Configuring the hosting device

**Note**
The initialization and registration of Remote Support Software Manager (RSSWM) can only be performed by a user who is logged on to the hosting device through the system console or Remote Desktop Connection session.

- For Windows 2003, you need to use the /console switch (c:\windows\system32\mstsc.exe /console).
- For Windows 2008 you need to use the /admin switch (c:\windows\system32\mstsc.exe /admin).

Do not attempt to initialize or register a hosting device through a nonconsole mode Terminal Services or Remote Desktop Connection session.

Hosting device hard requirements

Refer to the Insight Remote Support Standard Release Notes for minimum requirements for the hosting device.


Creating an administrator account

For security reasons, it is always best to set up a user with administrator rights on the hosting device. You can use that user when a user with administrator rights is required. This account can also be used for WMI.

1. Access your hosting device.
2. Right-click the My Computer icon at the hosting device desktop, and click the Manage option. The Computer Management window appears.
3. Expand Local Users and Groups, right-click Users, and click New User.
4. On the New User dialog box, enter the new user details and set the password options.
5. Click Create and then Close.
6. On the right pane of the screen, right-click the new user, and click Properties.
7. Click the Member Of tab of the new user’s Properties screen. Click Add, and then enter Administrators, Remote Desktop Users, Distributed COM Users and any other group name as required in the "Enter the object names to select" field.

8. Click Check Names, and click OK → OK to close.

9. Close the Computer Management window, log off from the current user, and log in with the newly created user.

**Note**
Apart from a local user account, you can also use a domain user account.

Setting advanced proxy settings on the hosting device browser

Use Internet Explorer on the hosting device to set advanced proxy settings.

1. On the desktop of the hosting device, right-click the Internet Explorer icon and click Properties.

2. Click Connections → LAN Settings.

3. Clear the Automatically detect settings check box.

4. Select the Use a proxy server for your LAN check box, and in the associated Address and Port Fields, enter the proxy server information.

5. Select the Bypass proxy server for local addresses check box.

6. Click Advanced and under the "Do not use proxy server for addresses beginning with" field, enter the exceptions.

7. Click OK → OK → OK.

8. After you have configured the proxy settings, you can verify the connectivity to HP backend by using the following methods:

   - To test the connectivity between the Remote Support Client on the Hosting Device and the HP Support Center, use the URL: [https://services.isee.hp.com/version/index.html](https://services.isee.hp.com/version/index.html) The response should be a version number for example 05.50.09.537.

   - To test the connectivity between the hosting device and the Software Management server within the HP Support Center, use the URL: [https://rsswm.software.hp.com:443/site](https://rsswm.software.hp.com:443/site) The response should indicate the Remote Support Software Management server is operating correctly.
Note
RSSWM communicates directly with the HP Support Center through the firewall or web proxy server, if a web proxy server is in use. RSSWM supports connecting directly to the Internet or connecting through a proxy server and supports all proxy servers conforming to the HTTP/1.0 Specification. It does not support proxies using proxy auto-configuration scripts, NTLM authentication (also known as Integrated Windows Authentication), or Kerberos authentication.

Installing Java Runtime on the hosting device browser

Java is used by WEBES, which is an application installed by HP Insight RSS. So, you should verify that Java has been installed on your web-browser.

1. From your hosting device’s web browser, click Tools → Internet Options, and then click the Advanced tab.
2. Scroll down through the settings.
   • If Java is installed, the Java section and setting(s) will appear in the list of settings.
   • If Java is not installed, you will not see any mention of Java. To install Java, access [http://java.com/en/download/index.jsp](http://java.com/en/download/index.jsp) from your browser, and download Java to your hosting device by following the instructions on the screen.
3. Complete step 1 and 2 again to insure Java is loaded properly.
4. Close the browser window.

Installing .NET Framework and upgrade Internet Explorer

.NET Framework is required by the SQL Express database used by WEBES. You can download the install package from the Microsoft website. HP Insight RSS recommend using the latest updates.

1. Use Windows Explorer to access the folder where you have the setup file.
2. Double-click the dotnetfx.exe file.
3. Accept all of the end-user license agreement and the defaults when prompted by the Microsoft .NET Framework 2.0 setup, and then click Finish.
5. Launch Microsoft Internet Explorer
6. Check Internet Explorer version. HP Insight RSS support IE version 7 or newer.
7. Launch Windows Updates and check for any new updates from Microsoft.
8. Perform Windows Updates from Microsoft. Some updates might require the server to restart.

---

**Note**
If .NET Framework 2.0 is not installed on the hosting device before the Insight RSS installation, the installation process will fail with a non specific error message. To resolve the issue, install .NET Framework 2.0 and then re-run the installation process. The .NET Framework 2.0 software version is specifically required.

**Caution**
Relationship between .NET Framework 2.0, 3.0 and 3.5: If you install .NET Framework 3.x on a system that does not have version 2.0 installed, the installer automatically installs version 2.0 for you. This provides the .NET Framework 2.0 requirement for Insight RSS. Do not uninstall .NET Framework 2.0 from a .NET Framework 3.x installation, because this breaks Insight RSS.

---

**Verifying SNMP settings on the hosting device**

1. Go to Start → All Programs → Administrative Tools → Services to set the SNMP Services parameters required for the hosting device to securely send and receive traps.
2. Double-click the SNMP Service.
3. On the Traps tab, make sure a community string is listed and local host and 127.0.0.1 exists as a trap destination.
4. Go to the Security tab, and ensure that Accept SNMP packets from any host is selected.
5. Restart the service for the changes to take effect.

**Installing ProLiant Support Pack on the hosting device**

**Note**
If Insight RSS is to be installed on a VMware Guest OS, the ProLiant Support Pack should not be installed.
To install the ProLiant Support Pack (PSP) on the hosting device, perform the following steps:

1. Run the self-extracting executable that contains the PSP.
2. Close the HP Self Extracting Package dialog box.
3. Run setup.exe in the folder that contains the extracted kit.
4. Make sure the Local Host <name of your Hosting Device> option is selected, and click Next.
6. Select the options for the bundle as applicable to your environment. A descriptor for each option is provided on the screen.
7. Click OK in the Select Bundle Filter screen.
8. Select the HP Insight Management WBEM Providers for Windows Server 2003/2008 check box to include it in updates to be installed.
9. Clear the HP Version Control Agent for Windows check box as there is no need to install this since HP Systems Insight Manager (HP SIM) is not being used.
10. Scroll down to the System Management Homepage, and click its Configure Now link.
11. Accept the defaults. On the User Access screen, select Local Access and Administrator to provide secure access to the System Management Homepage. In the Trust Mode screen, select Trust All since HP SIM is not being used.
12. Select IP Binding, if needed, and click Next.
13. Select IP Restricted Login, if needed, and click Finish.
15. On the Item Configuration window, you can define how frequently the IM agent collects data. The frequency can be between 5 seconds and 60 minutes. Select Enable SNMP Sets. Leave the default Data Collection Interval at 2 minutes.
16. Select the Enable SNMP Sets and Enable Remote Reboot check box. Click Save.
18. In the Windows User Account Name field, enter the administrator name you had created earlier. This is the account you have set up for administrator and WMI purposes.

19. Click Save.

20. Select the Reboot System After Installation check box, and select the If Needed option to cause a reboot if necessary.

21. Click Install from the HP Smart Update Manager UI.

The installation proceeds and reboots the server if any components require it.

Installing Insight RSS and Insight RSS Configuration Wizard

You can download the Remote Support Software Manager (RSSWM) software from

To install the Insight RSS software, perform the following steps:

1. Use Windows Explorer to access the directory on your hosting device where you have the setup file.


3. Click Unzip to extract the files, and click OK in the Winzip Self-Extractor popup.


5. Select the appropriate privacy settings and click Next.


7. In the Remote Support Software Manager Agent Initialization screen, enter the values into the fields.

8. Click Next. A CM Status screen will appear, displaying the status of the install process. You can view the installation log file to check the status or error during the installation.
Important
You will see a number of screens open and close, none of which require your assistance. It is recommended not to use the keyboard during installation process, because it might cause the installation to get cancelled accidentally. The combined download and installation time of the software depends on your local network and hardware performance, global Internet activity, and the HP network.

9. After all the components are installed, click Next

Using the Insight RSS Configuration Wizard
After the installation is complete, the opening screen of the HP Insight RSS Configuration Wizard appears.
If a security alert window appears, install the certificate locally, by automatically selecting the certificate store based upon the certificate type.

Note
If you have exited the Insight RSS Configuration Wizard before completing the configuration, you can restart it by browsing to the following URL in a web browser on the hosting device: https://localhost:7906/installwizard/index.html.

1. Click Next to continue.
2. Scroll down to the bottom of the End User License Agreement, select I Accept the license agreement, and click Next to continue.
3. The Collection of Operating System and Configuration Information screen appears. Under the heading May HP contact you, select the appropriate option and click Next to continue.
4. Enter the information in the Company Information table. (See Important Note below.)
5. Click Next.
6. Enter the information in the Contact Information table. (See Important Note below.)
7. Click Next.
8. Enter the details in the SMTP configuration screen.
9. On the WMI Credential screen, make sure the Monitor Windows systems using WMI check box is checked and enter the information.
10. Click Next.
11. The CommandView EVA credentials screen appears. Enter the credentials and click Next.

12. Make sure your information has been entered correctly in the Input of Configuration Data is Complete screen, and then click Next.

13. In the Input of Configuration Data is Complete screen, make sure the Launch the Insight RSS administration console check box is selected, and then click Done.

14. The HP Insight RSS admin console should appear on completion.

---

**Important Note**
Customer Contact Information is to be entered as a part of the Insight RS installation process.

Customers may be contacted by HP to:

- Verify system failure
- Diagnose the problem
- Recommend a fix
- Confirm delivery type i.e. Engineer onsite, CSR etc.
- Confirm time to initiate repair

Complete and accurate contact information is imperative for timely resolution of customer issues.

If the customer’s contact information changes, then it is their responsibility to update the information in the Insight RS software as soon as possible.

---

**Configuring Insight RSS and adding service providers**

**Configuring Insight RSS from the admin console**

1. Select the Systems tab, and click the Discover Devices link.
2. From the Discovery Settings popup, clear all of the check boxes except for the Custom IP Ranges check box.
3. Enter the IP address range.
4. Click Save Settings.
5. Click Discover Devices ➔ Start Discovery.
6. Once the discovery is complete, you should see your hosting device and the managed systems listed.

7. Select the Protocols tab of the Insight RSS admin console.

8. Highlight the default WMI managed protocol, and click the Edit Protocol link to display the Edit Managed Protocol screen.

9. You should recognize all of the information you have entered earlier in the Configuration Wizard.

10. Click Cancel.

11. With the Systems tab active, highlight your hosting device, and then click the Edit System link.

12. Enter the device specific information. Ensure to include entitlement, site, and contact information.

13. Click Apply Updates.

Adding service providers

**Note**

The Service Provider tab is used to configure who provides your support. If all of your support is delivered directly by HP, this screen can be ignored. If some or all of your support is delivered by a service provider on behalf of HP, as your preference, you should add the provider information and associate the corresponding managed devices with the appropriate provider. If you do not have the required service provider information, please contact that provider for instructions to configure the details requested in the tab.

1. Click the Service Provider tab.

2. Click Add Provider.

3. Enter the Provider ID and click Look Up. The details for the provider appear. Click Accept.

4. To associate a provider with a managed device, select the device from the Associate Providers table.

5. Select the Sales Provider from the Select Sales Provider drop-down menu. This should be the provider you prefer to work with for IT solutions.

6. Select the Support Provider from the Select Support Provider drop-down menu. This should be the provider who provides support for the managed device.

7. Click Update Selected Items to save the changes.
Installing the VMware agent and SMH on the hosting device hardware

One of the most important things to keep in mind when using a VMware ESX server as an Insight Remote Support Standard hosting device is that all hardware events on the server must be detected at the ESX level, rather than by a guest OS. To accomplish this, VMware Management agent software must be installed on ESX, which then reports hardware events, through SNMP, to the WEBES installed on the Windows Server guest OS.

1. Open a terminal session to the VMware ESX server.
2. Change directories to the location where the VMware management agent is located.
3. Unarchive the VMware Management agent: At the command line type tar –zxvf <filename> where <filename> is the name of the file, for example hpmgmt-8.2.0-vmware3x.tgz

In addition to unpacking the file, the previous command created two new directories, for example /hpmgmt/820 under your current directory.

Change directories to the lower subdirectory seen above, for example cd hpmgmt/820

**Note**
You can view the README for the installation by typing view README.txt at the command prompt. Use Ctrl-Z to exit the view command.

4. At the command prompt type ./PreInstall_Setup.sh
5. On completion of the script, you will be prompted for a reboot. Allow the reboot.
6. Open a terminal session to the VMware ESX server.
7. Change the working directory to the installation subdirectory. For example, cd /RS/hpmgmt/820
8. At the command prompt type ./installvm820.sh -install

The installation script performs some basic checks and then guides you through the installation process with a number of questions.

On completion of the install process, you will see a message indicating “HP Insight Manager agents have been installed successfully.”

Example of using ProLiant Support Pack version 8.2. Refer to the ProLiant Support Pack for the most current information.

For more information on HP ProLiant and VMware vSphere, visit [http://www.hp.com/go/vmware](http://www.hp.com/go/vmware)
Verifying the Windows guest OS on the hosting device is active

In these next few steps, you access VMware vSphere Web Access to determine the status of the Windows guest OS on the ESX.

1. Access the ESX Web User Interface (e.g. http:// your esx host FQDN or IP Address)

2. In the Credentials window, type in the VMware Host login name and password on the Credential form and click Login. The VMware ESX Service Console web page appears.

3. In the Virtual Machines column, click the system name of the guest OS.

4. Make sure the Power State is "Powered On"; if not, click the Restart Guest link.

5. Close the VMware Service Console window

Preparing to install RSS on managed servers

Removing conflicting software from managed servers

These steps are required only if you already have any version of the following software installed on a managed device.

<table>
<thead>
<tr>
<th>Installed software</th>
<th>How to remove</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP ISEE client</td>
<td>In Control Panel, double-click <strong>Add/Remove Programs</strong>.</td>
<td><strong>Important!</strong> ISEE A.03.95 and earlier is not the same application as HP Insight Remote Support Advanced and it should not be installed on any systems with HP Insight Remote Support Standard (Insight RSS).</td>
</tr>
<tr>
<td></td>
<td>In the Add/Remove Programs dialog, locate the ISEE entry, if any, and click <strong>Remove</strong>.</td>
<td></td>
</tr>
<tr>
<td>WEBES (including WCCProxy)</td>
<td>Log in to the managed system using an account with administrator privileges.</td>
<td>After ISEE has been removed, removing WEBES should also remove WCCProxy. If ISEE was not already removed, WEBES will not remove WCCProxy.</td>
</tr>
<tr>
<td></td>
<td>Completely close all tools that are running.</td>
<td><strong>Tip:</strong> Before removing WEBES, it is recommended that you access the System Event Analyzer UI and retrieve the system</td>
</tr>
<tr>
<td></td>
<td>In Control Panel, double-click <strong>Add/Remove Programs</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Add/Remove Programs dialog, locate the WEBES entry and click Change/Remove to run</td>
<td></td>
</tr>
<tr>
<td><strong>OSEM</strong></td>
<td>Log in using an account with administrator privileges.</td>
<td>Uninstallation completely removes all the files under the OSEM directories. If desired, you can manually back up configuration files such as <code>working.props</code>, <code>hosts.txt</code>, or <code>communities.txt</code>. You also may want to back up the notifications folder to preserve copies of all your problem reports. OSEM 1.3.7 or greater makes a copy of all configuration and state information during the uninstall process.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>Completely close all tools that are running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Control Panel, double-click <strong>Add/Remove Programs</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the <strong>Add/Remove Programs</strong> dialog, locate the OSEM entry and click <strong>Remove</strong> to run the setup wizard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Caution!</strong> In the setup wizard, the first <strong>Cancel</strong> button is your only opportunity to cleanly exit the uninstall routine. Afterwards, do not cancel or stop the uninstallation, even if a cancel or quit option is made available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Follow the prompts to proceed with uninstallation.</td>
<td></td>
</tr>
<tr>
<td><strong>HP Configuration Collector</strong></td>
<td>Log on using an account with administrator privileges.</td>
<td>serial number and product IDs from the Managed Entities pages. This information subsequently can be used when you configure managed system properties in Insight RSS on the hosting device.</td>
</tr>
<tr>
<td></td>
<td>Completely close all tools that are running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Control Panel, double-click <strong>Add/Remove Programs</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select <strong>HP ISEE Configuration Collector for EVA</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select <strong>Remove</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If it is not still needed for HPCC for SAN Environments, select</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the setup wizard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When prompted, choose the Remove option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Follow the prompts to proceed with the uninstallation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Add/Remove Programs dialog, verify that the WCCProxy entry is not present. If it is, you can remove it manually by selecting and clicking Remove.</td>
<td></td>
</tr>
</tbody>
</table>
each of the HP Configuration Collector modules and select **Remove** (Core, Hosts, Infrastructure, Nearline, and Online).

### Protocol

Managed servers communicate with the hosting device using the communication protocols listed in the table.

<table>
<thead>
<tr>
<th>Managed system</th>
<th>Communication protocol (RDC &amp; Monitoring Protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Simple Network Management Protocol (SNMP) or Web-Based Enterprise Management (WBEM)</td>
</tr>
<tr>
<td></td>
<td>WBEM uses TCP Port 443 (Level 2), SNMP uses TCP Port 161 (Level 2)</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you choose to rely on WBEM for your managed Windows system communication protocol, configuring SNMP on those managed Windows systems is optional. However, if you do not configure it, the managed Windows system will not fully communicate SNMP information with the hosting device.</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Web-Based Enterprise Management (WBEM)</td>
</tr>
<tr>
<td></td>
<td>WBEM TCP Port 443 (Level 2), ACC TCP Port 443 (Level 3)</td>
</tr>
<tr>
<td>Linux</td>
<td>Simple Network Management Protocol (SNMP) or Web-Based Enterprise Management (WBEM)</td>
</tr>
<tr>
<td></td>
<td>SNMP uses TCP Port 161 (Level 2)</td>
</tr>
<tr>
<td>OpenVMS</td>
<td>Event Log Monitoring Collector (ELMC)</td>
</tr>
<tr>
<td></td>
<td>WBEM TCP Port 443 (Level 2)</td>
</tr>
<tr>
<td>HP StorageWorks</td>
<td>Event Log Monitoring Collector (ELMC)</td>
</tr>
<tr>
<td>EVA series</td>
<td>Level 2 - CommandView EVA, Telnet 23</td>
</tr>
<tr>
<td>HP StorageWorks</td>
<td>Simple Network Management Protocol (SNMP)</td>
</tr>
<tr>
<td>Managed Server Type</td>
<td>Management Methodologies and Protocols</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>MSA 1000 series</td>
<td>SNMP uses TCP Port 161 (Level 2)</td>
</tr>
</tbody>
</table>
| HP StorageWorks MSA 2000 (P2000) series | Web-Based Enterprise Management (WBEM)  
                       | WBEM uses TCP Port 443 (Level 2)        |
| HP StorageWorks XP series | via CMS. Uses HTTPS on TCP Port 443. Redirect SVP to broadcast its data to a "drop box" on CMS |
| Fibre Channel SAN switches | uses SNMP (TCP Port 161), SSH (TCP Port 22) and Telnet (TCP Port 23) |
| HP StorageWorks P4000 (LeftHand/SANiQ) | uses CLIQ (SANiQ - SNMP on TCP Port 5989) |

**Configuring managed servers (Windows, HP-UX) for RSS**

In this series of steps, you use the "Push Client Software" feature of the Insight Remote Support Standard (Insight RSS) admin console to push HP Insight Management WBEM Providers for Windows to your managed Windows server.

1. Log into the hosting device and open the Insight RSS admin console.
2. Click the Push Client Software tab of the Insight RSS.
3. Highlight your managed Windows server, as shown, and click Push Software.
4. Click Yes when prompted for confirmation. The HP Smart Update Manager window appears.
5. Click the Configure Now link in the row associated with the HP Insight Management WBEM Providers for Windows Server 2003/2008 product.
6. In the Item Configuration window, enter the name of an account on the managed server in the Windows User Account Name field. This should be the account with remote WMI access privileges. The account can be a local user or domain user account.
7. Click Save.
8. Click Install.

9. In the Installation Results screen, click Exit.

10. In Push Client Software Finished screen, click OK.

11. Open the Insight RSS admin console. You should now see the protocol for the Windows End-Point Server is listed as WBEM.

---

**Important**

After you have configured and discovered your server, you need to enter the entitlement information by clicking the Edit System button. Refer to the “Hosting Device enablement” demo for details. Also, after you have configured the server, you should associate it with a service provider if the support is provided by a provider other than HP. To do this, you can go to the Service Provider tab.

---

**Note**

WBEM Providers must also be installed on the hosting device. A WBEM protocol with the same account credentials must also be configured in the Insight RSS admin console to allow communication between the hosting device and managed system.

---

End-to-end test to verify remote monitoring

The WMI test application was installed during the HP Insight Management WBEM Providers installation on the managed device.

To verify the communication between the managed Windows server through the WMI test:

1. Access your managed Windows server.

2. Click Start → All Programs → HP Insight Management WBEM Providers → Test WMI Events.

3. From the HP Test WMI Event Tool screen, select the Event ID=3 option.

4. Click Send Event, and then OK.

5. Close the HP Test WMI Event Tool window, and disconnect from the managed Windows server.

6. Access the System Event Analyzer screen of your hosting device, and click the WEBES Notification Status icon on the System Event Analyzer toolbar.

7. You should see a problem report for your managed Windows server.
8. Verify that the status is Delivered. You can also click the link to view the problem report.

Configuring SNMP on the managed Windows server with MSA

1. Access your managed Windows server with MSA.
2. Since SNMP will be used, configure the SNMP Service to point to the hosting device. Select Start → Administrative Tools → Services.
3. The Services window appears. Double-click SNMP Service.
4. The SNMP Service Properties dialog box appears. Click the Agents tab and verify the contact and location information.
5. Click the Traps tab, click Add.
6. Enter the IP address or FQDN of your hosting device and click Add.
7. Click the Security tab, make a note of communities and rights and click Apply.
8. Click OK to save your changes.
9. Restart the SNMP Service.

Important
After you have configured and discovered your server, you must enter the entitlement information by clicking the Edit System button. Refer to the "Hosting Device enablement" demo for details. Also, after you have configured the server, you should associate it with a service provider if the support is provided by a provider other than HP. To do this, you can go to the Service Provider tab.

Configuring HP-UX server prerequisites

Note
This demo uses HP-UX 11.23. For details on other HP-UX versions, refer to documentation at http://www.hp.com/go/hpux-core-docs or ITRC (http://itrc.hp.com ). Diagnostics information is available at http://docs.hp.com/en/diag.html

Using HP-UX Installation Advisory

The following steps uses the Installation Advisor utility from HP Insight Remote Support Standard to verifies that all remote support prerequisites are met.
Execute the InsightRsHpuxPrereqCheckv24.sh (previously known as TestRSPv24.sh) would verify the system configuration and provides any recommendations, configuration or patches needed before the system is ready to be monitored.

1. Launch Insight RSS Admin Console
2. On the Service Heath tab, click at the Installation Advisor link. This would pop-up a new window.
3. Scroll down to Utilities for Monitored HP-UX Devices section.
4. Download and save the InsightRsHpuxPrereqCheckv24.sh
5. Download and save the InsightRsHpuxSetup.sh
6. Open an FTP session to HP-UX server and upload both files. Suggest to save both files in the /tmp/rss folder.
7. Close the FTP session
8. Initiate a Terminal session with your HP-UX server, and log in using the user credentials.
9. Change directory to the /tmp/rss folder
10. Type sh InsightRsHpuxPrereqCheckv24.sh
11. Use the default=root for the CIM user
12. As the script checking the system configuration, write down the information related to missing patches or software required. Some patches might be optional. If the result of this script is "You appear to have all key pre-requirements for RSP", then proceed to the next task. If missing patches or software is needed, proceed to the sample software installation steps below.
13. If you must remove and reinstall System Fault Management, to assure it is the last prerequisite installed, use the following commands.

   /usr/sbin/swremove SysFaultMgmt

   /usr/sbin/swinstall –s autoselect_dependencies=false –s

SysFaultMgmt is the source of depot, which can be either HP-UX installation media or a depot server.
14. Repeat the execution of InsightRsHpuxPrereqCheckv24.sh after patching and make sure system is ready.

15. Execute the InsightRsHpuxSetup.sh script (sh InsightRsHpuxSetup.sh). Resolve any deficiencies and rerun the script.

16. Continue to next section (Creating a nonprivileged user on the HP-UX server).

**Example**

Download HP-UX software or patched - installation steps

1. Check the operating system version using the `uname -a` command. HP 11.11, 11.23, and 11.31 are supported.

2. If you have Instant Support Enterprise Edition (ISEE) installed, remove ISEE by using `/usr/sbin/swremove ISEEPlatform`

3. Check that the 11i patch bundle B.11.23.0409.3 (September 2004) is installed using the `swlist -l bundle` command. Look for the presence of patch bundle B.11.23.0409.3 (September 2004) in the command output.

4. In addition to the required bundle, there might be other required patches. To check whether a patch is installed, use the `swlist -l patch <patchname>` command. Refer to the Quick Start Guide for more information on these patches.

5. Check that OpenSSL A.00.09.07i.012 or later is installed using the `swlist | grep -i OpenSSL` command.

6. Check that OnlineDiagnostics is installed, and make sure it is B.11.23.10.05 or later, by using the `swlist | grep -i OnlineDiag` command.

7. Check that the OnlineDiag is reporting "EVENT MONITORING IS CURRENTLY ENABLED", EMS Version is A.04.20 or later, and the STM version is A.49.10 or later. To do this, use the `/etc/opt/resmon/lbin/monconfig` command.

8. Enter `q` to exit the EMS Monitoring Request Manager Main Menu.

9. Check that HP WBEM Services for HP-UX is installed, and make sure it is A.02.05.08 or later, by using the `swlist | grep -i WBEM` command.

10. Check that System Management Web is installed, and make sure it is A.2.2.7 or later. System Management Web is recommended for event monitoring; however, it is required for configuration collection. To do this, use the `swlist | grep -i SysMgmtWeb` command.
11. Check that hpuxwsApache is installed, and make sure it is A.2.0.49 or later. hpuxwsApache is required for configuration collection only. To do this, use the `swlist | grep -i hpuxwsApache` command.

12. Check that System Management Base is installed, and make sure it is A.2.0.49 or later, by using the `swlist | grep -i SysMgmtBase` command. System Management Base is required for configuration collection only.

13. Check that System Management Homepage is installed, and make sure it is at least A.2.2.6.2. If A.2.2.6.2 is installed, patch PHSS_36870 must also be installed. To do this, use the `swlist SysMgmtWeb SysMgmtHomepage` command.

14. System Fault Management must be installed on the HP-UX server. To make sure it is the last prerequisite component installed, you must uninstall it and then reinstall it.

15. Enter the `/opt/sfm/bin/sfmconfig -w -q` command to determine whether the diagnostic mode of the HP-UX server is set to SFM or EMS.

16. Now, you will configure SMH to automatically start on boot by `smhstartconfig -a off -b on`. Restart SMH by “/opt/hpsmh/lbin/hpsmh stop” followed by “/opt/hpsmh/lbin/hpsmh start”

17. Verify SMH is set to start on boot with the `smhstartconfig` command.

1. To check HP-UX patches, launch a Internet browser and enter `http://www.itrc.hp.com`
2. Click the Patch database link.
3. You may need to register (new user) or login to ITRC.
4. To search for a patch, enter the patch name (e.g. PHSS_37552). Click Search
5. Add the patch to the download. Multiple patches can be added before downloading them.
6. Once the patches downloaded, open an FTP session to HP-UX server and upload all the patches.
7. Use swinstall to install all the patches. (e.g. `swinstall -s /tmp/rss/PHSS_37552.depot`)
8. Restart all relevant services or daemons (if needed).
Creating a nonprivileged user on the HP-UX server

Now, you will create a nonprivileged account using the useradd command, and assign the user to the users group.

1. For this demonstration, you create a user named mgmnt, assign the user to the users group, and then set a user password of mgmnt.
2. From the command line of your HP-UX server, enter:
   
   ```
   # useradd -g users mgmnt
   # passwd mgmnt
   ```
3. When prompted, provide the password and confirm the password.

Configuring the current CIM parameters

1. Determine the existing CIM configuration with the `cimconfig -l -p` command.
2. Based on the previous output, ensure/set the variables in the CIM planned configuration.
3. Stop and start the CIM server to set the configuration changes in the CIM current configuration using `cimserver -s` and `cimserver` command respectively.
4. Verify the settings in the CIM current configuration using the `cimconfig -l -c` command.
5. Add read and write authorizations for the user mgmnt to each of the namespaces, root/cimv2, root/PG_InterOp, root/PG_Internal, root/cimv2/npar, and root/cimv2/vpar using the following commands:
   
   ```
   #cimauth -a -u mgmnt -n root/cimv2 -R -W
   #cimauth -a -u mgmnt -n root/PG_InterOp -R -W
   #cimauth -a -u mgmnt -n root/PG_Internal -R -W
   #cimauth -a -u mgmnt -n root/cimv2/npar -R -W
   #cimauth -a -u mgmnt -n root/cimv2/vpar -R -W
   ```
6. Verify the user authorizations using the `cimauth -l` command.

Adding an HP-UX server through the Insight RSS admin console

1. On the hosting device, open the admin console and click Add System.
2. Enter the full name of your HP-UX server and click Add New System.
3. To add a protocol to be used by the HP-UX server, click the Protocols tab.
4. Click Add Protocol, enter the name of the protocol and select the type as UNIX WBEM. Click Add New Protocol.

5. Click Edit Protocol to specify the credentials.

6. Enter the user credentials for the user mgmnt that you created earlier. Click Apply Updates.

7. Return to the Systems tab and the HP-UX Server should be listed. You can click Edit System to edit the system information and enter the entitlement information.

---

**Important**

After you have configured and discovered your server, you must enter the entitlement information by clicking the Edit System button. Refer to the "Hosting Device enablement" demo for details. Also, after you have configured the server, you should associate it with a service provider if the support is provided by a provider other than HP. To do this, you can go to the Service Provider tab.

---

End-to-end test to verify remote monitoring

1. Log in to your HP-UX server and use the
   
   `/etc/opt/resmon/lbin/send_test_event -v -a disk_em` command
   
   to send a test event to your hosting device.

2. Access the System Event Analyzer screen of your hosting device and click the WEBES Notification Status icon on the System Event Analyzer toolbar.

3. You should see a problem report for your HP-UX server.

4. Verify that the status is Delivered to ISEE
Configuring ProLiant Linux for RSS

Before you can monitor your ProLiant managed Systems, you must:

- Validate that the systems are supported systems by checking the Insight Remote Support Standard Release Notes
- Verify the correct ProLiant Support Pack (PSP) tools are installed and configured on your systems

**Note**

For supported Linux ProLiant systems, the IM Agents version 7.1 or higher must be installed (or verified if already installed) from the PSP before you can continue.

The ProLiant Support Pack (PSP) is a system-specific software bundle that includes drivers, utilities, and management agents for your ProLiant devices. The PSP is shipped in-box with every ProLiant on the HP SmartStart CD.

The most current version is also available at [www.hp.com/servers/psp](http://www.hp.com/servers/psp).


IM Agents for Linux HP ProLiant systems running Linux are supported by Insight Management Agents (IM Agents), which are also delivered through the PSP. IM Agents on the SmartStart CD and/or in the ProLiant Support Pack (PSP) version 7.1 and higher are supported for Insight Remote Support.

**Note**

On your Linux managed system, the `/etc/snmp/snmpd.conf` file contains the current SNMP configuration. During your configuration of the installation script of IM Agents, watch for information about this file. When the script prompts you about Configuring SNMP access from remote Management Station(s), be sure to include the IP address for your hosting device. If you do not, you will need to reconfigure this on the managed system.

**System Management Homepage**

System Management Homepage (SMH) is also part of the PSP. It provides additional reporting capabilities on the managed system itself. While not mandatory for Insight Remote Support, if you have not configured your SNMP services correctly to communicate with the hosting device during Insight
Management Agent installation, you will need SMH to reconfigure those settings.

**Note**
Before installing the PSP, make sure that any installations of ISEE, WEBES, WCCProxy, and OSEM are removed from the managed system

1. Unpack the archive by entering `gunzip <psp-filename>.gz`, where `psp-filename` is the name of the PSP release.

2. Untar the file by entering `tar -xvf <psp-filename>.tar`, where `psp-filename` is the name of the PSP release.

3. Locate the line containing `install***.sh`, and note the name of the file and the full path to that file. For example, `compaq/csp/linux/install792.sh`.

4. Change the current directory to the path determined in the previous step with the `cd <install path>` command, where `<install path>` is the path determined in step 3. For the above example, the command is `cd compaq/csp/linux`

5. Execute the install with the `./<install file name>` command, where `<install file name>` is the file name noted in step 3.

   - The installer checks for the installation of rpm packages that are required by some of the components. If any rpm packages are missing and are found on the system, you will be prompted to install them.

   - The HP ProLiant Linux Deployment Utility opens. It lists the components that will be installed as part of the PSP.

   - By configuring these components, you will configure SNMP for the management system while you're installing the PSP. You can reconfigure the SNMP settings later using the System Management Homepage, but the HP ProLiant Deployment Utility provides the most convenient interface for initial configuration. To configure a component, you select it from the list, right-click it, and select Configure Component from the context menu.

6. You should check the "Reboot Server after successful completion of ProLiant Support Pack if components require it?" check box. Then start the installation by clicking Install.

7. A message in a separate window, which might be hidden behind the Deployment Utility screen, appears asking if you want to save the configuration information. Click Yes and the installation will begin. A message box displays to notify you when installation is complete. Click OK.
8. Review the Installation Status screen. You should see a green square with a checkmark next to each component.

Configuring SNMP on a managed Linux server

After you have installed the PSP on your ProLiant Linux server, you access the snmpd.conf file to add the IP address for the hosting device for SNMP communication from the managed systems. You must do this for each Linux managed system.

1. In a web browser, access the System Management Homepage on the managed system: https://ipaddress:2381
2. Log in using the root user name and password for the managed system.
3. Click the Settings tab.
4. Click the SNMP Configuration link.
5. In the SNMP Configuration File, add a trapsink command that includes the IP address for your hosting device, for example trapsink 192.168.2.4 public, and click Change.

**Note**

For those Linux installations (for example Red Hat 4 or 5) that support the added security of view statements, the following adjustments should be made from the defaults. If you do not assign the trapsink entry as public, you must configure a new SNMP protocol for this managed system and any other using the same community string through the Insight Remote Support Standard Console on the hosting device.

6. For the hosting device to be able to collect all relevant information about the managed systems, you must scroll down in the SNMP Configuration File to the view systemview included entries. Comment out the default entries with a # character. Then add this entry: view systemview included .1 80, and click Change.
Adding the Linux ProLiant server through the Insight RSS admin console

1. On the hosting device, open the admin console and click Add System.
2. Enter the full name of your Linux ProLiant server and click Add New System.

   **Note**
   If you selected a value other than “public” for the read-only community string, you must add a protocol by selecting the Protocols tab.

3. You would now return to the Systems tab and the Linux ProLiant server should be listed. You can click Edit System to edit the system information and enter the entitlement information.

   **Important**
   After you have configured and discovered your server, you must enter the entitlement information by clicking the Edit System button. Refer to the “Hosting Device enablement” demo for details. Also, after you have configured the server, you should associate it with a service provider if the support is provided by a provider other than HP. To do this, you can go to the Service Provider tab.

End-to-end test to verify remote monitoring

1. In a web browser, access the System Management Homepage on the managed system: https://ipaddress:2381
2. Log in using the root user name and password for the managed system.
3. Click the Settings tab.
4. Click the SNMP Configuration link.
5. At the bottom of the SNMP Configuration window, select Send Trap.
6. Access the System Event Analyzer screen of your hosting device, and click the WEBES Notification Status icon on the System Event Analyzer toolbar.
7. You should see a problem report. Verify that the status is “Delivered.”
Configuring an OpenVMS managed system for RSS

**Note**
When installing or upgrading managed systems to work with HP Insight Remote Support Standard version 5.50 installed on the Hosting Device, you MUST REMOVE ANY and ALL previous versions of WEBES or the HP ISEE client that may be currently installed. The Event log Monitoring Collector (ELMC), previously known as WCCProxy, must also be removed.

For more information, visit http://www.hp.com/go/ovms-docs

1. Extract the ELMC installation software package by entering the command:

   `run <ELMC_filename>`

   where

   `<ELMC_filename>` is the name of the installation package.

   For example, ELMCV25BL20KIT1_Mar-25-2009_OVMS64.EXE

2. Execute the DCL script by entering the command:

   `@ wccproxy_install install`
Adding the OpenVMS server through the Insight RSS admin console

1. On the Hosting Device, open the admin console and click Add System.
2. Enter the full name of your OpenVMS server and click Add New System.
3. You would now return to the Systems tab and the OpenVMS server should be listed. You can click Edit System to edit the system information and enter the entitlement information.

**Important**
Once you have configured and discovered your server, you need to enter the entitlement information by clicking the Edit System button. Please refer to the Hosting Device enablement demo for details. Also, once you have configured the server, you should also associate it with a Service Provider if the support is provided by a provider other than HP. To do this, you can go to the Service Provider tab.

Configuring managed storage array (EVA, P4000) for RSS

**Verifying that CommandView EVA software is installed**

1. Go to Start → Control Panel → Add or Remove Programs.
2. Verify that CommandView EVA Software Suite is listed.
3. Go to Start → Administrative Tools → Services and verify that the HP StorageWorks CIM Object Manager service is listed and started.

**Note**
The above mentioned steps are valid for verifying CommandView EVA 8.x (or newer) is installed. If your Storage Management Server has CommandView 7.x (or older) installed, go to Control Panel and ensure that the following components are listed in the Add/Remove Programs dialog:

- HP StorageWorks CommandView EVA
- HP StorageWorks SMI-S CIMOM
- HP StorageWorks SMI-S EVA
Creating an administrator account

1. Access your Storage Management Server.
2. Right-click the My Computer icon at the hosting device desktop, and click the Manage option. The Computer Management window appears.
3. Expand Local Users and Groups, right-click Users, and select New User.
4. In the New User screen, enter the new user details and set the password options.
5. Click Create and then Close.
6. In the right pane of the screen, right-click the new user, and select Properties.
7. Click the Member Of tab of the new user’s Properties screen. Click Add, and then enter Administrators, Remote Desktop Users, Distributed COM Users, HP Storage Admins, HP Storage Users and any other group name as required in the "Enter the object names to select" field.
8. Click Check Names, and click OK to close.
9. Log off from the current user and login with the newly created user.

Note
Apart from a local user account, you can also use a domain user account

Discovering and configuring the storage management server and the EVA in the HP Insight RSS admin console

It is important to note that Storage Management Server supports both SNMP and WBEM. It is recommended that one of the protocols be turned off to prevent dual notification of a failing device.

Configure SNMP Setting for Storage Management Server

1. In Storage Management Server, open Services console from Administrative Tools.
2. Within the Services window, scroll down to locate SNMP Service.
3. Double click SNMP Service.
4. Click Agent tab to verify the contact & location information.
5. Click Traps tab to specify the hosting device IP address.
6. Under Trap destinations, click Add button to enter the IP address.
7. Click Security tab to verify the Community Name and Rights.
8. Select Accept SNMP packets from any host.
9. Click Apply and then OK button.
10. Restart SNMP Services. If prompted whether to restart other service, click Yes.
11. Close the window.

Configure Host Notification option in HP CommandView EVA
1. On the Storage Management Server, double click Command View EVA icon at desktop.
2. Login user name with admin privilege and the password. Click Log on.
3. In Command View EVA software, click EVA Storage system.
4. At the Initialized Storage System Properties page, click System Options button to set the SNMP trap destination.
5. In System Options page, click Configure host notification option.
6. To specify the SNMP trap destination, click Modify host list button.
7. At the Host name field, enter hosting device system name or IP address. Leave the Notify Port as SNMP.
8. Click Save Changes.
9. At Configure Host Notification page, click OK.

! Important
It is NEVER acceptable to unplug a device on an EVA for the purpose of creating an event to verify end-to-end connectivity between the EVA and HP Data Center.

Adding and configuring the storage management server and the EVA in the Insight RSS admin console
1. On the hosting device, launch Insight RSS Admin Console.
2. In RSS Admin Console, click Systems tab.
3. Click Add system to add the EVA Storage Management Server. You may use Discover Devices option and specify IP address range to discover multiple SMS.
4. Enter SMS system name in the Add a new Managed System dialog.
5. Storage Management Server and EVA Storage System will appear in the Systems tab after refresh.
6. You can update the system details for SMS & EVA.
7. First, update the Storage Management Server detail by selecting the Storage Management Server and click Edit System.

8. Depending on customer entitlement, scroll down to select the valid entitlement type and enter the rest of the information.

9. Select the customer Site and Primary Contact information. This is important because HP support will based on this information to reach the customer for timely resolution of system issues.

10. Click Apply Updates.

11. To verify the CommandView system details, select the system and you can see the system information at Summary tab below. To verify the rest of the information, click on the other tabs like Entitlement, Contact & Site, and Device Protocols.

12. Secondly, update the EVA Storage System detail by selecting the EVA and click Edit System.

13. Depending on customer entitlement, scroll down to select the valid entitlement type and enter the rest of the information.

14. Select the customer Site and Primary Contact information. This is important because HP support will based on this information to reach the customer for timely resolution of system issues.

15. Click Apply Updates.

16. To verify the EVA details, select the system and you can see the system information at Summary tab below. To verify the rest of the information, click on the other tabs like Entitlement, Contact & Site, and Device Protocols.

---

**Important**

Take note that Storage Management Server supports both SNMP and WBEM. It is recommended that one of the protocols be turned off to prevent dual notification of a failing device.

---

**Send SNMP test trap from SMS**

If the SNMP protocol is used, the following steps are showing how to send SNMP test trap with HP Insight Management Agent in Storage Management Server.

1. Launch the HP Management Agents from Control Panel.

2. In Management Agents for Servers window, Click SNMP Settings tab.

3. Click Send Test Trap button and wait for the reply message.
4. At the message, click OK.
5. Click OK to close the Management Agents window.

**Verify the SNMP Test Trap at Hosting Device**

1. Launch System Event Analyzer.
2. In the System Event Analyzer window, click the WEBES Notifications button at top toolbar.
3. At the right pane, you will see the SNMP test trap.
4. Under the RSC Incident column, click the incident to view the detail.

**To install WBEM provider to SMS**

It is important to note that Storage Management Server supports both SNMP and WBEM. It is recommended that one of the protocols be turned off to prevent dual notification of a failing device. WBEM provider for SMS software can be push from hosting device under Push Client Software feature.

1. First, launch the Insight RSS Remote Console.
2. In the console, click Push Client Software tab.
3. Select the SMS from the “Select Systems to Update” list. Then click Push Software button.
4. Click Yes when prompted for confirmation.
5. HP Smart Update Manager will connect to Storage Management Server and perform software checking. A software list window will be shown.
6. For the WBEM Providers, click “Configure Now” link and provide the valid user name. Then click Save button.
7. Click Install.
8. HP System Update Manager will prompt the installation result. Click Exit to close the window.
9. Push Client Software window appears. Click OK to close.
10. Click Systems tab to update the system details.
11. Select the Storage Management Server and click Edit System.
12. Turn off the SNMP protocol by select OFF from SNMP drop-down list.
13. At WMI or WBEM drop-down list, select default WMI protocol.
14. Scroll down and click Apply Updates.

15. To verify the Storage Management Server details, select the server and you can see the server details at Summary tab below. To verify the rest of the information, click on the other tabs like Entitlement, Contact & Site, and Device Protocols.

**Send WMI Test event from SMS**

In Storage Management Server, send a WMI test event and later verify the event in hosting device. First at Storage Management Server, run the Test WMI Events program under HP Insight Management WBEM providers.

1. At HP Test WBEM Events Tool, select Event ID=3 and click Send Event button.
2. An Event has been sent and you can find the event in the NT event viewer.
3. Click OK to close

**Verify the Test WBEM Event at Hosting Device**

1. Launch System Event Analyzer at the Hosting Device.
2. In the System Event Analyzer window, click the WEBES Notifications button at top toolbar.
3. At the right pane, you will see the WMI Test Event.
4. Under the RSC Incident column, click the incident to view the detail

**Test the ELMC protocol from SMS**

In Storage Management Server, send an ELMC test event and later verify the event in hosting device. ELMC software can be push from hosting device to Storage Management Server. See the section install WBEM Providers for SMS.

1. At the Storage Management Server, open the command prompt window.
2. At the command prompt window, type the command `wccproxy test` and press Enter key.

**Verify the ELMC Test at Hosting Device**

1. Launch System Event Analyzer at the Hosting Device.
2. In the System Event Analyzer window, click the WEBES Notifications button at top toolbar.
3. At the right pane, you will see the ELMC Test Event.
4. Under the RSC Incident column, click the incident to view the detail.

**Note**
It is NEVER acceptable to unplug a device on an EVA for the purpose of creating an event to verify end-to-end connectivity between the EVA and HP Data Center.

---

**Configure CommandView EVA on EVA4400 Management Module**

*(Array Based Management)*

EVA Support with CommandView on ABM In EVA 4400, Command View can be launched from the Controller Management Module. We can perform Array Based Management (ABM) on EVA4400 and no dedicated Storage Management Server is required.

**Configure Host Notification option for EVA**

1. Use web browser in hosting device, to access ABM Command View.
2. At the web browser, type the URL as “https://<Command View IP>:2372”, where Command View IP is the IP address of the EVA4400 Management Module.
3. Login user name with admin privilege and the password. Click Log on.
4. At the Initialized Storage System Properties page, click System Options button to set the SNMP trap destination.
5. In System Options page, click Configure Host Notification option.
6. To specify the SNMP trap destination, click Modify Host List button.
7. At the Host name field, enter hosting device system name or IP address. Leave the Notify Port as SNMP.
8. Click Save Changes.
9. At Configure Host Notification page, click OK.

**Add ABM CommandView managed system and EVA into RSS**

1. At the hosting device, launch the Insight RSS Admin Console.
2. In RSS Admin Console, click Systems tab.
3. Click Add system to add the ABM CommandView system. You may use Discover Devices option and specify IP address range to discover multiple EVA4400.

You can also add a single system instead of network discovery. To add a new Managed System dialog, specify the ABM CommandView system IP Address and then click Add New System.

1. ABM CommandView system and EVA4400 will appear in the Systems tab after refresh.
2. In EVA ABM CommandView system, the valid entitlement information, serial number and product number need to be manually entered in RSS Admin Console.
3. Before update the ABM CommandView system details in Admin Console, open the Command View EVA software from the web browser to gather the necessary information.
4. In Command View software, expand the EVA tree. Locate the Controller Enclosure Properties under Hardware folder.
5. Write down the Serial Number and Product Number of the EVA4400.
6. Return to RSS Admin Console.
7. Select the ABM CommandView system and click Edit System.
8. Change the System Sub-type from unknown to CommandView Server.
9. Select the valid entitlement type and enter the rest of the information.
10. Manually enter the Serial Number and Product Number. Information can be gather from CommandView EVA or physical hardware.
11. Scroll down to select the customer Site and Primary Contact information. This is important because HP support will based on this information to reach the customer for timely resolution of system issues.
12. Click Apply Updates.
13. To verify the CommandView system details, select the system and you can see the system information at Summary tab below. To verify the rest of the information, click on the other tabs like Entitlement, Contact & Site, and Device Protocols.

To ensure the successful monitor the newly added storage node, check the Service Health tab.

14. Update the entitlement, site & primary contact information for the EVA.
15. Click Service Health tab.
16. Select the ABM CommandView system and EVA.
17. From the Action drop-down list, choose Verify Selected Devices, and click Run Action button.
18. Refresh the console.

If the systems are successfully monitored, green icon will be shown under monitoring column.

Discovering and configuring the P4000 (HP LeftHand SAN) central management console and P4000 storage node in the Insight RSS admin console

**P4000 - Patch 10076 installation**

HP Insight Remote Support has a minimum requirement of HP P4000 SAN/iQ version 8.5, therefore only platforms supported by version 8.5 and higher will be able to migrate to HP Insight Remote support. In addition to SAN/iQ version 8.5, patch 10076 is required for Remote Support.

2. Select either LeftHand NSM Storage Systems or P4000 SAN Solutions.
3. Select the option that represents your product.
4. Select Download drivers and software.
5. Select your product.
6. Select Cross operating system (BIOS, Firmware, Diagnostics, etc.).
7. Download the patch version 10076.
8. Launch the HP StorageWorks P4000 (LeftHand/SANiQ) Central Management Console (CMC).
9. Enter username and password to log in to node.
10. Select the first storage node you want to upgrade.
11. Click Storage Node Tasks and select Install Software.
12. On the Install Software window, click "Browse..." and select the patch upgrade file that you downloaded from the web site.
13. Select "Open Install File"
14. Select the storage nodes that require the patch.
15. Select Install file on selected Storage nodes one at a time (Recommended).
16. Click Install.
17. Read the message prompted and click Install.
18. After the installation completed, click OK.
19. You may check the Install Status dialog for more information.
20. Click Close to close the Install Status dialog

**Configure SNMP Setting for P4000 node with CMC**

1. Launch HP LeftHand Centralized Management Console (CMC) from Hosting
device or any windows machine with CMC.
2. Enter username and password to log in the P4000 node.
3. Expand the node and select SNMP.
4. At the SNMP General tab, ensure the Agent status is “Enabled, running”
   and Community String is public
5. Click SNMP Traps tab to define the IP address for hosting device.
6. At SNMP Traps tab, click SNMP Trap Task button and select Edit SNMP
   traps.
7. At Edit SNMP traps window, specify the Community String. (In this demo,
   we will use public)
8. Click add button to define IP address for hosting device.
9. Enter the hosting device IP address and select trap version 1 and click OK.
10. Click OK at Edit SNMP Traps window.

**Add P4000 node in Insight RSS admin console**

1. On the hosting device, open the admin console and click Add System.
2. In Add a new Managed System dialog, specify the storage node name and
   then click Add New System.
4. If SANiQ protocol is not defined, click Protocol tab.
5. At the Protocols tab, click Add Protocol.
6. Enter protocol name. (In this demo, we use LeftHand.)
7. Select the protocol type as SANiQ.
9. Select the new added protocol, (In this demo, enter LeftHand.)
10. Modify the protocol credential by clicking Edit Protocol.
11. Enter the user name and password and click Apply Updates
12. Return to System tab to update P4000 Storage node details
13. Select the P4000 node and click Edit System.
14. Select the SANiQ protocol defined in the previous step.
15. Depending on customer entitlement, select the valid entitlement type and enter the rest of the information.
16. Scroll down to select the customer Site and Primary Contact information. This is important because HP support will based on this information to reach the customer for timely resolution of system issues.
17. Click Apply Updates.
18. To verify the storage node details, select the node and you can see the system information at Summary tab below. To verify the rest of the information, click on the other tabs like Entitlement, Contact & Site, and Device Protocols.
19. To ensure the Insight RSS able successful monitor the newly added storage node, check the Service Health tab.
20. Click Service Health tab.
21. Select the P4000 storage node.
22. From the Action drop-down list, choose Verify Selected Devices, and click Run Action button.
23. Refresh the console.
24. If the node is successfully monitored, a green icon will be shown under Monitoring column.

Send Test SNMP and verify P4000 SNMP setting
1. Launch the CMC, login and expand the P4000 node
2. Select SNMP and click SNMP Traps tab.
3. Click SNMP Trap Tasks and select Send Test Trap.
4. SNMP trap sent message prompted and click OK.
**Verify Test SNMP trap at hosting device**

1. Launch System Event Analyzer.
2. Enter user profile name and click logon.
3. In the System Event Analyzer window, click the WEBES Notifications button at top toolbar.
4. At the right pane, you will see the test trap.
5. Under the RSC Incident column, click the incident to view the detail.

**Verifying collections**

Collections are scheduled to run once a month. The date and time of the initial collection is randomized; however, subsequent collections will occur on that same day and time of the month. It is not possible to change the collection schedule. To verify collections, perform the following steps:

1. Open System Event Analyzer on your Hosting Device.
2. Click Configure WEBES Managed Entities on the SEA toolbar. You should see the configuration collection listed under the Last Collection column associated with your End-Point Server. If the collection exists in SEA, the configuration collection process between the Managed Device and WEBES is operating properly.
3. Click the collection link to view the collected information in the associated .xml file.
References:

1. HP Insight Remote Support Standard documentation
   
   http://www.hp.com/go/insightfoundation-manuals

   - HP Insight Remote Support Standard Quick Start Guide
   - HP Insight Remote Support Standard Release Notes
   - HP Insight Remote Support Standard Frequently Asked Questions

2. HP Insight Remote Support Standard Software


3. System Event Analyzer (SEA) user interface, documented in the WEBES User Guide


4. HP ProLiant Support Pack documentation and downloads

   http://www.hp.com/servers/psp

5. HP Insight Management WBEM Providers documentation and downloads

6. Installation Queries

- In case of installation issues, go to Insight RS Technical Support at http://www.hp.com/go/rstechsupport and use the support contact information.