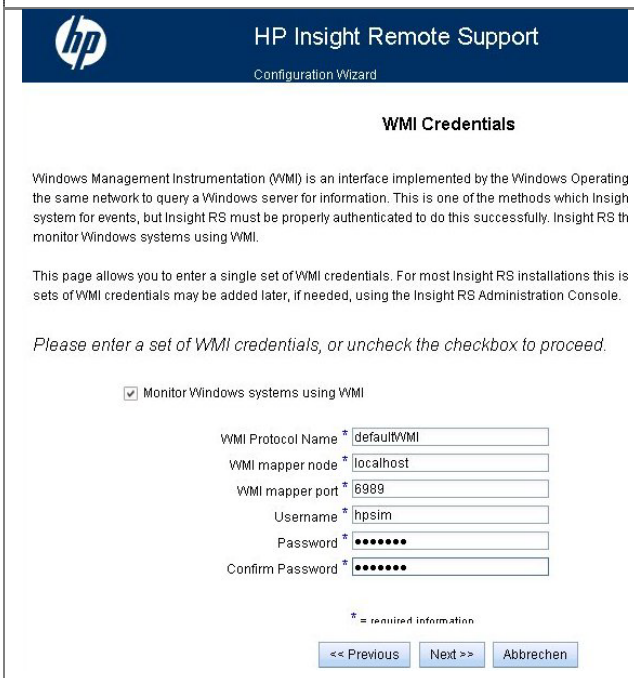


These are the primary contact information, where HP is using in case a problem incident has been sent to HP's call system.



Local mail notification setup.

You may also modify the "From" mail address, to figure out more easily which IRS server did send it.

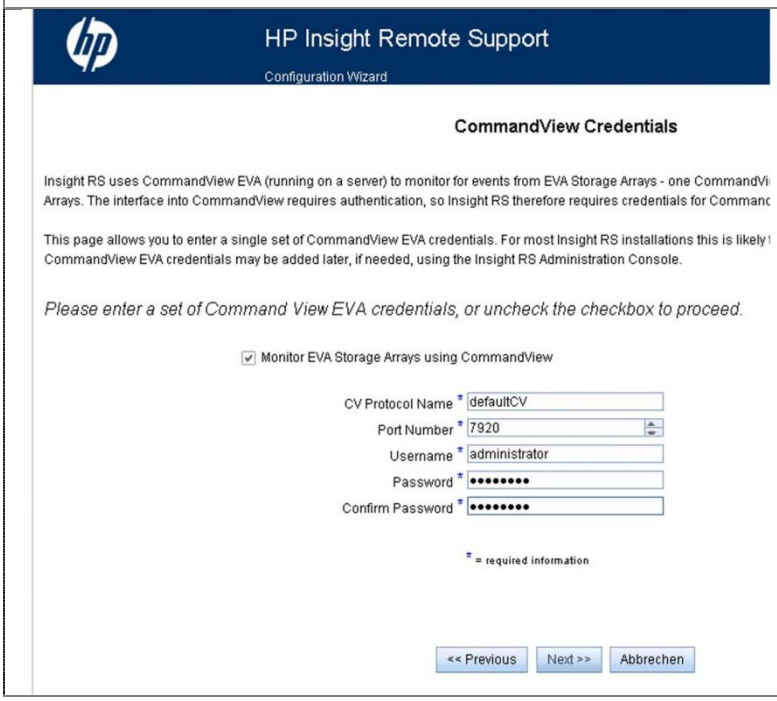


If known, the WMI transport and authentication credentials can be added now.

They can be modified anytime.

With IRSS A.05.50 on you can define your preferred WMI port (recommended default port 6989).

The Pegasus WMI mapper will automatically be configured with this information.

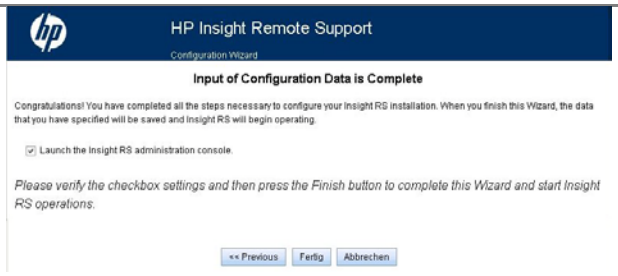


To access Command View WEBES uses ELMC_WCCProxy and a user account to log into CV.

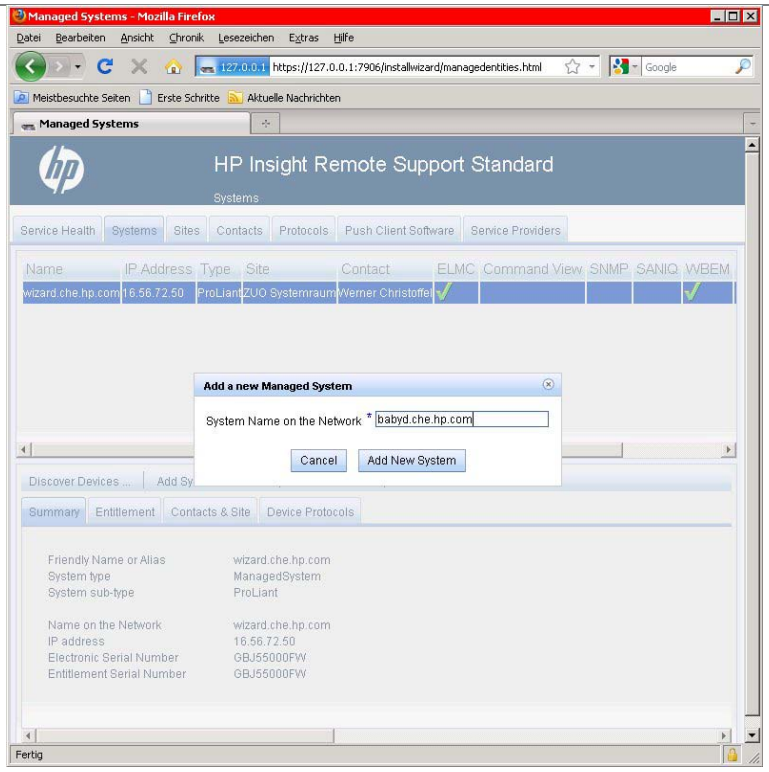
(It's highly recommended to use the default port 7920)

Enter the username and password, which is being used by Command View EVA.

Now you can have a quick check, before IRS is being configured with the entered information.

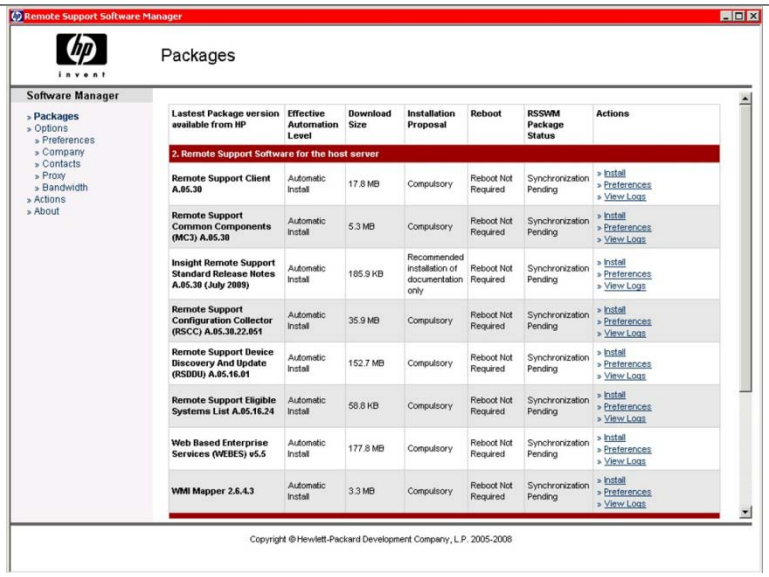


To add the first managed systems, activate Launch the IRS administrator console.



Now you can add your firs devices, when you first click onto the Systems tab then by the Discover Devices or Add Device function.

IRS is optimized for up to 50 managed devices.
In a bigger environment limit the IP address range to 100 maximum, when IRS has to discover the devices automatically.



RSSWM must show all compulsory kits as installed.

When you see "Synchronization Pending" go into "Options" – "Preferences" and click on "Synchronize Now".

Remark: This button has become available with the IRS kit A.05.30.

3.3 RSSWM Installation Success Check

The following Start menus can be visible (its short description):
"Start" > "Programs" > "Hewlett-Packard" > "Remote Support Software Manager"

- "Initialize Remote Support Software Manager"
  is visible, when the installation partly succeeded only
- "Uninstall Remote Support Software Manager"
  does uninstall/deactivate the RSSWM
- "Remote Support Software Manager User Interface"
  menu link replaces the "Initialize" one, if RSP has been successfully installed

3.4 IRS Packages Visible in "Add or Remove Programs"

- HP OpenView Configuration Management Agent — part of RSSWM
- (Radia transport software) — part of RSSWM
- Hewlett-Packard Remote Support Client — IRSS
- HP Insight Remote Support — IRSS
- HP LeftHand CLI — Adapter for P4000 storage device
- HP Mission Critical Common Component (MC3) — MC3
- HP Remote Support Configuration Collector — IRSS - RSCC
- HP Remote Support Discovery Engine — IRSS
- HP WEBES 6.x — V 6.x
- WCCProxy — ELMC_WCCproxy V6.x
- psqlODBC — PostgreSQL interface
- Pegasus WMI Mapper V2.x — IRSS WBEM/WMI communication

- Microsoft .NET Framework 2.0 or higher used by RSSWM

3.5 Kit Locations for Managed Devices

Depending on the Services additional software packages have to be installed on the managed devices. The following kits will become available on the IRSS server, located in

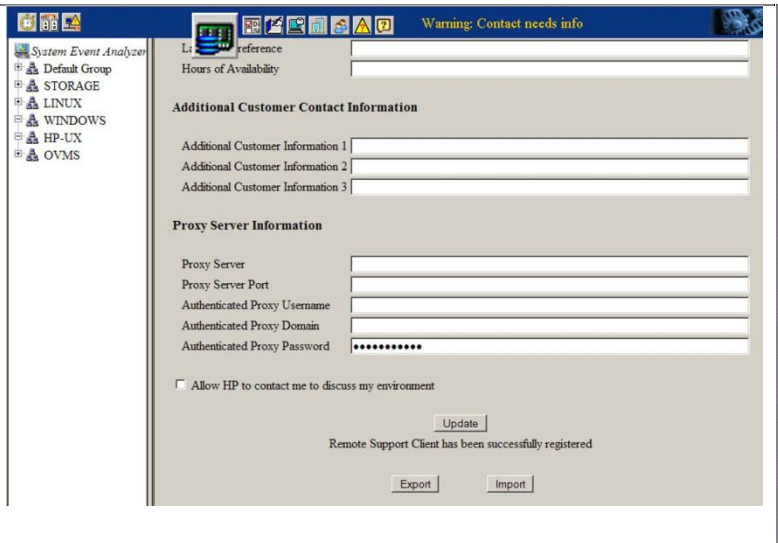
`C:\Program Files\HP\Installers`

- ELMC = ELMC_WCCProxy for Windows
  (to be installed also on command view EVA servers)
- MC3 = necessary on the IRS server
  (to be installed also on command view EVA servers)
- ReleaseNotes = list of supported devices and information about the installed version
- RSC = necessary on the IRS server
- RSC\Windows\EndNodePush = PSP Kit for Windows (delivered with IRSS)
- RSDE = Remote Support Discovery Engine
- UC\RSCC = necessary on the IRS server
- WEBES = necessary on the IRS server
- WMI Mapper = (Pegasus WMI Mapper (CIMOM)) necessary on the IRS server

3.6 Configure the access to the Content Server

With a new installation you may be led automatically to the RSC Settings page.
The message "Remote Support Client has been successfully registered" says, that the connection to **`servies.isee.hp.com`** is working.

Please enter always the correct address and contact information.
This information can be modified any time.
Open the WEBES / SEA user interface (https://<IRS-server>:7906)



Click onto the (here enlarged) icon.

Scroll down to the bottom and check for / add the proxy information you have used in RSSWM.

Click to update.

The message "Remote Support Client has been successfully registered" must be displayed.

Possible connectivity test to HP:
- press the "Update" button
The proxy settings can be changed or released, if the connection to HP fails, then press the "Update" button again.

3.7 Submitting a test incident, RSC remote connection test

You can submit test incidents in the following way:
go to `C:\Program Files\HP\RemoteSupport\bin`
run `iseeInterfaces.exe –send_support_information –test_event`
result: incident number, like `9EA5042f-60BA-4C9C-8D23-7FB41DC5EE22`

To submit a test event which includes WEBES, you must press the button "Test Event" in WEBES under "WEBES Notification Settings".

4 Add / Discover Devices and Protocol Configuration

Start the IRS Admin Console under
"Start" > "Programs" > "Hewlett-Packard Services Tools" > "Insight RSS Admin Console"
or by
https://<IRS-server>:7906/Installwizard/managedentities.html

4.1 Add / edit protocols

Recommendation: Add all known protocols with all known credentials now, before you start to discover the managed devices.

Example: When the HP-UX systems use different usernames and/or passwords, which are necessary for the WBEM communication, add (name) first the necessary UNIX-WBEM communications. The protocol with the matching credentials will automatically been taken.
If all necessary protocols have been added and configured, devices like EVAs appear very quickly, as soon as the SMS has been discovered or added.

Setting up a complete protocol:

1. Select "Add Protocol" – add the protocol you need
2. Select "Edit Protocol" – enter the necessary credentials

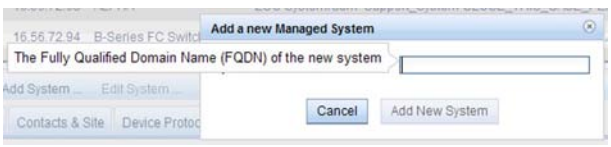
4.2 Add / Edit Sites and Contacts

Important: Do not add a Site and/or a Contact with empty mandatory fields linked to a managed device. This will result in "Undelivered: ISEE;" service incidents.
Add Sites and Contacts here for devices which are located in different Places and where there is an allocated Contact.
This information is being placed on top of the GCSS case, if a service incident will be sent to HP.
WEBES V5.6 Update 1 or higher – Managed Sites: must not remain empty!!

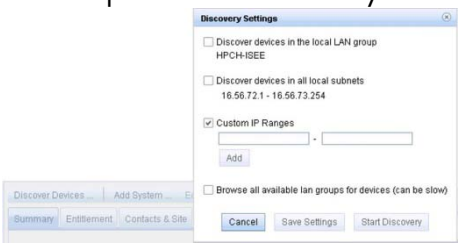
- Postal Code
  (otherwise the incidents are not being submitted to HP)

4.3 Add / Discover a Managed Device

To add a single device select "Systems", then select „Add System …" and enter the full qualified node name or its IP address.

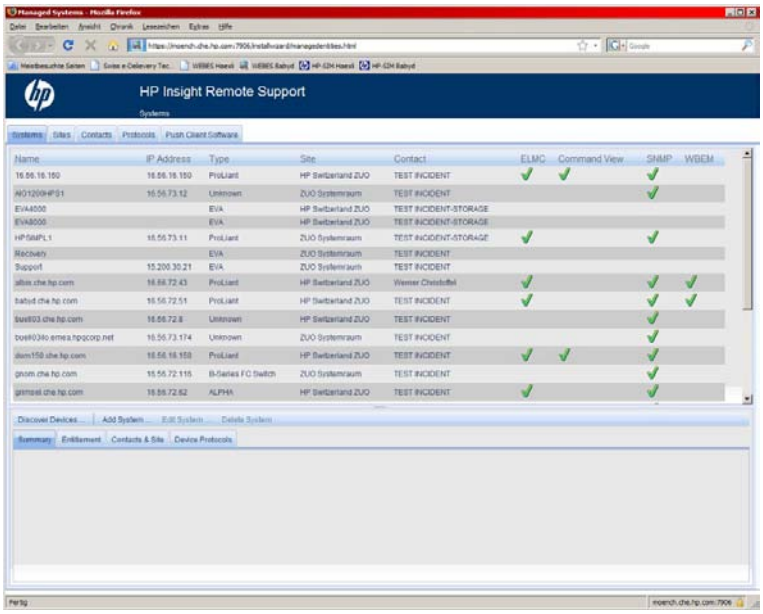


For multiple devices select “Systems” then select “Discover Devices…”



Discover devices can be used to scan within a workgroup, IP ranges, etc.
Important: to prevent unexpected behaviour, limit the IP range to 100 maximum.

EVAs are automatically being added as soon as the command view server has been added to the list.



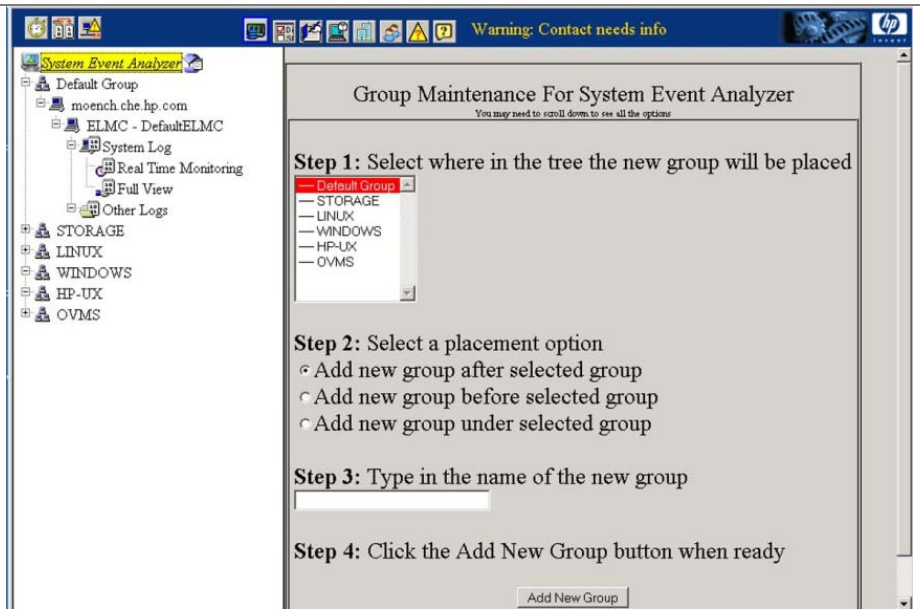
The device list may look like in this example.
Important: To prevent from unexpected behaviour close the WEB browser, which is displaying this user interface as soon as you have finished your work here.

4.4 Add Groups and Devices to the SEA List

To add the devices into the “System Event Analyzer” list may be very helpful to check

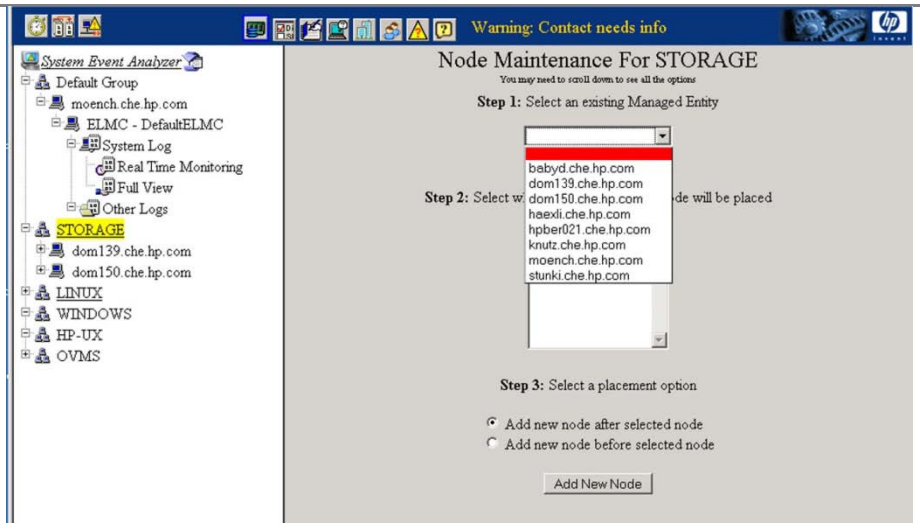
- if the necessary settings are really correct and complete
- for some troubleshooting

This operation is described in detail in the WEBES User Guide
Complete the device configuration in IRS by adding the devices in WSEA.
Enter WEBES using a WEB browser (https://<IRS-server>:7906).



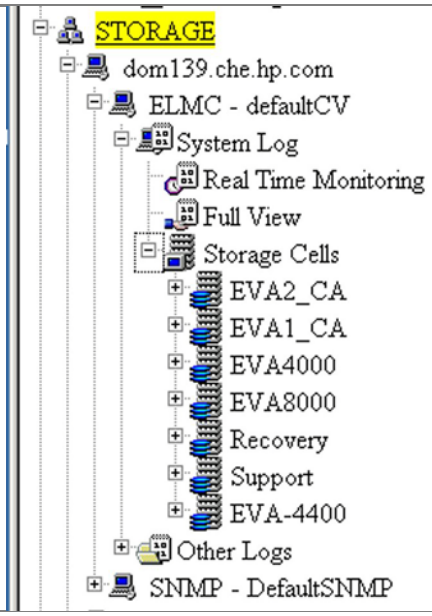
Create new groups as necessary by clicking onto "System Event Analyzer"

Follow the steps 1 to 4



Now select the group, where you want to add a new device.

Follow the steps 1 to 3



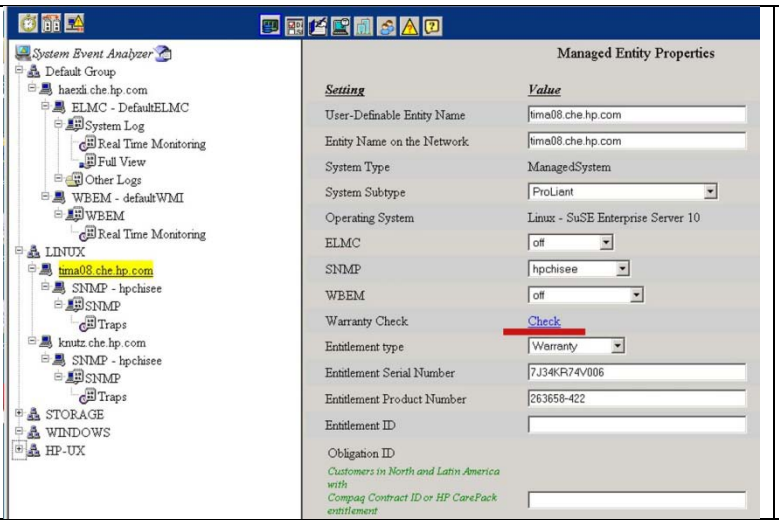
To add EVAs, only the command view server has to be added.

The active EVAs are automatically being listed up under the ELMC protocol

4.5 Entitle a device

Service incidents of devices without support coverage may not be transferred to WFM.

An entitlement check can be done in WEBES



.. click onto 
.. click "View Full List"
.. select your system
.. add the missing product number
.. click on "Check"

On a public HP-WEB site you'll see the result.

Alternatively the entitlement check can be done in www.itrc.hp.com under "Warranty Check".

5 IRS User Interfaces

The most important user interfaces can also be accessed by using a WEB browser.
The WEB browser based user interfaces can also be accessed by another system within the company internal network.

5.1 IRS Admin Console (Managed Entities)

"Start" > "Programs" > "Hewlett-Packard Service Tools" >" IRS Admin Console"

https://127.0.0.1:7906/installwizard/managedEntities.html

The "link" can be copied onto the desktop of
%Start Menu\Programs\Hewlett-Packard Service Tools\IRS Admin Console

5.2 WEBES / WSEA user interface

"Start" > "Programs" > "Hewlett-Packard Service Tools" > "System Event Analyser" > "System Event Analyser"

https://127.0.0.1:7906

5.3 RSSM User Interface (Remote Support Software Manager)

"Start" > "Programs" > "Hewlett-Packard" > "Remote Support Software Manager" > "Remote Support Software Manager User Interface"

Or you can add an icon onto the desktop with the following items
`C:\Program Files\HP\CM\RSSWM\GUI\swmui.hta` (shortcut on the desktop)
and
`C:\ProgramFiles\HP\CM\RSSWM\GUI\img\favicon.ico` (proper icon for RSSWM)

6 Windows Systems

6.1 Used Application Ports

-	ICMP (ping)		IRSS → MD	discover the device
-	TCP	135	MD ←→ IRSS	WBEM/WMI – DCOM communication start
-	TCP	→ 1024	MD → IRSS	WBEM/WMI Data transfer, one additional free port in the range of 1024 – 65535 (mostly between 1024 – 2000)
-	SNMP	161	IRSS → MD	communication to the Insight Agent if SNMP is being used
-	SNMP Trap	162	MD → IRSS	SNMP traps (incidents)
-	WBEM/WMI	6989	IRSS ←→ WMI	If WBEM/WMI is used instead of SNMP; WBEM communication between WEBES and Pegasus WMI Mapper (port number may be a different one)

6.2 To be installed on the managed device

To use the most actual version of PSP for the IRS server is recommended. The most actual PSP kits can be downloaded directly from http://www.hp.com/bizsupport or from http://h18013.www1.hp.com/products/servers/management/psp .
Basically a PSP kit will be installed with the basic installation of the OS using the Smart Start CD.

6.3 To be configured in IRS – SNMP

The entire described credential configuration can be done in
`https://<irs_server>:7906/installwizard/managedentities.html`
and in
`https://<irs_server>:7906` (WSEA user interface)

Important: the read only community name and the trap community name must be the same.

First:

- Specific SNMP community name(s) may be defined/added on the managed device(s)
  - In WEBES under "Managed Protocols" ( ) add a SNMP protocol by pressing the button "NEW"
- Name the protocol like SNMP_public
- Enter now the Read Community name
  If multiple community names are being used, you can configure several different SNMP protocols in WEBES.

Second:
Now the managed devices using SNMP communication can be configured and discovered.

6.4 Configure / Verify WBEM/WMI Settings

Note: The Port for IRS to Pegasus WMI Mapper communication will be set to 6989 per default during the installation of IRS A.05.50 and newer.

When WMI communication should be used instead of SNMP for Windows systems (SMH) the Pegasus WMI mapper will be used to enable this communication between the managed device and IRS.
The WMI mapper itself communicates with IRSS via WBEM. In such a case, if two applications are running on the same system, which communicate via WBEM to IRS, the two applications need different ports.

Proposal: use port 6989 for the Pegasus WMI mapper communication. The default WBEM port 5989 remains free for other WBEM communication.

Steps to do

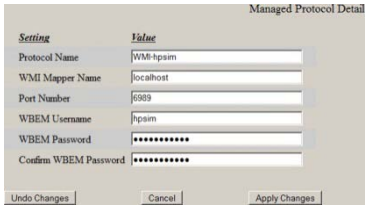
- stop the service **"Pegasus WMI Mapper"**
- add or modify the entry **httpsPort=6989** by editing the file
  `C:\Program Files\The Open Group\WMI Mapper\`
  `cimserver_planned.conf`

```
enableRemotePrivilegedUserAccess=true
enableHttpsConnection=true
enableHttpConnection=false
sslCertificateFilePath=C:\hp\sslshare\cert.pem
sslKeyFilePath=C:\hp\sslshare\file.pem
httpsPort=6989
```

- start the service **"Pegasus WMI Mapper"**
- check for the new application port using the command **C:\> netstat –aon**
- check for the process by **C:\>tasklist /fi "PID eq <process-number>"** , example:

```
C:\Users\Administrator>tasklist /fi "PID eq 7084"
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
WMIServer.exe                 7084 Services                   0      8'604 K
```

- Configure now the WBEM/WMI protocol in WEBES under "Managed Protocols" by
  - pressing the NEW button
  - select as Protocol Type "WMI WBEM Windows"
  - give a name like "WMI_Mapper" (press Apply Changes)
  - add / modify the port number to 6989
  - add the privileged user name and password, which is being used to access the managed device's SMH.

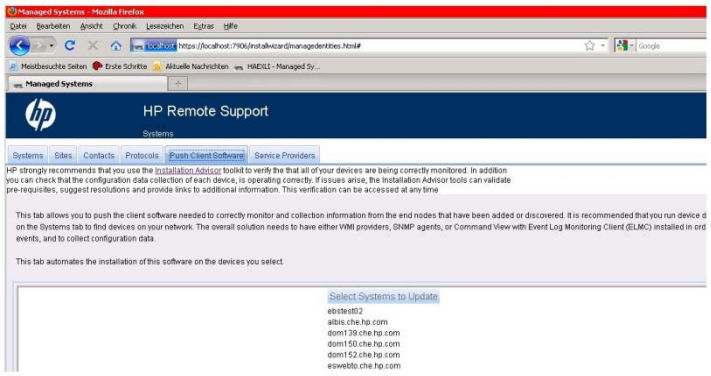


The user name must exist at least on the managed device.

Now all managed devices using WBEM/WMI communication can be discovered and configured.

6.5 Push Client Software

For Windows Systems it is also possible to install/update the insight agents (PSP) by the "Push Client Software" function in the IRS Admin Console (The version, which is being delivered with the IRSS kit is 8.25). This PSP kit is located in
`C:\Program Files\HP\Installers\RSC\Windows\EndNodePush.`
This kit is also being automatically updated by RSSWM (but not automatically installed).



A PSP kit, which covers the IRS supported Windows versions is located in
`C:\Program Files\HP\Installers\RSC\Windows\EndNodePush`

This kit is being used by the "Push Client Software" function to install and update other Windows systems with PSP (SMH)

7 EVA – Storage

7.1 Used Application Ports

-	ICMP (ping)		IRSS -> SMS	Discover the SMS (protocol UDN)
-	SNMP	161	IRSS -> SMS	communication to the Insight Agent
-	SNMP Trap	162	SMS -> IRSS	SNMP Incidents
-	WBEM / WMI	6989	SMS <-> IRSS	if WBEM / WMI is being used instead of SNMP (or a different port, depending on the configuration) Communication with Pegasus WMI Mapper
-	ELMC WCCproxy	7920	IRSS <-> SMS	service incidents

Note: The command view server has to be configured as described in the chapter Windows System. When the Command View server is being discovered into IRS, the active EVAs in CV will automatically be recognized via the ELMC_WCCProxy protocol.

7.2 To be installed on the SMS / SMA

If the Command View Server is a separate System

Important:

- If the hardware box is a SMA, use ONLY the qualified Insight Management Agent.
- ELMC_WCCProxy 2.5 or newer is necessary for CV EVA V9.0 or above
- ELMC_WCCProxy 6.xx is highly recommended for CV EVA 9.3 or newer

Supported:
Command View EVA V7.1 and newer, if IRS is being installed on a different server.
Command View EVA V8.0.1 and newer if IRS has to be installed on the same server.

Command View EVA is available from http://www.hp.com/support/downloads
Command View V 8.xx needs a license, for which has to be paid for.

To be installed on the SMS (Command View Server):

- Command View EVA Version 7.01 or newer
- SMI-S EVA and SMI-S CIMOM (for CV versions up to 7.xx)
- SMI-S (CIMOM) services (for CV 8.xx or above)
- ELMC_WCCProxy (available on the IRS server)
- MC3 kit (available on the IRS server)

The IRS kits are located in `C:\Program Files\HP\Installers\`

- SMH - IM Agent / PSP kit (SMH most actual version recommended)
- SNMP configured to send traps to the IRS server

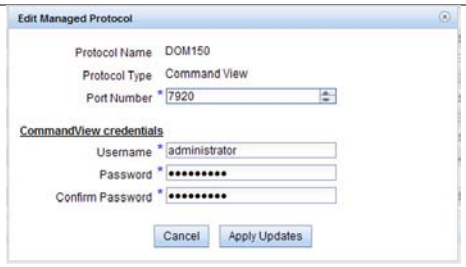
The service name of SMI-S CIMOM service for CV V8.xx and above is
"HP StorageWorks CIM Object Manager"

When a Command View server has to be upgraded from ISEE to IRS, all components have to be removed except:

- Command View EVA Version 7.01 or newer
- SMI-S EVA
- SMI-S CIMOM

7.3 ELMC_WCCProxy Command View Credentials

The modifications can be done on
https://<IRS Server>:7906/installwizard/managedentities.html



The Username and Password of ELMC-Command View must match with the CV-EVA one.

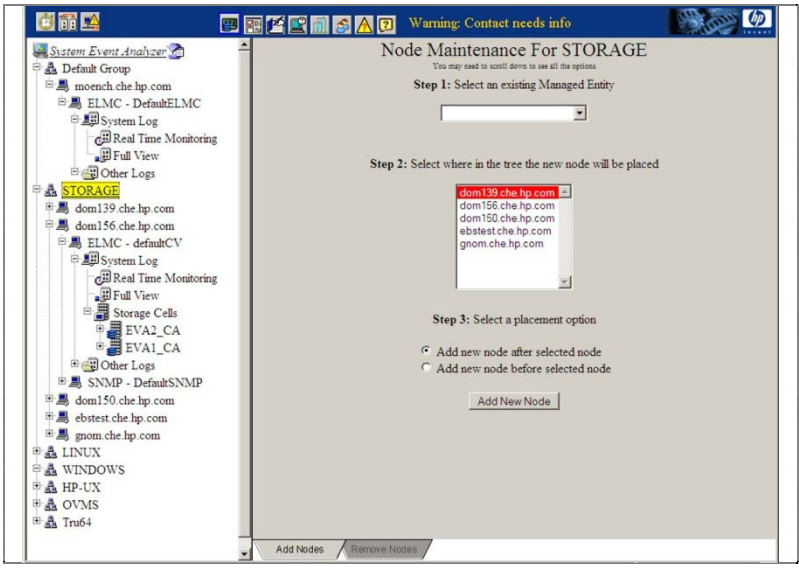
Example: configured for the SMS DOM150.

When different command views with different usernames and passwords are being used, you can make a set of ELMC-Command View protocols with different names.

7.4 Configuring EVAs into WEBES

These steps are also described in chapter 4.
The detailed description is available in the WEBES documentation.

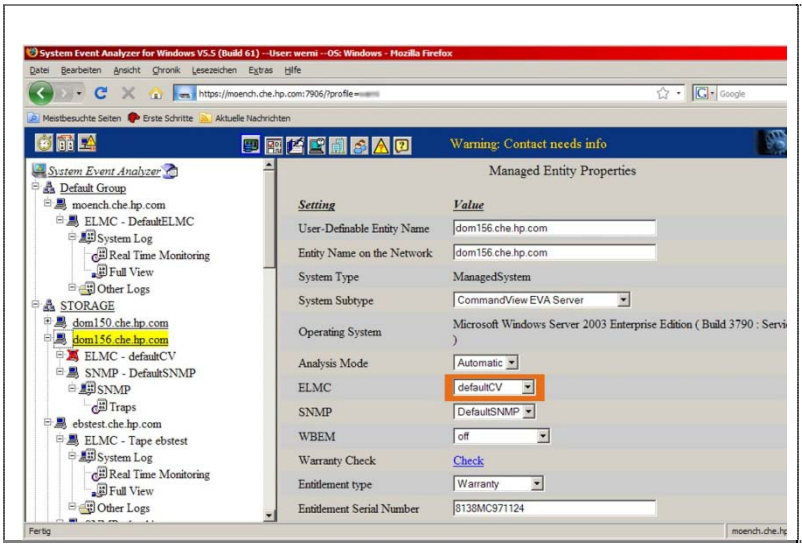
The following steps are necessary, that the service incidents and the configuration collection are being processed correctly.
Add the EVAs to the "System Event Analyser" list.



Create a group, like STORAGE

Add the SMS / SMA into the group STORAGE.

The active EVAs of the become automatically visible



If you see red crossed device protocol, this must be corrected, before the EVAs will become visible.

Solution:
Add / modify a "Command View EVA" protocol with the user of the Command View.
Select the corresponding configured ELMC protocol.

7.4.1 End to end test (test incident up to CV 9.2)

- `C:\ wccproxy test` on the Command View server (SMS)

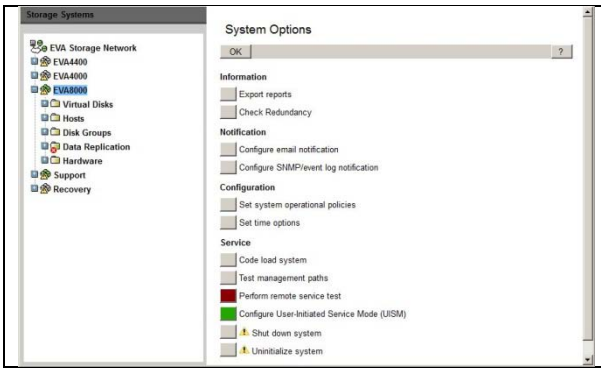
- `C:\ wsea test nosys` on the system where WEBES is installed
  Expected in WSEA: Incident with "ISEE Incident" number
  (the event date is Wed 2 Oct 2002)
- With WEBES 6.0 or newer the preferred method is to press the button "Test Event" in WEBES under "WEBES Notification Settings" , (click onto)
  (the event date is the date where you've submitted the service incident)

Enter Command View EVA
- Select a disk group and set the Occupancy alarm to 1%
  set it back to the previous value a moment later

Expected in WSEA: Incident without "ISEE Incident" number

7.4.2 Submit test incidents (CV 9.3 and newer)

If WEBES 6.1 and IRS A.05.50 or newer is installed, the following (red marked) options can also be used to submit a test incident.



- In command view select an active EVA.
- Then click on System Options.
- Now click on "Perform remote service test"

The test incidents you're raising now will be sent into the HP backend.

If the alarming has to be turned off for service purpose, this can be done by pressing onto (the green marked) button "Configure User-Initiated Service Mode (UISM)".

7.5 Command View EVA Log in Problems

The foreseen user must be participant of at least of one of the uses group

- HP Storage Admins
- HP Storage Users

You've still get the message

```
Insufficient privileges
```

Execute the following command on the server or management module on which you are installing HP Command View EVA:

```
C:\Program Files\Hewlett-Packard\XF\bin\win-32>XfAppMgr register
XFSecurity.cfg
```

The following response indicates that login is enabled:

```
Registered application roles and privileges using config file:
XFSecurity.cfg.
```

8 Tape Libraries

Some types of tape libraries are now supported.

The different libraries can be configured in a very similar way.

8.1 VLS - HP Storage Works Virtual Library Systems

NOTE: SNMP needs to be configured and enabled for the monitored device to be able to send events to the *Hosting Device.*

On the VLS side:
check for
- the correct SN can be found (examples)
for the VLS 6000 series
on the cover of the Virtual Library System

VLS 6600

VLS6800

-- for the VLS 9000 series
on the primary server (looks like a ProLiant server)

Has to be done in Command View TL:
- Select the VLS and add the SNMP credentials

- When the library has been configured into IRSS, you can submit a test trap (hpHttpMgOKHealthTrap, will not be sent to HP)

In IRSS:
could be done using the WESA user interface https://<IRS-server>:7906 or the managed entities interface https://<IRS-server>:7906/installwizard/managedentities.html
- Check if a SNMP protocol has been set with the community name, which has been set in Command View-TL
- The VLS can now be added/discovered using the IP address of the system on which CV-TL is running.

Add all necessary credentials (minimum expected information):

- System sub-type: Virtual Tape Library (VLS)
- Entitlement: select contract if you have on for this device, for example
- Serial Number: device's SN
- Product Number: device's PN
- Entitlement ID: if you've selected contract above, you can add here the corresponding SAID

8.2 Command View Server TL

Important: The CV TL version must match the firmware version used in the tape library.

9 P4000 – Left Hand Storage Device

9.1 Used Application Ports

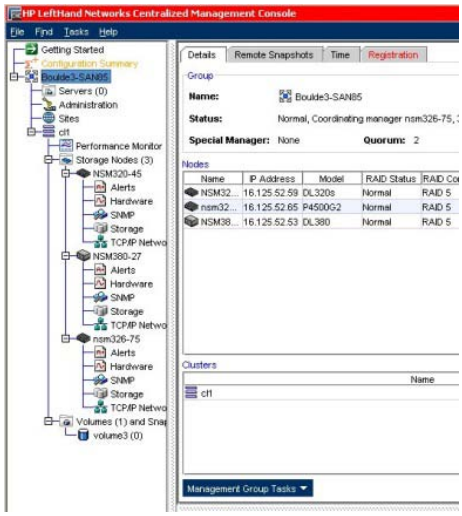
-	ICMP (ping)		IRSS -> MS	discover function by HP-SIM, UDN
-	SNMP	161	IRSS -> MS	communication to the P4000's and CMC
-	SNMP Trap	162	MS -> IRSS	service incidents

9.2 Requirements

- CMC 8.5 Software or newer. Available at www.hp.com/go/P4000downloads
  This software can be installed on the CMS or on a separate system
- P4000 firmware patch 10076
- IRS Advanced A.05.50 or newer
- The SNMP properties must match the ones of the system where CMC is running

Important: The "Health Check" support for P4000 will discontinue in 1H 2011.

9.3 Configuring the P4000 Storage Systems Communication



- All P4000 must be correctly configured in CMC
- Verify in CMC that SNMP is enabled for each storage system
- Verify that the used SNMP community name exists also in WEBES
- Verify that the SNMP traps oft CMS and the P4000 will be sent to the IRS server

9.4 Discover / add the P4000 into WEBES / IRS

- Discover the System, where CMC is installed on
- Discover the P4000
- Add the missing credentials and check whether they are visible in the Remote Support Eligible List

- The CMC software offers to send a test trap

10 SAN Switches

A number of SAN switches are supported now if WEBES V5.6 or newer is installed.
IRS can communicate with the SAN switches via SNMP protocol.

On the switch (refer to the switch's manual):

- Enable and configure the SNMP communication in the SAN switch.
- Enter the target IP address of the IRSS system
- If necessary/possible add the read / trap SNMP community name, which is being used in the customer's local network.
- If necessary, define the error levels, which should send incidents

In IRSS:
could be done using the WESA user interface https://<IRS-server>:7906 or the managed entities interface https://<IRS-server>:7906/installwizard/managedentities.html

- Check if a SNMP protocol has been set with the community name which has been set in switch
- The switch can now be added/discovered
- Add all necessary credentials (minimum expected information):
  - System sub-type: FC Switch (expected)
  - Entitlement: select contract if you have on for this device, for example
  - Serial Number: device's SN
  - Product Number: device's PN
  - Entitlement ID: if you've selected contract above, you can add here the corresponding SAID

Quick test:

- You may now submit a test SNMP trap, if it's possible to do it with this switch.

11 Linux Systems

The most actual PSP kits can be downloaded from http://www.hp.com/support
Some additional documentation is available on http://www.hp.com/go/proliantlinux

Important: RHEL 5.5 needs IRS A.05.60 or newer

11.1 Used Application Ports

- ICMP (ping)		IRSS	-> MD	discover the SMS, UDN
- SNMP port	161	IRSS	-> MD	communication to the Insight Agent
- SNMP port	162	MD	-> IRSS	SNMP traps

11.2 To be installed on the managed device (Red Hat)

Requirements that all SMH services will run:
- Sun Java runtime kit (V 1.6.xxx recommended)

Possible Requirements, to be installed:
- Packages: rpm-build, rpm-devel
- Unpack the PSP # gunzip psp-xxx.xxx.xx.tar.gz
  # tar -xvf psp-xxx.xxx.xx.tar

Start the installation
- PSP V8.40 and newer # ./hpsum

Note: Starting with Linux ProLiant Support Pack 8.40 and later, please ensure the following RPMs are also installed.
- For Red Hat Enterprise Linux 5 x86 servers: compat-libstdc++-296-2.96-132.7.2.i386 or later
- lm_sensors-2.8.7-2.i386 or later
- net-snmp-5.3.1-14.el5.i386 or later
- perl (needed to provide the libperl.so)
- libnl (needed for QLogic and Emulex drivers)

- PSP prior V8.40 go to # ./compaq/csp/linux
  # ./install815.sh example: PSP version 8.15)

Installing without GUI # ./install815.sh -NUI -y
select the packages, which you want to install

Refer also to the HP IRS Quick Start guide, for more information.

11.3 To be installed on the managed device (Suse Linux)

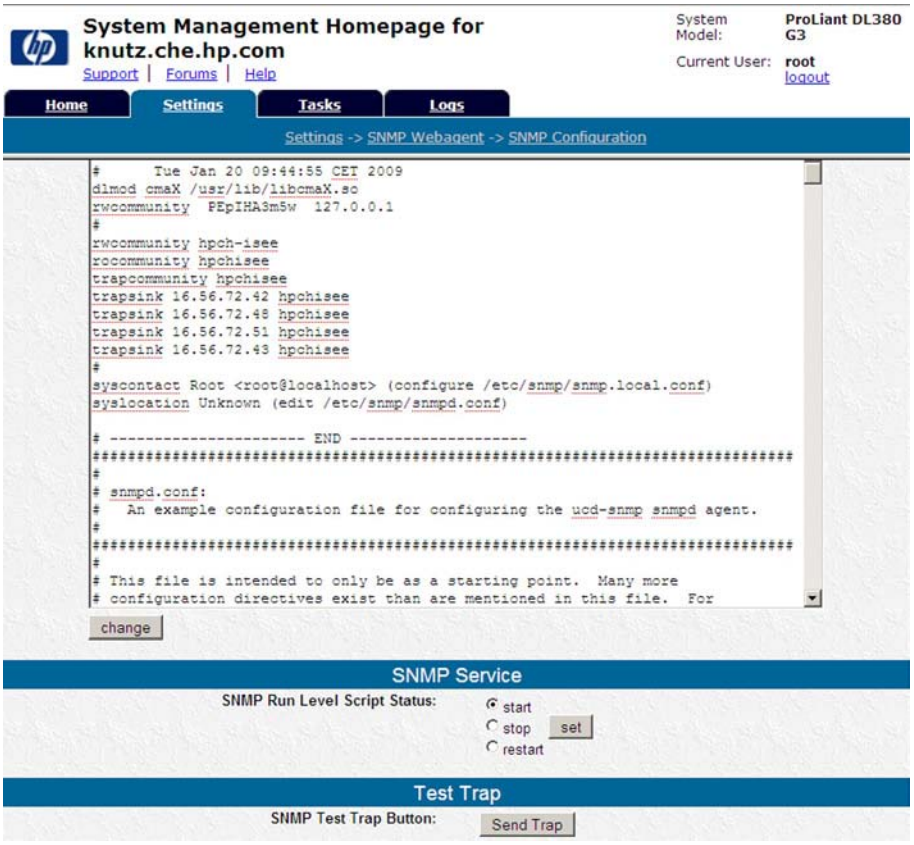
Requirements that all SMH services will run:
- Sun Java runtime kit (V 1.6.xxx recommended)
- The PSP kit is to be installed in the same way as for RedHat Linux.

11.4 To be configured in the SMH

- A specific SNMP name may be defined/added

- The target IP address must be added that the SNMP traps are being sent to the correct target instance(s)

In this example the system sends its SNMP traps to four different instances with the trap communication name “hpchisee”.



These setting can also be edited /modified directly in /etc/snmp/snmpd.conf.

11.5 PSP and snmp tips and tricks

man hp-snmp-agents help information about the insight agent

RedHat Linux:

- “panic” while booting the system after having installed/updated the PSP
  Get the system up again (also more time to fix the problem)
- write down the information of the “panic” reason
  try to start the system with a different kernel
  you may comment out the boot information of the faulty kernel in /boot/grub/grub.conf

SMH (completely) empty:

- **Important:** always check very carefully for the supported version of the PSP for that specific system.
- Try to restart the service hp-snmp-agents

```
# /etc/init.d/<service> status (start, stop, restart)
  - hp-snmp-agents
  - hpsmhd
  - snmpd
  - snmpdtrapd
```

- In extreme cases, try to install step by step the next older hp-snmp-agents-xxxxxxx.xxx package until information is there again.

SMH / PSP configuration files:
/opt/hp/hp-snmp-agents/cma.conf config the snmp behavior

Traps not being submitted:

- Check to have the packages net-snmp, net-snmp-utils, net-snmp-libs installed.

11.6 Citrix XEN Server - how to find HP Insight Agents

You can google with the expression

- "HP SNMP Agents for Citrix XenServer"
- "HP SNMP Agents for Citrix XenServer 5.6" (with version number)
- hp-agents-xs.iso

11.7 Important note to be read on the SMH

The server needs to have **'sudo'** installed in order to start or stop the snmp daemon and to send test traps. 'sudo' grants controlled root access to groups or users.
If installed after **hp-snmp-agents** please run a **'/sbin/hpsnmpconfig'**.
In case of VMware ESX 3.x series, please run **'/etc/init.d/hpasm reconfigure'** after installation of hpasm.
These buttons will NOT work if 'sudo' is configured to only run when the user is logged into a 'real' tty.
To be able to perform the operations of start, stop, restart of the snmpd daemon, the user must comment out the line **'Defaults requiretty'** in the **/etc/sudoers** file. See man sudoers for details about the 'requiretty' flag.
If present, this flag will need to be removed from the **'/etc/sudoers'** configuration file.
The 'send trap' button also requires a tool **snmptrap** to be present on the system. This tool is often bundled with the snmp stack (Suse) or in a package called 'net-snmp-util' (Red Hat).

12 ESXi

12.1 Used Application Ports

-	ICMP (ping)		IRSS -> ESXi	discover the ESXi host
-	TCP port	5989	IRSS -> ESXi	WBEM communication
-	TCP port	7906	ESXi -> IRSS	service incidents

12.2 Check for the HP Kit being installed

Important: The HP version of the ESXi kit is necessary.

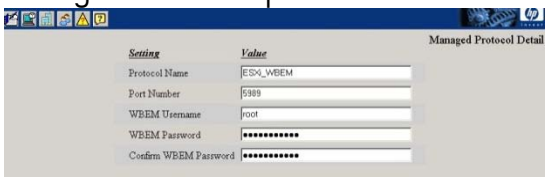
The manual HP VMware ESXi management environment integration note describes most of the necessary steps to add a ESXi device into HP-SIM.
Some of this information is also helpful to add an ESXi environment into IRSS.

Possible way to check that the correct kit has been installed (some proposals):

- ESXi 3.5 `# cd / , # cat oem.txt contains hp~`
- ESXi 4.0 #

12.3 Discovering / Adding the Device

1. Ask for / create the username and password to log in to ESXi (how to start see below)
2. Configure a WBEM protocol in WEBES and add the necessary credentials:



3. Add / discover the ESXi device.
4. Check for the following information in "Managed Entity Properties"
   - System Type: Managed System
   - System Subtype: ProLiant ESXi Server
   - Operating System: VMware ESXi 4.0.0 build-xxxxx
   - WBEM ESXi_WBEM (example name)

5. Add a new device group, ESXi for example, in System Event Analyzer
6. Add the device into this group.
   this tries also to force a WEBES/WBEM subscription in ESXi.

12.4 WEBES Subscription Test

You may see a java error, when you want to use this command.

Run on the CMS the following command
C:\> desta launchwhc 127.0.0.1 (or) <CMS_Node_Name>

12.5 Enter Command Line Mode and activate SSH access

1. At the console of the ESXi host, press **ALT-F1** to access the console window.
2. Enter **unsupported** in the console and then press Enter. You will not see the text you type in.
3. If you typed in unsupported correctly, you will see the Tech Support Mode warning and a password prompt. Enter the password for the root login.
4. You should then see the prompt of ~ #. Edit the file inetd.conf (enter the command **vi /etc/inetd.conf**).
5. Find the line that begins with #ssh and remove the #. Then save the file. If you're new to using vi, then move the cursor down to #ssh line and then press the **Insert** key. Move the cursor over one space and then hit backspace to delete the #. Then press **ESC** and type in **:wq** to save the file and exit vi. If you make a mistake, you can press the **ESC** key and then type it **:q!** to quit vi without saving the file.
6. Once you've closed the vi editor, run the command **/sbin/services.sh restart** to restart the management services. You'll now be able to connect to the ESXi host with a SSH client.

   ESXi 3.5 Update 2 or later the service.sh command no longer restarts the inetd process which enables SSH access. You can either restart your host or run **ps | grep inetd** to determine the process ID for the inetd process. The output of the command will be something like 1299 1299 busybox inetd, and the process ID is 1299. Then run **kill -HUP <process_id>** and you'll then be able to access the host via SSH.

12.6 SSH Access using OpenSSH with HP-SIM

On the CMS in command mode:
`C:\ ssh - l <login-name> segnes01.che.hp.com`

12.7 Submit Test Incident

Up to now: no "test event" command available
Try with pulling a disk or unplug a power cable, if possible, for example.

12.8 ESXi – Checking WBEM information

```
/etc/sfcb # cat sfcb.cfg
httpPort:                   5988
enableHttp:                 true
httpProcs:                  2
httpsPort:                  5989
enableHttps:                true
httpsProcs:                 4
```

```
provProcs:                  16
restrictHttpToLoopback:     true
doBasicAuth:                true
basicAuthLib:               sfcBasicAuthentication
useChunking:                true
keepaliveTimeout:           1
keepaliveMaxRequest:        10
sslKeyFilePath:             /etc/vmware/ssl/rui.key
sslCertificateFilePath:     /etc/vmware/ssl/rui.crt
sslClientTrustStore:        /etc/sfcb/client.pem
sslClientCertificate:       ignore
certificateAuthLib:         sfcCertificateAuthentication
registrationDir:            /var/lib/sfcb/registration
providerDirs:               /lib /lib/cmpi
enableInterOp:              true
```

Stuff of HP:
`/var/lib/sfcb/registration/repository/root/hpq`

12.9 Miscellaneous

List of HP supported OS

Check the ESXi version on the ESXi system
`#vmware -v`

`/var/lib/sfcb/registration/repository/root/hpq`
Commands working in ESXi:

- `# find / -name <filename>`
- `# fdisk -l`
-

13 HP-UX

IRSS A.05.40 performs also a basic configuration collection of HP-UX systems.

13.1 Used Application Ports

-	ICMP (ping)		IRSS -> MS	discover function by HP-SIM, UDN
-	HTTP port	2301	IRSS -> MS	start/enter SMH when it is in standby mode
-	HTTPS port	2381	IRSS -> MS	enter the SMH
-	WBEM	5989	IRSS -> MS	default WBEM CIMOM port
-	HTTPS	7906	MS -> IRSS	service incident to WEBES

13.2 Prerequisites check on HP-UX

Note: To check the prerequisites automatically on the HP-UX system, you can run the Installation Advisory tool `InsightRsHpuxPrereqCheckv24.sh` .
On the IRS system the advisory tools and a quick user guide are located in `…\HP\svctools\common\ca\html\installwizard\InstallationAdvisor` .
HP internally these tools are available on
http://intranet.hp.com/tsg/ww3/SDA/Pages/InstallationAdvisor.aspx

These items must exist and running (example for HP-UX 11.23). (For more details refer to the HP IRSA Managed Systems Guide).

Product	**Version min.**	**HP-UX Verification Command**
Supported HW model		**`model`**
Operating system		**`uname –a`** or **`osinfo`**
QPKBASE (recommended)	B.11.23.0712.070	
OS Patch Requirements	B.11.23.0409.3	
OpenSSL or HPUXBaseAux.openssl (OE)	A.00.09.07i.012	**`swlist –l product openssl`**
Online Diagnostic	B.11.23.10.05	**`swlist | grep –i OnlineDiag`**
WBEMServices	A.02.05.08	**`swlist | grep –i WBEM`** and **`swlist WBEMServices`**
System Fault Management	B.05.00.05	**`swlist SysFaultMgmt`** **`or`** **`swlist –l product SysFaultMgmt`**
Check that the cimserver is running	A.02.07	**`/opt/wbem/bin/cimserver -v`**
check for a working CIM provider and SFM ProviderModule -> OK		**`/opt/wbem/bin/cimprovider –ls`**
Additionally necessary for collection services		
HPUXBaseAux.SysMgmtBase	A.02.49	**`swlist SysMgmtBase`**

or SysMgmtBase.SysMgmtBase	→ SMH-UILIB → SMH-UILIB-COM	or **swlist –l product SysMgmtBase**
System Management Web (SMH)	A.2.2.7	**swlist SysMgmtWeb SysMgmtHomepage**
hpuxwsApache	A.2.0.49	**swlist hpuxwsApache** or **swlist –l product hpuxwsApache**

13.3 Add, Configure the HP-UX system to send service events

Add the HP-UX system into IRS as described above (IRS Admin Console).
Check / add / edit a UNIX-WBEM protocol (Username, Password to be checked).

Check if EMS is running

```
# /opt/sfm/bin/sfmconfig –w –q
```

Set hardware monitoring to SFM

```
# /opt/sfm/bin/sfmconfig –w –s
```

13.4 Creating WBEM Subscription using a non-privileged user

If there's a need to use an account with limited user rights, it could be created and tested as described below. Some commands depend on the HP-UX version.

- Create a user like:

```
#useradd -g users hpirs
#vipw   (to check the user in the database)
```

Add / modify the password of

```
# passwd hpirs      => <your-password>
```

- Add the read and write authorization for the new WBEM user to each of the following namespaces:

```
#cimauth -a -u hpirs -n root/cimv2 -R -W
#cimauth -a -u hpirs -n root/PG_InterOp -R -W
#cimauth -a -u hpirs -n root/PG_Internal -R -W
#cimauth -a -u hpirs -n root/cimv2/npar -R -W
#cimauth -a -u hpirs -n root/cimv2/vpar -R -W
```

- Verify the user's authorizations by:

```
# cimauth -l
     hpirs, root/cimv2, "rw"
     hpirs, root/PG_InterOp, "rw"
     hpirs, root/PG_Internal, "rw"
     hpirs, root/cimv2/npar, "rw"
     hpirs, root/cimv2/vpar, "rw"
```

Verify the settings in the CIM current configuration. Check for / set the bold marked value to true.

```
#cimconfig -l -c
     enableAuditLog=false
```

```
sslClientVerificationMode=optional
enableSubscriptionsForNonprivilegedUsers=true
shutdownTimeout=30
authorizedUserGroups=
enableRemotePrivilegedUserAccess=true
enableHttpsConnection=true
enableNamespaceAuthorization=true
enableHttpConnection=false
```

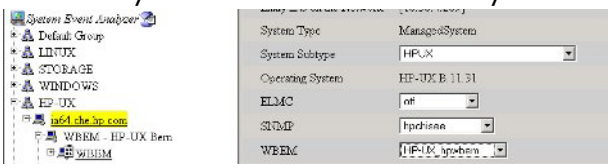
could be done by:

```
#cimconfig -s enableSubscriptionsForNonprivilegedUsers=true -p
#cimserver -s          (stop the cimserver)
#cimserver             (start the cimserver)
#cimconfig -l -c       (check the current settings)
```

13.4.1 Make and check the WBEM subscription

To be done in WEBES:

- Add (or modify) a "UNIX WBEM" protocol in Managed Protocol Details.
  Add / update this protocol with the user name and password, which should be used for the subscription
- Add the system to the Managed Entities list, if not already done, and select your protocol, if it's not done automatically.
- Check the connection to the HP-UX system by
  - add the system to the device list of "System Event Analyser" and check that display symbol of the WBEM protocol is not red crossed.
  (to do a recheck immediately, the device can be removed and add again.)



- On the HP-UX system the WEBES subscription should look like:

```
# evweb subscribe -L -b external|grep -i -e webes

HPWEBES_<irsserver>_1_Filter_HP_AlertIndication
HPWEBES_<irsserver>_1_Handler_HP_AlertIndication
select * from HP_AlertIndication          UNKNOWN
```

Remark: <irsserver> is expected to be the full qualified node name of the IRS server.

13.4.2 Send a test event

```
# /opt/sfm/bin/sfmconfig –t –a
```

or by

```
# /opt/resmon/bin/send_test_event disk_em
```

or by

```
# /etc/opt/resmon/lbin/send_test_event fpl_em
# /etc/opt/resmon/lbin/send_test_event ia64_corehw
```

On the HP-UX system the event number 103 should be displayed in

```
/var/opt/resmon/log/event.log
```

13.5 Successfully configured but no Service Incidents in WEBES

Some suggestions how to troubleshoot the problem.

- Possible DNS problems; proposal to check:

```
# telnet 16.56.72.42 7906
Trying...
Connected to . <IP address of IRS Server>
Escape character is '^]'.

# telnet moench.che.hp.com 7906
Moench.che.hp.com: Unknown host
```

Add the node name into hosts (WEBES subscription contains node names).
Example entry:

```
#
# -IRS servers
16.56.72.42   moench   moench.che.hp.com  # IRS Standard
```

- If the result is like

```
# telnet <IRS Server> 7906
Trying...
telnet: Unable to connect to remote host: Connection timed out
#
```

there is no access to WEBES on the IRS server.
Open the access from the HP-UX system to the IRS server.

Further you can check:

Issue:
Syslog reports error "PGS00410: LOCATOR IS NOT VALID: <host>:7906"Solution
Root cause*: Customer is using DNS for host name resolution. The /etc/resolv.conf file does not have the read permission for the <wbem user> user, where the cimservermain is run from the user <wbem user>.*

Add also the read rights for the other user groups for

```
# chmod 644 /etc/resolv.conf
```

And if necessary

```
# chmod 644 /etc/hosts
```

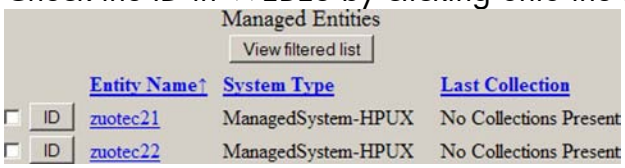
Check the rights with the command

```
# ls -ll
```

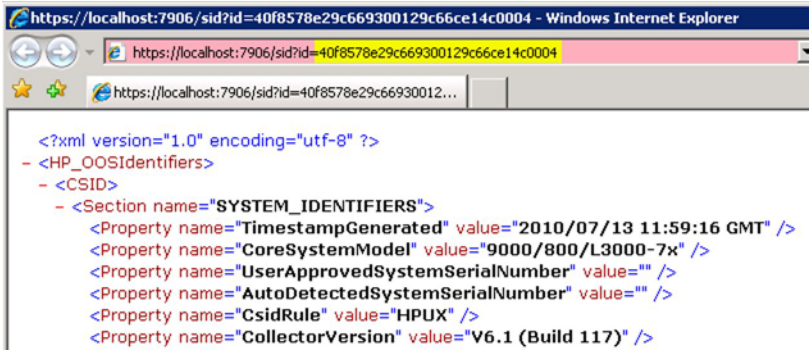
13.5.1 HP-UX Indications are not reaching WEBES – System Identifier (ID)

Important: Only one WEBES subscription with a corresponding WEBES System Identifier which points to one specific IRS/WEBES server is permitted to exist in the HP-UX. All other WEBES identifiers must be deleted.
Important: When a WEBES upgrade has been made without using the WEBESBackup of the previous version, this check/clean up must to be done.

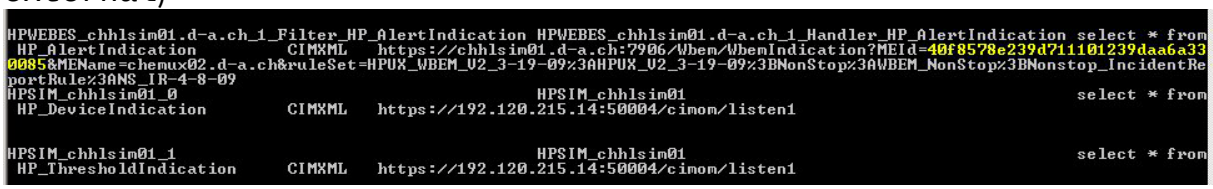
1. Check the ID in WEBES by clicking onto the ID button



Get the ID (yellow marked)



2. Check the ID on the HP-UX system (command `# evweb subscribe -L -b external`)



   This (yellow marked) number Must match with the above one.

3. Delete the WEBES subscription in HP-UX. How to, see the chapter below.
4. Delete the system in WEBES
5. Restart the DESTA_Service
6. Check for the existence of the system; if not add it in WEBES
7. To force a subscription, add the device into the "System Event Analyser" list
8. Compare the ID in WEBES with the subscription and its ID on the HP-UX system
9. If the IDs match, submit a test event

Recommendation: Step 8. And 9. may be repeated a day or two later.

13.5.2 HP WBEM Services for HP-UX - How to Delete External Subscriptions

Issue:

During the configuration of Remote Support Pack (RSP), WBEM subscriptions were created on the HP Systems Insight Manager (SIM) Central Management Server (CMS).
RSP is being configured on a different CMS now. The original CMS server is no longer available. The subscriptions are still listed on the HP-UX managed nodes. The evweb command does not allow to delete them:

```
# evweb subscribe -D -n HPSIM_cms_0
Are you sure you want to delete the subscription (y/n)? [n]:y
Deletion of external subscriptions is not supported.
```

How can the subscriptions be removed?

Solution:

The System Fault Manager (SFM) **evweb** command does not allow to remove external subscriptions created on a CMS.

WBEM version A.02.07.02 (March 2008) and later added the **cimsub** command:

"Indication Subscription Management (cimsub) - Provides a command line interface to manage CIM indication subscriptions on the local CIM Server. Refer to the man page for more information. The new command would support enabling, disabling, or removing a subscription, display of selected subscription information, as well as removal and display of filters and handlers."

Use **cimsub** to list the subscriptions. Look for an entry with the hostname of the original CMS:

```
# cimsub -ls
root/cimv2      root/cimv2:WEBES_cms_Filter_HP_Alertindication
root/ccimv2:CIM_IndicationHandlerCIMXML.WEBES_cms           Enabled
# cimsub -lf
root/cimv2:WEBES_cms_Filter_HP_Alertindication
"select * from HP_Alertindication"
# cimsub -lh
root/cimv2:CIM_IndicationHandlerCIMXML.HPWEBES_cms
https://ip:7906/Wbem/WbemIndication...
```

The name space is always **root/cimv2** . The second entry listed by **cimsub -ls** is the filter. Use this value for the **-F** option.

The first entry listed by **cimsub -lh** is the handler. Use this value for the **-H** option.

Then remove the subscription.

Example:

```
# cimsub -ra -n root/cimv2
   -F root/cimv2:WEBES_cms_Filter_HP_AlertIndication
   -H root/cimv2:CIM_IndicationHandlerCIMXML.HPWEBES_cms_Handler..
```

Repeat for all subscriptions for the original CMS. Then verify with **cimsub** and **evweb** that the subscriptions were removed:

```
# cimsub -ls
# cimsub -lf
# cimsub -lh
# evweb subscribe -L -b external
```

Note: If you have an older version of WBEM, it is recommended to update WBEM. Earlier WBEM versions do not allow removing subscriptions.

14 OpenVMS

14.1 Used application ports

- ICMP (ping) IRSS -> MD discover the device, UDN
- TCP port 7920 MD <-> IRSS ELMC_WCCproxy communication

14.2 To be verified, whether OpenVMS systems are supported.

Important: The ELMC_WCCProxy kit must be version 2.5 or higher

Supported: OpenVMS Alpha V7.3-2 and newer
OpenVMS Itanium V8.2-2 and newer

Recommended: Install ELMC_WCCProxy V6.1 on OpenVMS 8.3 and newer

14.3 Installation of ELMC_WCCProxy

Copy the ELMC-WCCproxy kit from the CMS onto the OpenVMS System:

```
ftp> bin
ftp> put ELMC_WCCproxy_V6x_xxxx_xxxxx_OVMSAlp.EXE
```

On the OpenVMS system (example OpenVMS Alpha) unpack the kit by

```
$ run ELMCV61BL1KIT1_JUN-29-2010_OVMSAlp.EXE
```

Install the kit using the command

```
$ @WCCPROXY_INSTALL INSTALL
```

or if you want to decide the installation location yourself (example)

```
$ @WCCPROXY_INSTALL.COM install masterwebes SYS$DISK:[ELMC]
```

Check for the installed product and version

```
$ prod show prod WCCPROXY     or by
$ WCCPROXY VERSION
```

Check if WCCproxy is being started in SYSMAN (will be automatically started a boot time)

```
$ mc sysman start show file WCC*
```

It could also be started in SYSTARTUP_VMS.COM by adding

```
$ @SYS$STARTUP:WCCPROXY$STARTUP.COM
```

In a cluster environment, where the systems use the same system disk, move this file to

```
SYS$COMMON:[SYS$STARTUP]
```

Check if WCCproxy is running:

```
$ SHOW SYSTEM/PROC=WCC*   or by
$ WCCPROXY STATUS
$ WCCPROXY VERSION
```

14.3.1 Configure the system into WEBES

Enter WSEA by `http://<irs-server>:7906` and go to Managed Entities.
Add the OpenVMS system.
Add all missing Credentials, (minimum required):

- System Subtype = ALPHA or IA64
- The Serial – and Product Number

14.4 Submit Test Incidents

Preparation:

- Download the ELMC-Test kit from the public WEBES page
- Create a directory on the VMS system, where the files have to be placed
  Example: `create/dir DSA100:[ELMC_TEST]`
- Copy the ELMC-Test kit onto the VMS system, unpack it (it can be unzipped before)
- Check the location of the file `ERRLOG.SYS` (default location: `SYS$ERRORLOG`)
- Modify the data path for `test_event.bin` in the file `test_event.cfg` accordingly:
  Example:

```
DSA100:[ELMC_TEST]test_event.bin
   all at 0.1 bin
```

Recommended:

- create a procedure like `ELMC-WCCPROXY_TEST.COM` with the commands.
  Example:

```
$!-------------------------------------------------------------
$! set the symbol MBX
$! submit test event using WCCProxy
$!-------------------------------------------------------------
$ MBX :== "$DSA100:[ELMC_TEST]ALP_MBX_DRIVER.EXE"
$!
$! - to show the help text type MBX
$! MBX
$!
$! - run the test event
$ MBX test_event.cfg SYS$ERRORLOG:ERRLOG.SYS
$!
```

Run now this procedure to submit test cases

```
$ @ELMC-WCCPROXY_TEST.COM
```

15 Tru64

15.1 Used application ports

- ICMP (ping) IRSS -> MD discover the device, UDN
- TCP port 7920 MD <-> IRSS ELMC_WCCproxy communication

15.2 Installation of the ELMC kit (WCCProxy)

Preparation and installation

- Check for the existence of error log file by
  `# ls -l /var/adm/binary.errlog`
- Operating Systems 4.0F, 4.0G, 5.1A or higher
- Check for sufficient disk space , 61MB minimum
  `# df –h /usr/opt`
- Copy ELMC from the CMS to the Tru64 system and install it by
  `# gunzip ELMC_WCCProxy_<version>KIT1_<date-year>_Tru64UNIX.tar.gz`
  `# tar –xvf ELMC_WCCProxy_<version>KIT1_<date-year>_Tru64UNIX.tar`
  `# setld –l kit`

Select the WCCProxy kit to install
Enter "Yes"

```
# wccproxy status    <-- ELMC should be running
```

The Tru64 system can now be configured in HP-SIM
- Select "Options" – "Discovery" – "Manual" (if the node is not visible yet)
- complete all system profile credentials in "Edit System Properties"
- run "Options" – "Identify Systems"

15.3 Create Test Incident

Preparation:

- Download the ELMC-Test kit from the public WEBES page (Webes V5.5)
- Create a directory on the VMS system, where the files have to be placed
  Example: `mkdir /usr/users/chwerner/ELMC_TEST`
- Copy the kit into this location and unpack it with the command
  `# tar –xvf tru64_elmc_test_files.tar`
- Enter the new subdirectory
- Modify the data path for `test_event.bin` in the file `test_event.cfg` accordingly:
- Example:
  `/usr/users/chwerner/ELMC_TEST/MBX_DRIVER_FILES/test_event.bin`
  `all at 0.1 bin`

Run now this procedure to submit test cases

```
# ./mbx_driver test_event.cfg /var/adm/binary.errlog trace
```

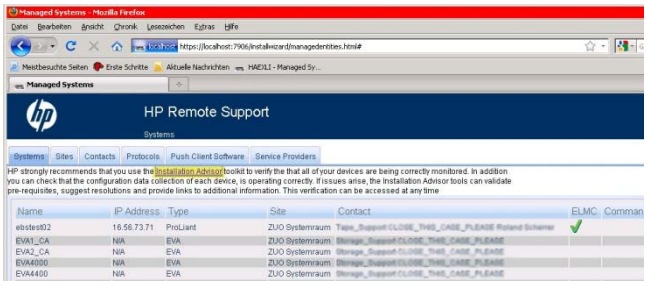
16 RSCC – Remote Support Configuration Collection

IRSS runs configuration collections of supported managed devices on monthly base based on built in rules. This is not always working. It may also helpful to run a collection immediately. Beginning with IRS A.05.40 it is possible to force configuration collections immediately.

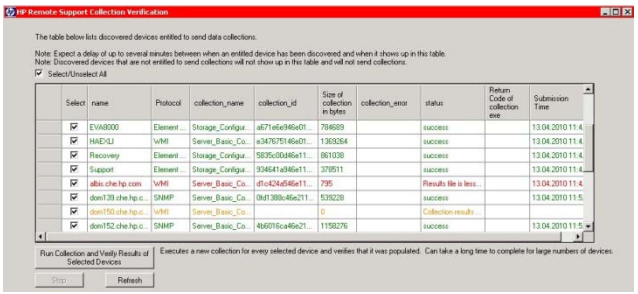
The collections are being stored in
`C:\Program Files\HP\UnifiedCollector\data\ucresults`

16.1 Managed Device Configuration Collection test with Installation Advisor

Information about this tool is available on
https://localhost:7906/Installwizard/managedentities.html



The collector can also be started directly by running
`InsightRsDataCollectionCheck.exe` which is located in
`C:\Program Files\HP\svctools\common\ca\html\installwizard\InstallationAdvisor`



Select a single, multiple devices, etc. and start the collector. The collections are located in
`C:\Program Files\HP\UnifiedCollector\data\ucresults`

If a collection has been successfully submitted to HP can be verified in
`C:\Program Files\HP\RemoteSupport\logs\submitProxiedData.log`

16.2 Helpful Commands

Check the configuration collectors start date and time:
`C:\ ucadmin getschedule -all`

If `InsightRsDataCollectionCheck.exe` does not show the EVAs which are listed in Managed Entities, the collection may be forced with the following tool:

- Enter the location of the batch file by `cd %UC_HOME%\bin`
- Add the Weekly-IBI-EVA-Schedule by `uc_ibi_eap_sched.bat –install`
- Check the new settings by `uc_ibi_eap_sched.bat –list`

- The "weekly" collection should be set back to "monthly" when the collector has started to work as expected by `uc_ibi_eap_sched.bat –remove`

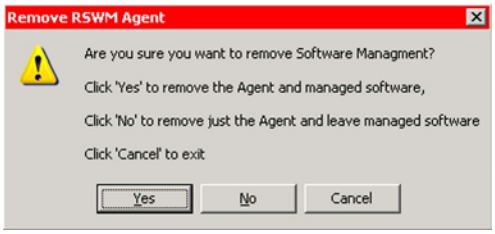
Important: This procedure is basically foreseen for the Early Acceptance Program. It could happen, that this batch file will be removed from the productive IRS kit without notice.

17 Uninstalling IRS

17.1 Steps to remove IRS

1. Uninstall all packages in RSSWM

2. Uninstall RSSWM by
   "Start" > "Programs" > "Hewlett-Packard" > "Remote Support Software Manager" >
   "Uninstall Remote Support Software Manager"



   Select:
   YES to remove (uninstall) all IRSS components (including WEBES)
   NO to remove RSSWM only.
   IRSS itself remains running. No automatic updates of IRS components possible.
   → then ignore the following steps.

3. Check in "Start > "Settings" > "Control Panel"
   - for Windows 2008 "Program and Features"
   - for Windows 2003 "Add or Remove Programs"
   if WEBES 5.5 was installed, that only Microsoft SQL Server 2005 remains installed, if a reinstallation is being foreseen with this WEBES version.
   if WEBES 5.6 was installed, that only PostgreSQL 8.3.x remains installed, if a reinstallation is being foreseen with this WEBES version.
   if WEBES 6.x was installed, no database product is visible

4. Delete in C:\Program Files
   - WCCProxyLog with its contents
   - WebesLog with its contents

5. You may delete the content of C:\WebesBackup

6. You may delete the content of C:\Program Files\HP

18 Appendix A Locations and Log Files IRS

18.1 Collecting a full set of Log Files for Trouble Shooting

When you may gather the whole collection of the IRS log files for some reasons, run **`collectRSLogs.bat`** which is located in
`C:\Program Files\HP\svctools\common\ca\html\installwizard\InstallationAdvisor`

The files will be stored in a ZIP file, as shown in the example.

```
Summary
=======
Currently Installed ISEE Version is  A.05.40.17
OSEM IS NOT Installed on this Managed system
Currently Installed WEBES Version is  5.6
HPCC for EVA IS NOT Installed on this Managed system

The WCCProxy Service is     Running
The DESTA    Service is     Running
The HP ISEE  Service is NOT Running

IMPORTANT
=========
PLEASE transfer the ALBIS_Tools_chk.zip
collected by this utility to HP via
Email or other suitable mechanism.

The ALBIS_Tools_chk.zip file
has been left in the C:\temp\Tools_Check folder.
```

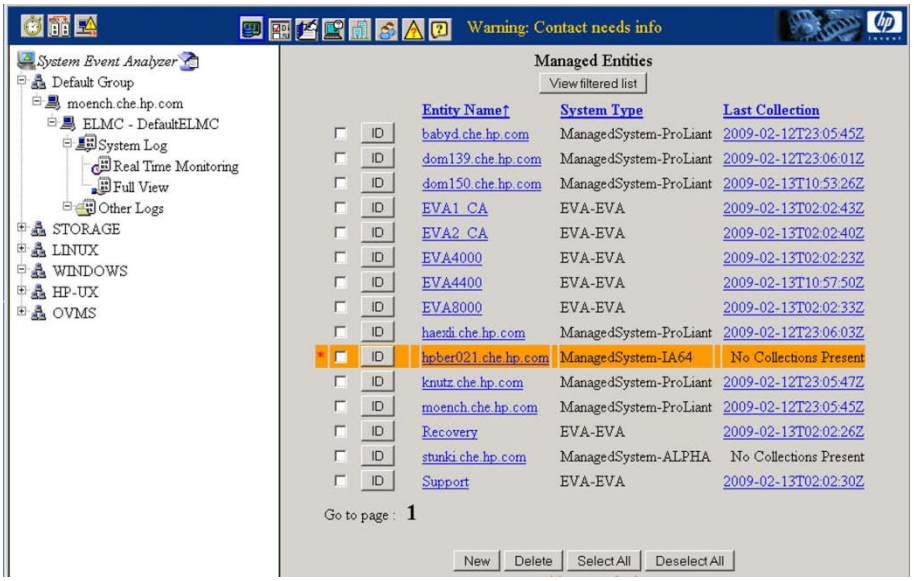
18.2 Location of Incidents and Collections

Successfully submitted incident are being stored in :
`C:\ Program Files\HP\RemoteSupport\data`
Collections can be found in:
`C:\ Program Files\HP\UnifiedCollector\data\ucresults`

Here the directories contain (<incident-number>

- Metadata<incident-number>.xml
  - actual incident status
- <incident-number>.zip
  - incident description

In WEBES itself, there is only the last collection or attempt of a collection accessible by clicking onto the collections date.



To review older collections, you have to go through the incident list in %\UnifiedCollector\data\ucresults

18.3 RSSWM Installation Log Files

- Windows 2003:

```
C:\Documents and Settings\<user who installed it>\Application
Data\hp\rsp\5.50.200.0\ RSSWM_Installxxx.log
```

- Windows 2008:

```
C:\Users\<user who installed it>\AppData\Roaming\hp\rsp
\5.50.200.0\ RSSWM_Installxxx.log
```

The number reflects also the IRSS version. If there are more than one of such directory, check the creation date of the log files to ensure that you get the correct ones.
Important: some of these directories may be hidden.

18.4 Remote Communication to HP

C:\Program Files\HP\RemoteSupport\logs

- submitProxiedIncident.log
  problem and test incidents, which have been sent successfully to HP or if they have failed.
  The remote incident number is always being shown when the incident has been successfully sent to HP.
- submitProxiedData.log
  configuration collections, etc.
- iseeclient.log
  the whole remote communication with HP.

- C:\Program Files\HP\RemoteSupport\data
  The detailed information of the incidents are located here in XML format.
  The incident state from « submitted » to « closed » can also be reviewed here.

"Undelivered: ISEE;"

- C:\Program Files\HP\RemoteSupport\logs	iseeclient.log
- C : \Program Files\HP\svctools\specific\wccproxy\logs	WCC_MC3.log WCC_SNMPTrapHandler.log
- C:\ Program Files\HP\svctools\specific\Webes\logs	WEBES.xx.log

18.5 Local communication with the managed devices

C:\Program Files\HP\UnifiedCollector\log

- uc.log
  was the collection successful ?
- IBI_WMI_Server_Collection.log
  WMI-WBEM communication
-

18.6 WEBES

The most important log files are named here

C:\Program Files\HP\svctools\specific\Webes\logs

- Director_out.txt

C:\Program Files\HP\svctools\specific\desta\logs\

- HealthCheck.log
  In case there are no hints been found in this log file about E2E failing targets, this test can be disabled with the command `C:\DESTA WHC E2E OFF`.

18.7 Helpful URLs

Public accessible

- Kits to be found by its SPxxxx description
  ftp://ftp.compaq.com/pub/softpaq/
- WEBES, OSEM, ELMC documentation and kits
  http://www.hp.com/services/webes
- IRS Standard kit to download
  https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=RSSTANDARD

- Download PSP kits for Windows and Linux
  http://h18013.www1.hp.com/products/servers/management/psp/index.html

- HP Technical Forum and much more
  http://www.itrc.hp.com

- HP-SIM Information
  http://www.hp.com/go/hpsim
  HP Insight Foundation
  http://h18013.www1.hp.com/products/servers/management/core-management-100.html

- eSMG
  https://www.hp.com/go/esmg
-

HP internal:

HP Data Center Servers

- AMC
  https://isee-amc.austin.hp.com/console
- Storage Environmental Portal
  http://customer.storage.hp.com/data/DoDHome.aspx
- eSMG
  http://esmg.sdc.hp.com
-

19 Appendix B WEBES Tips

19.1 Export / Import Managed Entities and User Profiles

Export:

If you want to make a scratch installation of a WEBES or IRS server, you can export all information of WEBES, except the incidents, performing the following steps

- Enter WEBES/WSEA with the user "user-adv"
- Click onto the button of managed Entities

- On the bottom of this page you can now press the button "Export"
- The exported data will be put into the following files
  `C:\Program Files\HP\svctools\specific\desta\data\managedentities\`
  - `ManagedSites.xml`
  - `ManagedContacts.xml`
  - `ManagedProtocols.xml`
  - `ManagedSites.xml`
  - `RSC.xml (if it's an IRSS installation)`

- This information you can use to quickly set up an empty WEBES installation.

Import:

Check if the directory tree
`C:\Program Files\HP\svctools\specific\desta\data\managedentities\`
exists. If not complete it.
Copy the exported `*.xml` files into that location.
By pressing the import button these data will be imported into WEBES.

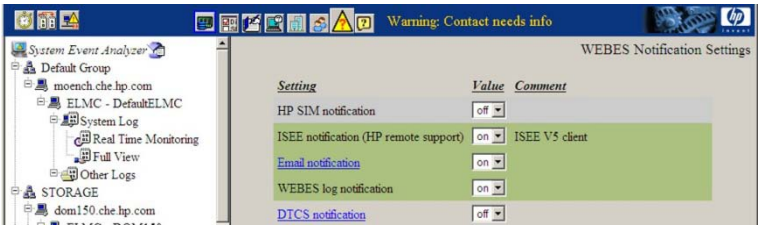
19.2 After reboot WEBES does not run anymore

- Check for the existing services WCCproxy and DESTA_service.
- Check that WCCproxy is running
- Try to start the service DESTA_service

- If it fails, you can try the following
- Register the DESTA_Service again using the command:
  `"C:\Program Files\HP\svctools\common\share\DESTAService.exe" -i -JVMProcess yes -RunPriority Normal -FF 1000`

- Try to start the DESTA_Service again.

19.3 End to End (E2E) error



1. In WEBES V5.5 turn the "WEBES log notification" on. (per default always on)
2. Check for and enable the service if necessary

```
C:>desta whc status
whc end to end testing: Enabled
whc smtp notification: Enabled
whc logging: Enabled

C:>desta whc log on
```

If the messages are still be sent, until the problem has been found, turn off the end to end check by the command

```
C:\> desta whc e2e off
```

Possible further reasons:

- WEBES itself is not running, because of an application crash
- WEBES itself is not running, because the database remains down
- WEBES has been stopped by a user
- The system on which WEBES is running is slow (long E2E response time)

19.4 Log Files where to find information about the E2E problem

```
C:\Program Files\HP\svctools\specific
       \WEBES\logs\   WEBES.x.log
       \desta\logs\   HealthCheck.log
       \ca\logs\      prob.log
```

19.5 Scheduled Task / Task Scheduler for health check of WEBES

With the WEBES installation 3 scheduled jobs are being configured too, which are checking the state of WEBES running the following command:

- AT1 (cmd/c "C:\PROGRA~1\HP\svctools\common\bin\desta.bat launchwhc")
- AT2 (cmd/c "C:\PROGRA~1\HP\svctools\common\bin\desta.bat launchwhc")
- AT3 (cmd/c "C:\PROGRA~1\HP\svctools\common\bin\desta.bat launchwhc")

The numbers of the jobs **AT** may differ on the different systems.

- These services can be found in Windows 2003 under
  „Start" – "Programs" – "Settings" – "Control Panel" – "Scheduled Tasks"

- These service can be found in Windows 2008 under
  "Start" – "Programs" – "Administrative Tools" – "Task Scheduler"

These jobs may also remain, if WEBES has been uninstalled.
These or some of these jobs may be removed when they're causing regularly E2E error messages.

19.6 Moving HP symbol on the screen.

Starting the WEBES user interface
(https://<webes-server>:7906)

The Logon box is expected to appear quiet quickly.

In most cases WEBES does not have access to its database.

WEBES V6.x has Postgre SQL V8.4x or newer integrated in its kit. It is running as a sub service of WEBES.

- If WEBES is running a lot of postgres.exe processes must also exist.
- Port 7950 must be open on the system for the communication between WEBES and PostgreSQL

WEBES V5.6x uses Postgre SQL V8.3 database software.

- If WEBES is running a lot of postgres.exe processes must also exist.
- Port 7950 must be open on the system for the communication between WEBES and PostgreSQL

20 Appendix C WEBES DB in Postgre SQL Server

WEBES V5.6 and newer use Postgre SQL database software.

20.1 Used application ports

- TCP port 7950 IRSS <-> IRSS communication between WEBES and Postgre SQL

20.2 WEBES 6.x with (integrated) PostgreSQL 8.4.x

PostgreSQL is now integrated in WEBES. Location of the installed database software
`C:\Program Files\HP\svctools\common\database\<application>`
`C:\Program Files\HP\svctools\specific\desta\database\data`

- There is no visible PostgreSQL service.
- There is no installed PostgreSQL software visible in "Add / Remove Programs"

Please refer to the most actual "WEBES Installation, Configuration and Usage Guide".

Additionally you see the product psqlODCB (is the official PostgreSQL ODBC Driver) which located in `C:\Program Files\psqlODBC`

20.2.1 Upgrade from WEBES 5.6 to 6.x

The PostgreSQL installation of WEBES 5.6 is not being used anymore by WEBES 6.xx.
During the upgrade the service postgres will be stoped and disable.
After successfully upgraded to V6.xx you can:

- uninstall PostgreSQL 8.3.x in "Add / remove Programs", if WEBES 5.6 was installed
- delete the user postgres (this one is not necessary anymore)

20.2.2 Upgrade from WEBES 5.5 to 6.x

Microsoft SQL 2005 Express is not necessary anymore for WEBES.
After successfully upgraded to V6.xx:

- stop and disable the MSSQL service "WEBESDB", if WEBES 5.5 has been installed. If MSSQL 2005 can be uninstalled depends also on other tools which use this database software.

20.3 WEBES 5.6 with PostgreSQL 8.3.x

Location of the installed database software
`C:\Program Files\PostgreSQL`

If the database installation fails with the WEBES installation follow the following description `C:\Program Files\HP\Installers\WEBES\PostgreSQL.htm`.

20.3.1 Service must be started

Service Name	Status	Startup Type	Log On As
PostgreSQL Server 8.x	Started	Automatic	.\postgres

If the database installation fails with the WEBES installation follow the following description C:\Program Files\HP\Installers\WEBES\PostgreSQL.htm.

20.3.2 Possible Problems

PostgreSQL startup problems:

- Startup of PostgreSQL end with error 193 - Message in system log:
  The postgresql-8.3 service failed to start due to the following error:
  postgresql-8.3 is not a valid Win32 application.
  -> reinstallation of PostgreSQL necessary
  (probably PostgreSQL 8.4 has to be installed instead)

WEBES UI shows a circling HP symbol (https://<irs-server>:7906):

- PostgreSQL-8.x service running but no database created:
  the databases are located in c:\Program files\PostgreSQL\8.x\data\base
  (7 directories expected here)
  -> create the databases as described below
- Databases for WEBES exist, but still circling HP symbol:
  select "Properties" by right clicking onto the service PostgreSQL-8.x
  enter in LogOn the password Webe$rules8552

20.3.3 Manual Installation

PostgreSQL 8.3 or 8.4 may be downloaded for free from http://www.enterprisedb.com/products/pgdownload.do#windows . You should get a file called something like PostgreSQL-8.3.7-2-windows.exe. PostgreSQL needs to use SuperPassword as "Webe$rules8552" and port as 7950 for the functioning of WEBES.
Also, the 5.6 version of Webes includes the PostgreSQL 8.3 version. - It is located in: C:\Program Files\HP\Installers\WEBES\ postgresql.exe.

PostgreSQL can be installed from the command prompt by executing the following command:

```
postgresql.exe --mode unattended --superpassword Webe$rules8552
--serverport 7950
```

To verify that the installation was successful, check the **postgresql-8.x** service is running or not. The service should be running after the installation.

Create the Webes Role and Databases

If the PostgresSQL 8.x has successfully been installed, you can now create the Webes Role and Webes databases. Start psql by "Start – Programs – PostgreSQL 8.4 – SQL Shell (psql)".

```
Server [localhost]:  <return>
Database [postgres]:  <return>
Port [7950]:  <return>
Username  [postgres]:  <return>
Password for user postgres:  Webe$rules8552
```

Now execute the following commands:

```
CREATE ROLE "WEBES" WITH SUPERUSER LOGIN PASSWORD 'Webe$rules8552' CREATEDB;
CREATE DATABASE destadb WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE ed WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE me WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE wbemdb WITH OWNER = "WEBES" ENCODING = 'UTF8';
```

Verify no errors occur. If the above commands succeed, the desta service can now be started.

Recreating the Webes Databases

If the Webes databases are missing or have become corrupt, it may be necessary to drop and re-create them..

Before executing the drop commands, verify that the Desta Service is not running.

Executing the "drop" command will physically delete the database files.

Start psql by "Start – Programs – PostgreSQL 8.4 – SQL Shell (psql)", then execute

```
DROP DATABASE IF EXISTS destadb;
DROP DATABASE IF EXISTS ed;
DROP DATABASE IF EXISTS me;
DROP DATABASE IF EXISTS wbemdb;
```

If the above commands run without error, then you may safely re-create the databases:

```
CREATE DATABASE destadb WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE ed WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE me WITH OWNER = "WEBES" ENCODING = 'UTF8';
CREATE DATABASE wbemdb WITH OWNER = "WEBES" ENCODING = 'UTF8';
```

If errors occur during execution of any of the above commands, then removing and re-installing PostgreSQL may be the preferred option. See below.

Removing PostgreSQL

The best way to remove PostgreSQL is through "add/remove programs". The command line method has been proven to be problematic.

A dialogue is displayed, which allows the user to follow the UI instructions. After the uninstallation you have to manually delete the PostgreSQL folder from Program Files folder.

Delete the user postgres in "Computer Management".

20.3.4 Additional necessary configuration steps

Important: The page "RSC Settings" remains empty until the system, where this IRS has been installed on, is listed up on the left side under "System Event Analyzer" – "Default Group".

If you've successfully entered WEBES by https://<irs-server>:7906, check/do the following steps:

- add the system under "Managed Entities". (press Apply Changes)
- add all necessary profile information (press Apply Changes)
- add it in SEA to the "Default Group" by clicking on Default Group

Now you can continue by configuring the access to the Content server.

21 Appendix F RSSWM

Must be installed and running
- .NET Framework 2.0 functionality

RSSWM components (HPCA Application) :
- RADIA for the remote transport
- HP Client Automation Application Self-Service Manager

21.1 Services used by RSSWM

Visible services for RSSWM A.05.50.200 an newer
- HP RSSWM Unattended Install Facility
- HPCA MSI Redirector
- HPCA Notify Daemon
- HPCA Scheduler Daemon

21.2 Installation problems, which may occur

Problem:
After having entered the user credentials, the following error message may appear:
The entered credentials are correct:
Unable to install service necessary to manage products that require administrative credentials for future updates. This installation may have future problems managing these updates. Contact your support representative for more information. Util.SetContextSvcCredentials:
C:\Program Files\HP\Installers\SWM-SIM\itm_swm_create.bat returned non-zero exit code:
C:\Program Files\HP\Installers\SWM-SIM\itm_swm_create.bat

Reason (detected):
The RSSWM installation routine is unable to check the user credentials.

Problem:
Reboot: Error stopping the OVCM MSI Redirection Service.
Affected process: rsswm_radskman

Reason (detected):
File system has been configured to restrictive.

21.3 RSSWM not installed – how to check installed components

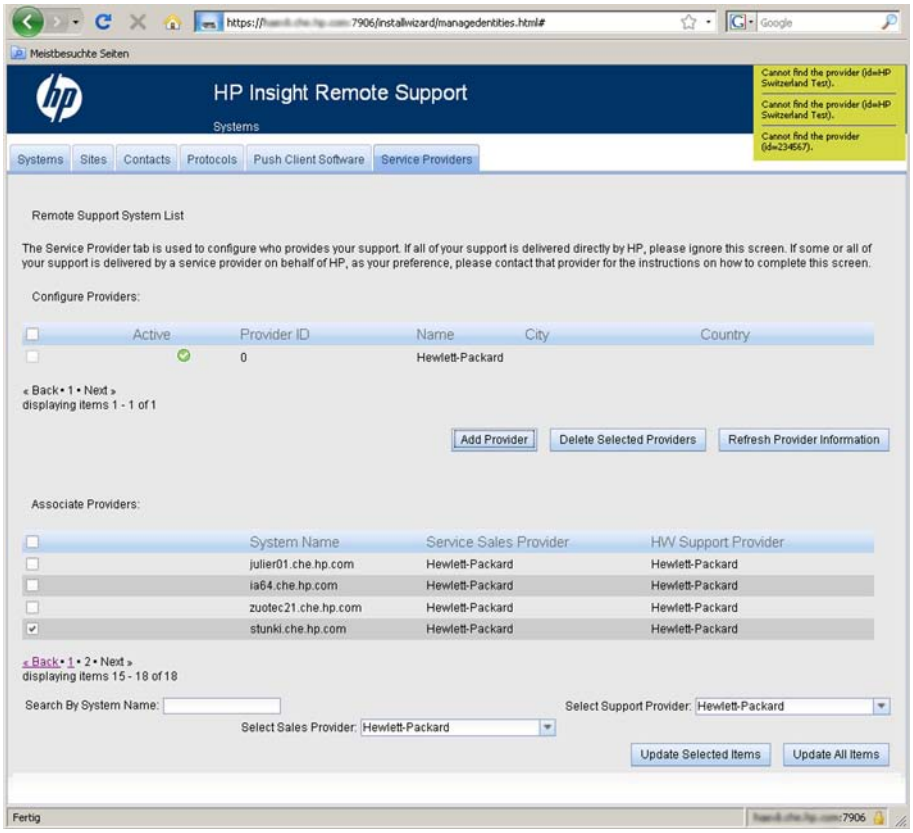
You can do it by
- Start > Programs > Hewlett-Packard > Remote Support Software Manager > View Status of Remote Support Components

- or by calling
  "C:\Program Files (x86)\HP\Installers\Lib2\RSSWM_Viewer.exe"

- IF you click onto the blue text, the latest IRS kit can be downloaded.

22 Appendix E Service Providers

Per default HP is the service provider who handles the support cases. HP forwards the support case to a partner or handles it itself.
When a HP partner is authorized to receive service requests directly, its address can be added here.
Important: You must ask for the Provider ID. This ID will only be given to authorized HP persons and authorized partners.
The partner must ask his HP contact, whether he is on the list of authorized providers and for his ID.



- click on “Add Provider” to enter the provider ID
  this ID will be checked immediately
- if the information appears, accept it to save it
- now add the new provider information to the foreseen devices

23 Appendix G Miscellaneous

23.1 Installation of SMH / PSP messages

HP Insight Management Agents for Windows Server 2003/2008
➔ Results in the message:
The software is not supported for installation on this system.

The installation program couldn't find the appropriate system management controller driver which is required but is not currently installed. Please install the appropriate system management controller driver and then rerun the setup program.

Press 'Close' to exit Setup.

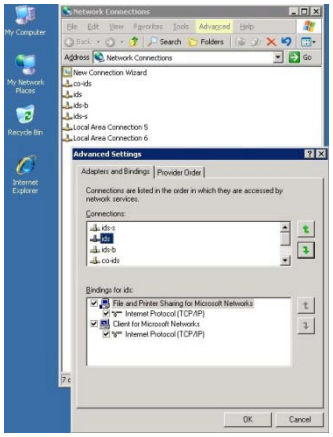
This agent cannot be installed, when no ILO information and its drivers are being found.

23.2 Windows - Selecting the Ethernet interface for remote access

When a system uses several Ethernet interfaces, **it is very important**, that the IRS connection to the HP backend uses the correct one. It's IP address will be registered in AMS.

- Check the net-interface which is being used, to access the public network
- click on "Start" - "Run" - enter taskmgr
- click on Networking"
- download a SW kit, for example, to discover the used interface
- If another of the interface has to be used for the IRS remote access, this one should be placed on top of the list.

For Windows 2003:



Modify the order of the interfaces:
- Right click onto the icon "My network"
- Click onto an active network interface and
- click on "Advanced", then "Advanced Settings"
- Select your interface (blue marked)
- Put it to the top position using the green arrows
- Click OK
- Check if the connection to the public network uses the selected interface (a reboot may be necessary)

23.3 Microsoft Error Codes

A list of Microsoft error codes and its meanings can be found on
http://msdn.microsoft.com/en-us/library/aa368542%28VS.85%29.aspx

23.4 Various IRSS Commands

- Verify whether the IRS Client is active (connection successful to the HP Backend).

```
C: :\Program Files (x86)\HP\RemoteSupport\bin
 iseectl –get –name CLIENT_STATE
```
-> expected ACTIVE

- Reconnecting / connectivity check IRSS with the HP backend

```
registerClient.cmd -forcereg
  837507DF-16B4-4FB1-A421-5DF8212F955A
```
Check the log file in
…\RemoteSupport\Logs\ regIncident.log
for the incident number and its status.

The same check can be done in WEBES under "RSC Settings" by pressing the Update button.

- Get more information of the log files during trouble shooting:

```
C:\Program Files (x86)\HP\RemoteSupport\bin
 iseectl –set –name LOG_LEVEL –value debug
```

when finished problem shooting set it back to

```
 iseectl –set –name LOG_LEVEL –value info
```