



Hewlett Packard
Enterprise

HPE Insight Remote Support

Software Version: 7.6

Installation and Configuration Guide

Document Release Date: November 2016

Software Release Date: March 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Intel®, Itanium® and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

© 2012 Google Inc. All rights reserved. Chrome™ is a trademark of Google Inc.

Contents

Preface	6
Document purpose and audience	6
Product overview	6
Related documents	7
Document revision history	7
Sign up to receive Insight Remote Support communications	8
Support information	8
We appreciate your feedback!	8
Chapter 1: Understanding installation process and requirements	9
Upgrade Insight Remote Support	9
Fulfill Hosting Device system requirements	10
Fulfilling hardware requirements	10
Number of monitored devices supported	11
Configuration collection capabilities	12
Fulfilling operating system requirements	14
Supported Microsoft Windows operating systems	14
Supported Microsoft Hyper-V server	15
Supported VMware operating systems	16
Supported Citrix XenServer operating systems	16
Fulfilling software requirements	16
Install web browsers	16
Install .NET Framework	17
Perform a Windows Update	17
Fulfilling access requirements	17
Fulfill networking requirements	18
Fulfill communication requirements	18
Configuring communication from a web browser to Insight RS	18
Configuring communication from the Hosting Device to HPE	19
Configure the Hosting Device to use DNS	19
Verify Hosting Device connectivity with HPE	21
Configuring communication between the Hosting Device and monitored devices	22
Install SNMP on the Hosting Device	22
Configure Traps	23
Set SNMP Trap service startup type	23
Update WMI Mapper to monitor Windows Server 2012 devices	23
Monitor the Hosting Device	24
Chapter 2: Installing Insight Remote Support for the first time	25
Download and install Insight Remote Support	25
Locating log files	27

Logging on to the Insight RS Console	28
Known issue: Cannot log on to the Insight RS Console as an administrator	28
Resolve certificate warning	29
Internet Explorer	29
Mozilla Firefox	30
Google Chrome	31
Chapter 3: Completing the Setup Wizards	33
Complete the Monitored Device Setup Wizard	33
Configure your devices	34
Configure protocol access credentials	34
Discovery sources	36
Discover devices	38
Export health report	39
Complete the Hosting Device Setup Wizard	40
Receiving remote support	40
Optimize environment	40
Remote support software updates	41
Contact information	41
Site information	42
Registering HPE Insight Remote Support	43
Test connectivity to HPE	43
Register with HPE	43
Integrate Insight RS with HPE Insight Online	44
HPE Authorized Channel Partners	45
Chapter 4: Completing post-installation configuration tasks	46
Verify Hosting Device health	46
Verify warranty and contract information	46
Verify device status	47
Resolve monitored device status issues	48
Send test events and generate collections	49
Clear status errors	49
Configure the backup settings	50
Set the backup target location	50
Set the number of backup versions	51
Integrate with HPE SIM	51
Install the HPE SIM Adapter	51
Configure the HPE SIM Adapter	52
Enable and configure email notifications	53
Forward service events to another management application	55
Trap type variables and descriptions	57
Enable operator-level user authentication	59

Enable SSLv3 (if required)	59
Determine which devices are affected by SSLv3 disablement	61
Disable SNMP automatic discovery	62
Add device groups	62
Chapter 5: Restoring from backup	64
Manually run backup schedules	64
Viewing successful backup information	65
Identifying backup failures	65
Restoring Insight RS from backup	65
Chapter 6: Uninstalling Insight RS	67
Disable Insight Online	67
Close support cases	67
Delete devices from Insight RS Console	67
Disable connection to HPE Insight Online	68
Uninstall the Insight RS software	69
Cleanup Hosting Device	69
Appendix A: Export and import of device information	70
Export a bulk CSV file	70
Import a bulk CSV file	70
Edit a bulk CSV file	71
Glossary	74
Index	79

Preface

Document purpose and audience

This document provides the necessary information to install and configure HPE Insight Remote Support (RS) on a Hosting Device and provides steps to troubleshoot the installation.



Important: This document only covers installing and configuring Insight RS on the Hosting Device. Your monitored devices may require additional software components and configuration that needs to be completed separately. Device configuration should be performed prior to the installation of Insight RS. The information necessary to configure monitored devices is described in the *HPE Insight Remote Support Monitored Devices Configuration Guide*. If you have not completed the installation and configuration information described in both of these documents, Insight RS may not work properly.

This document is intended for HPE's customers, HPE business partners, and HPE account teams. This document is intended to guide both HPE customers and HPE support personnel through the installation and configuration of Insight RS.

Product overview

Insight RS is a software solution that enables reactive and proactive remote support to improve the availability of supported servers, storage systems, and other devices in your data center. Insight RS relies on several HPE components and communication between various software applications within the customer enterprise and between the customer enterprise and HPE to deliver support services. Software components may be installed on the Hosting Device or on monitored devices depending on their purpose.

Insight RS can be used on its own or can be integrated with HPE Systems Insight Manager (SIM).

For more information about Insight RS, go to: www.hpe.com/services/getconnected.



Important: To configure Insight RS correctly, it is essential that you read this document thoroughly *before* proceeding with the installation of Insight RS.

Related documents

For additional Insight RS documentation, go to: www.hpe.com/info/insightremotesupport/docs.



- *HPE Insight Remote Support Release Notes*
This document provides product details and information about which monitored devices and Hosting Devices are supported for use with the Insight RS solution.
- *HPE Insight Remote Support Quick Installation Guide*
This document provides a checklist for installing and configuring Insight RS.
- *HPE Insight Remote Support Installation and Configuration Guide*
This document provides detailed information about installing and configuring Insight RS.
- *HPE Insight Remote Support Monitored Devices Configuration Guide*
This document provides information to configure the devices that will be monitored by Insight RS.
- *HPE Insight Remote Support Security White Paper*
This document provides an overview of the security features available in Insight RS.
- *HPE Insight Remote Support Upgrade Guide*
This document provides information about upgrading Insight RS to version 7.6.
- *HPE Insight Online Getting Started Guide*
This document provides information about the prerequisites for using HPE Insight Online, and explains how to use Insight Online to manage your company's HPE devices, contracts and warranties.

Document revision history

Edition	Software Version	Publication Date	Change Summary
1.4	7.6	November 2016	<ul style="list-style-type: none"> • Updated HPE data center URL to api.support.hpe.com/v1/.
1.3	7.6	September 2016	<ul style="list-style-type: none"> • Added info about maximum device count in Insight Online.
1.2	7.6	August 2016	<ul style="list-style-type: none"> • Update for Patch release. • Added SNMP Service Event Adapter MIB details.
1.1	7.6	June 2016	Added information about SNMP automatic discovery configuration setting.
1.0	7.6	March 2016	Initial release.

Sign up to receive Insight Remote Support communications

The HPE Insight Remote Support product team uses HPE's Support Communication process to communicate important news such as Engineering Advisories, Customer Advisories, Engineering Notices, and Customer Notices.

To sign up to receive Support Communications using HPE Subscribers Choice, go to: www.hpe.com/software/swupdatealerts.

When you subscribe, search for *Insight Remote Support*.

Support information

HPE recommends you consult the Insight RS documentation to resolve issues. The documentation is designed to guide you through a successful installation and configuration. However, if you need further support for Insight RS, help is available through HPE local Response Centers. For contact details, go to: <http://www.hpe.com/services/getconnected>.

Before contacting support, you can check if your issue has a solution available. Note that a valid contract and HPE Passport log on is required to view issue solution documents.

To view Insight RS issue solutions, complete the following steps:

1. Go to www.hpe.com and browse to **Support** → **Support & troubleshooting**.
2. On the **Troubleshooting** tab, click **See All** to browse all product categories.
3. In the **Enter product name/number** field, type **Insight Remote Support** and click the search icon.
4. In the search results, click **HPE Insight Remote Support Next Gen Software**.
5. On the **Top issues & solutions** tab, click **View all** to see the solutions.

We appreciate your feedback!

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Insight Remote Support, 7.6 Installation and Configuration Guide

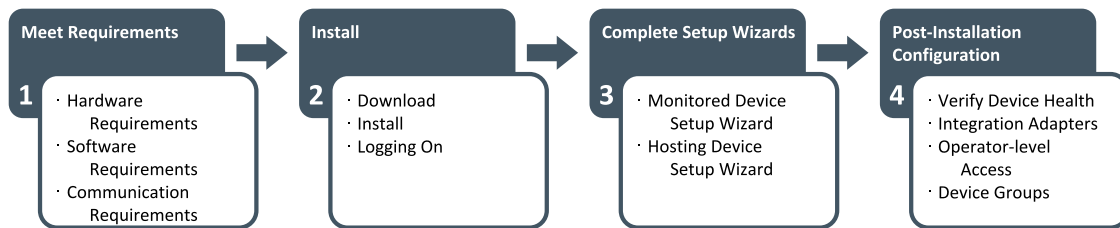
Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to techdocs_feedback@hpe.com.

Chapter 1: Understanding installation process and requirements

This chapter provides an overview of the Insight RS installation process and identifies the system requirements for the Hosting Device.

Perform the following steps for a first time installation of Insight RS on your Hosting Device.



Upgrade Insight Remote Support

If Insight RS is installed on your Hosting Device, see the upgrade instructions provided in the *HPE Insight Remote Support Upgrade Guide* at: www.hpe.com/info/insightremotesupport/docs.

Before getting started, review the following table. It lists the functionality that was available in earlier versions of Insight RS but is not currently available in Insight RS 7.6.

Table 1.1 Insight RS 5.x functionality not available in Insight RS 7.6

Functionality	Details
Hosting Device	<ul style="list-style-type: none"> All Microsoft Windows 2003 operating system versions will <i>not</i> be supported on any Insight RS 7.x versions.
Products that will <i>not</i> be supported by any 7.x version	<ul style="list-style-type: none"> HPE Enterprise Secure Key Manager HPE Secure Key Manager HPE Dynamic Smart Cooling HPE SAN Virtualization Services Platform HPE Modular Array HPE Enterprise Modular Array HPE Raid Array HPE Enterprise Storage Array M-series Switches (McData) Carrier-grade Servers (cx2620, cc3310) HP 9000 rp2400 series (A-Class), rp5400 series (L-Class), and D,K,R,T,V (Class) servers PA-RISC versions of HP 9000 SD-A and SD-B servers HPE Neoview Systems IBM AIX servers Sun Solaris servers

Table 1.1 Insight RS 5.x functionality not available in Insight RS 7.6, continued

Functionality	Details
Mission Critical Service Delivery (Insight RSA only)	<p>Capabilities to deliver the following mission critical services:</p> <ul style="list-style-type: none"> • HP-UX System Health Check assessments (not available within Insight RS 7.x, but available as a standalone client) • TAM-S and CCMon Services • Unreachable Device Notification

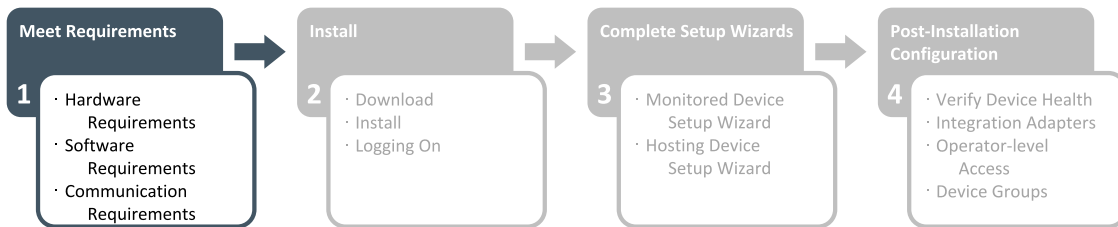
Fulfill Hosting Device system requirements

The Hosting Device must meet the hardware and software requirements defined in the *HPE Insight Remote Support Release Notes* and summarized in the Hardware, Operating System, Software, Access, and Communication Requirements sections below.

The Hosting Device can monitor a maximum of 3,500 devices (see ["Number of monitored devices supported" on the next page](#)). To monitor more than 3,500 devices, you can set up multiple Hosting Devices in your environment. However, to avoid duplicate reporting of events and data, make sure you **do not** monitor the same device by multiple Hosting Devices.

Important: Make sure the system date is set correctly on the Hosting Device.

Important: To protect your privacy, do not use sensitive information in the name of the Hosting Device server. The server name will be visible in the Insight RS Console and HPE Insight Online, and can be viewed by HPE support and your HPE Authorized Channel Partner.



Fulfilling hardware requirements

Insight RS is supported only on the following HPE ProLiant servers:

- For up to 2,500 devices, any HPE ProLiant G4 or above (x64 system) with at least 4 CPU cores and with Insight Management Agent or WBEM Provider support
- For 2,500 to 3,500 devices, any HPE ProLiant G7 or above (x64 system) with at least 4 CPU cores and with Insight Management Agent or WBEM Provider support

Note that ProLiant Gen8 MicroServers are supported as Hosting Devices.

Important: iLO port sharing is **not** supported on a ProLiant Gen8/Gen9 Hosting Device.

See the *HPE Insight Remote Support Release Notes* for more details about Insight Management Agent and Wbem Provider support.

The following tables outline the minimum and recommended Hosting Device specifications:

Important: If you are installing or retaining HPE Systems Insight Manager on the same Hosting Device, then the extra resources and requirements needed for this application should be added accordingly. See the *HPE Systems Insight Manager Installation and Configuration Guide for Windows* at <http://www.hpe.com/info/insightmanagement/docs> for details.

Important: When running the Hosting Device in a virtual environment, HPE recommends increasing the memory and disk space recommendations by 10% when the Virtual Machine (VM) is created. Do this for each VM added to the ProLiant.

Table 1.2 Hosting Device sizing requirements based on number of managed devices

	Memory Size	Free Disk Space
Up to 500 devices	Minimum 8 GB for new installations Recommended 8 GB, 12 GB if using SIM	2 GB during a new full installation 24 GB for operation ¹
Up to 2,500 devices	Minimum 12 GB for new installations Recommended 16 GB, 20 GB if using SIM	2 GB during a new full installation 64 GB for operation ¹
Up to 3,500 devices	Minimum 16 GB for new installations Recommended 20 GB, 24 GB if using SIM	2 GB during a new full installation 300 GB for operation (must be at least 150 GB free) ¹

¹The disk space requirements are affected by the number and type of devices if collections are configured (strongly recommended and in some case a requirement of the contract type). Please see the *HPE Insight Remote Support Release Notes* for details.

Number of monitored devices supported

This solution has been optimized to support up to 3,500 monitored devices per Hosting Device. If you need to monitor more than 3,500 devices, HPE recommends that you use multiple Insight Remote Support installations, either on multiple physical servers or installed on its own supported virtual machine.

Normally, each physical device counts as one device when calculating the overall maximum device number, e.g. a ProLiant server and its iLO 4 only count as a single device. However, there are some exceptions that need to be taken into account as listed below. The device count is based on the frequency and size of collections, and the Hosting Device resources required to gather the collections for the device type.

- HPE ProLiant Gen8 servers using the embedded iLO 4 capabilities when AHS collections are turned on, count as 5 devices (without AHS collections, each server counts as one device)
- Each networking switch counts as 4 devices
- Each HPE StoreVirtual 4xxx Storage Node counts as 30 devices
- Each HPE StoreAll Network Storage System counts as 4 devices
- Each Tape Library counts as 4 devices

- Each HPE 2000/MSA device counts as 4 devices
- Each HPE P6000 Enterprise Virtual Array counts as 8 devices
- Each VMware® vCenter™ server installation counts as 4 devices
- Any device that is configured as part of a SAN collection, adds an additional count of 4 devices

Configuration collection capabilities

HPE Insight Remote Support 7.6 has the ability to collect configuration information from your monitored devices managed centrally from the Hosting Device.

These services are initiated when the devices register and further collections are automatically scheduled by default. These configuration collections enable the following:

- HPE Support to provide improved technical support.
- Data collections provide HPE (or your nominated HPE Authorized Channel Partner) with information on the monitoring health of each of your devices. This is displayed in Insight Online if you have chosen this option.
- Certain HPE Proactive services have a mandatory requirement for remote support monitoring and collections enabled on all devices for the customer to receive all the features and service deliverables provided under the service. This means HPE is not obligated to provide delivery of proactive entitlements for disabled collections for these devices until such time as the remote support monitoring and collection functionality is restored.
- Optionally, if during installation or subsequently you have requested HPE or your preferred HPE Authorized Channel Partner to provide recommendations that may improve your environment.



Important: Dependent on the collection type, additional disk space needs to be allocated to allow configuration collections to operate correctly. Note, all collections have a number that are retained for historic records. Additionally, collections are compressed by a ratio of ten to one when they are retained but consideration for disk space should be given if multiple collections are run at the same time. The only exception is Active Health System (AHS) Collections that are not compressed. Please see "[Collection types and disk space requirements](#)" below for details on how to calculate the required disk space.

Table 1.3 Collection types and disk space requirements

	Schedule frequency (default schedule)	Average size per collection (compressed)	Number of collections retained
Active Health System (AHS) Collection			
Applicable for HPE ProLiant Gen8 and Gen9 servers only, independent if the server is using the embedded management capabilities in the iLO 4 or using a diagnostic agent installed on the operating system.			
HPE ProLiant Gen8 and Gen9	Weekly	25 MB	3
Server Basic Configuration Collection			
Windows and Linux on HPE ProLiant	Monthly	200 KB	5
VMware® ESX® and VMware® ESXi™ on HPE ProLiant	Monthly	75 KB	5
HP-UX	Monthly	800 KB	5

Table 1.3 Collection types and disk space requirements, continued

	Schedule frequency (default schedule)	Average size per collection (compressed)	Number of collections retained
HPE Integrity Superdome 2 Onboard Administrator	Monthly	10 KB	5
HPE Integrity Superdome X Onboard Administrator	Monthly	18 KB	5
HPE Integrity Superdome X partition (SLES, RHEL, Windows 2012 R2, VMware vSphere) (size per partition)	Monthly	18 KB	5
OpenVMS	Monthly	35 KB	5
Onboard Administrator for c-class Enclosures	Monthly	20 KB	5
Virtual Connect Modules	Monthly	10 KB	5
StoreVirtual (P4000) Family Configuration Collection			
HPE StoreVirtual 4xxx (P4000 SAN Solutions)	Daily	900 KB	7
Network Configuration Collection			
HPE ProVision-based Switches (E-Series/ ProCurve)	Weekly	100 KB	5
HPE ComWare-based Switches (A-Series/ 3Com)	Weekly	13 KB	5
HPE Networking Routers	Weekly	18 KB	5
VMware vCenter Server Collection			
This collection size includes all the configuration information from VMware vCenter and all of its virtual machines. The size varies based on the size and complexity of the cluster being monitored. More virtual machines in the cluster will increase the size.			
VMware vCenter Server	Weekly	5 MB	3
Storage Configuration Collection			
P6000 Enterprise Virtual Arrays	Weekly	250 KB	5
HPE StoreFabric SAN switches	Weekly	100 KB	5
HPE StoreEasy Storage (Commercial NAS)	Monthly	450 KB	5
HPE ESL/HPE StoreEver EML/HPE StoreEver MSL	Weekly	25 KB	5
HPE SureStore 2000 (Modular Smart Arrays)	Weekly	100 KB	5
InfiniBand switches	Weekly	100 KB	5
SAN Configuration Collection			
These collections are in addition to the collections listed above but are only required to fulfill the deliverables of a SAN Proactive Services contract			
HP-UX	Weekly	800 KB	5

Table 1.3 Collection types and disk space requirements, continued

	Schedule frequency (default schedule)	Average size per collection (compressed)	Number of collections retained
OpenVMS	Weekly	35 KB	5
Windows/Linux on HPE ProLiant	Weekly	200 KB	5
Virtual Connect Modules	Weekly	10 KB	5
P6000 Enterprise Virtual Arrays	Weekly	250 KB	5
HPE ESL/HPE StoreEver EML/HPE StoreEver MSL	Weekly	25 KB	5
HPE StoreFabric SAN switches	Weekly	100 KB	5
HPE StoreVirtual 4xxx (P4000 SAN Solutions)	Weekly	900 KB	5
HPE SureStore 2000 (Modular Smart Arrays)	Weekly	100 KB	5
Virtual Library Systems	Weekly	5 KB	5
InfiniBand switches	Weekly	100 KB	5
Operational collections			
This collection is manual on request from HPE Support.			
Support Data Collection	On demand	10 MB	2

Fulfilling operating system requirements

Insight RS 7.6 can be installed on a Windows HPE ProLiant server or Windows virtual guest on a VMware, Citrix or Hyper-V virtual machine.



Important: SIM and Insight RS 7.6 support different versions of the Microsoft Windows operating system. If you intend to synchronize Insight RS with SIM, make sure the Hosting Device operating system is supported by both SIM and Insight RS. For SIM operating system support, see the *HPE Insight Management Support Matrix* at: <http://www.hpe.com/info/insightmanagement/docs>.

Supported Microsoft Windows operating systems

The following Microsoft Windows operating system versions are supported with English, French, Italian, German, Spanish, Dutch, Traditional Chinese, Simplified Chinese, Korean, and Japanese International Server. Operating systems are **not** supported unless included in the below list.



Important: Only 64-bit (x64) versions of Microsoft Windows operating systems are supported.

- Microsoft Windows Server 2012 R2
 - Standard Edition
 - Datacenter Edition
- Microsoft Windows Server 2012

- Standard Edition
- Datacenter Edition
- Microsoft Windows Server 2008 R2 for x64 including Service Pack 1
 - Standard Edition
 - Enterprise Edition
- Microsoft Windows Server 2008 Service Pack 2 for x64
 - Standard Edition
 - Enterprise Edition
 - Datacenter Edition
- Microsoft Windows Web Server 2008 Service Pack 2 for x64

Installing Insight RS on an HPE StoreEasy Storage system is supported when Insight RS monitors only the StoreEasy Storage system and the storage presented to the system.

- Windows Storage Server 2012 R2
 - Standard edition
- Windows Storage Server 2012
 - Standard edition
- Windows Storage Server 2008 R2
 - Standard edition
 - Enterprise edition
- Windows Storage Server 2008 Service Pack 2
 - Standard edition
 - Enterprise edition



Important: Installing or upgrading Insight Remote Support on a Microsoft Windows server configured as a domain controller is not supported.



Important: Support for Microsoft Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012 is limited to the full server version only and is not available for the core version as much of the required functionality is unavailable in this version. This also excludes Windows Server core versions running the Hyper-V role.

Supported Microsoft Hyper-V server

Hyper-V virtual machines are supported if the Microsoft Windows virtual guest operating system is a supported Hosting Device operating system.

The following Microsoft Windows versions are supported:

- Microsoft Hyper-V Server 2012 R2
- Microsoft Windows Server 2012 R2 using Hyper-V role
- Microsoft Hyper-V Server 2012

- Microsoft Windows Server 2012 using Hyper-V role
- Microsoft Windows Server 2008 R2 using Hyper-V role

Supported VMware operating systems

The following VMware versions are supported:

- VMware vSphere ESXi 6.0
- VMware vSphere ESXi 5.5 including Update versions
- VMware vSphere® ESXi 5.1 including Update versions
- VMware ESXi Server 4.0, 4.1, 5.0
- VMware ESX Server 4.0 and 4.1 including Update versions

Support is provided on a VMware ESX or ESXi supported HPE ProLiant server utilizing 64-bit VMware Guests running Windows Server 2008 or 2012 variants as described in "[Supported Microsoft Windows operating systems](#)" on page 14.

Support is provided for the following VMware vSphere® capabilities when the Hosting Device is installed in a VMware Windows virtual machine:

- VMware vSphere® vMotion® when the Hosting Device is moved to another server in the same cluster
- VMware vSphere Fault Tolerance to provide Hosting Device hardware resilience using two servers running in parallel for continuous fault tolerance for an Insight Remote Support installation. For details of this capability please refer to <http://www.vmware.com/products/vsphere/features/fault-tolerance.html>



Important: VMware vCenter features that are not supported on a Virtual Machine based Hosting Device include VM cloning, VM copying and Physical to Virtual (P2V) Migrations with the VMware vCenter Converter. Supported VMware vCenter features include VMware Distributed Resource Scheduler (DRS) and VMware High Availability (HA).

Supported Citrix XenServer operating systems

The following Citrix XenServer versions are supported:

- Citrix XenServer 6.0, 6.1 and 6.2 including Update versions
- Citrix XenServer 5.5 and 5.6 including Update versions

Fulfilling software requirements



Important: Make sure the system date is set correctly on the Hosting Device.

Install web browsers

The following web browsers are supported for Insight RS:

- Microsoft Internet Explorer, versions 9.x, 10.x and 11.x
- Mozilla Firefox, versions 42.x
- Google Chrome, version 48.x

Install .NET Framework

Microsoft .NET Framework 3.5 or later is required.

To verify your version of the .NET Framework, complete the following steps:

Windows 2008

1. On the Hosting Device, open the **Server Manager**.
2. In the Server Manager, click **Features** and verify that .NET Framework 3.5.x or later is listed in the right pane.
3. If the .NET Framework is not listed, click the **Add Features** link.
4. In the Select Features screen, expand **.NET Framework 3.5.x Features**.
5. Select the .NET Framework 3.5.x check box, and then click **Next**.
6. In the Confirm Installation Selections screen, review the selections and click **Install**.
7. When the installation completes, click **Close**.

Windows 2012

1. On the Hosting Device, open the **Server Manager**.
2. In the Server Manager, click **Local Server** and verify that .NET Framework 3.5.x or later is listed in the Roles and Features section of the right pane.
3. If the .NET Framework is not listed, click **Tasks** → **Add Roles and Features**.
4. On the Select Features screen of the Add Roles and Features Wizard, expand **.NET Framework 3.5.x Features**.
5. Select the .NET Framework 3.5.x check box, and then click **Next**.
6. In the Confirm Installation Selections screen, review the selections and click **Install**.
7. When the installation completes, click **Close**.

Perform a Windows Update

HPE recommends performing a Windows Update on the Hosting Device before installing Insight RS. Make sure you restart the Hosting Device after the updates are installed.

The Insight RS installer's prerequisite checker prevents installation if any software updates have queued file rename or deletion operations waiting for the next reboot. The best practice is to reboot prior to beginning the Insight RS installation, in particular if Windows Update applied any software patches.

Fulfilling access requirements

To install Insight RS, you must have *administrative rights* to Microsoft Windows on the Hosting Device. Insight RS requires use of the same Windows account on the Hosting Device to install and configure Insight RS.



Important: Due to enhanced security features in Windows 2008 and later, HPE recommends that you run the installation as user administrator or as a user in the Administrators group.

Insight RS should only be installed by a user who is logged on to the Hosting Device through the system console or a console-mode Remote Desktop Connection (RDC) session. Do not attempt to install Insight RS through a non-console mode RDC session.

To access the Hosting Device remotely with Windows RDC, use one of the following console-mode switches:

- When connecting from a Windows XP, Windows 2000, or Windows 2003 system, use the `/console` switch:

```
c:\windows\system32\mstsc.exe /console
```

- When connecting from a Vista, Windows 2008, Windows 2012, or Windows 7 system, use the `/admin` switch:

```
c:\windows\system32\mstsc.exe /admin
```

Fulfill networking requirements

Make sure the following network requirements are met before installing Insight RS:

- IPv6 is not supported and needs to be disabled on the Hosting Device. Insight RS only supports the IPv4 networking protocol.
- Make sure your Hosting Device has a valid static IP address, and that it is connected to your network. Dynamic IP addresses are **not** supported. Changing the static IP address of the Hosting Device after Insight RS installation is **not** supported and requires reinstallation of Insight RS.



Note: Network Address Translation (NAT) is not supported for communications between the Hosting Device and monitored devices.

Fulfill communication requirements

There are three communication paths within Insight RS that require settings to your firewall. Make sure that the correct firewall openings are configured to allow communication between the components.

For a complete list of ports used by Insight RS, see the *HPE Insight Remote Support Security White Paper* at www.hpe.com/info/insightremotesupport/docs.

SSLv3 is disabled by default in Insight RS, but it can be re-enabled with an `rsadmin` command. With SSLv3 disabled, Insight RS uses Transport Layer Security (TLS) for communication. Insight RS attempts to communicate through the most secure protocol available (today that is TLS 1.2), and if that does not work Insight RS tries the previous version (TLS 1.1) and so on until it finds protocol that works. If it cannot find a protocol, the communication fails.

For more details about Insight RS communication, see the *HPE Insight Remote Support Security White Paper* or the *HPE Insight Remote Support Security Presentation*.

Configuring communication from a web browser to Insight RS

Port 7906 (HTTPS)—Open port 7906 on the Hosting Device to access the Insight RS user interface on the Hosting Device from other systems inside of the same network. Also make sure that Windows firewall allows the connection to port 7906.

Configuring communication from the Hosting Device to HPE

Insight RS communicates directly with the HPE Data Center through the firewall or web proxy server (if a web proxy server is in use).

Insight RS supports connecting directly to the Internet or connecting through a proxy server. Insight RS *does not* support proxies using proxy auto-configuration scripts, NTLM (NT LAN Manager) authentication, or Kerberos authentication.

The Insight RS configuration may fail if your firewall or security software filters network communication between the Hosting Device and the HPE Data 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 Hosting Device and the HPE Data Center. Verify that it passes any HTTP standard protocol between the Hosting Device and the HPE Data Center, so that it meets the communication requirement (TCP 443 outbound with established back).

Configure the following port and alias in your firewall:

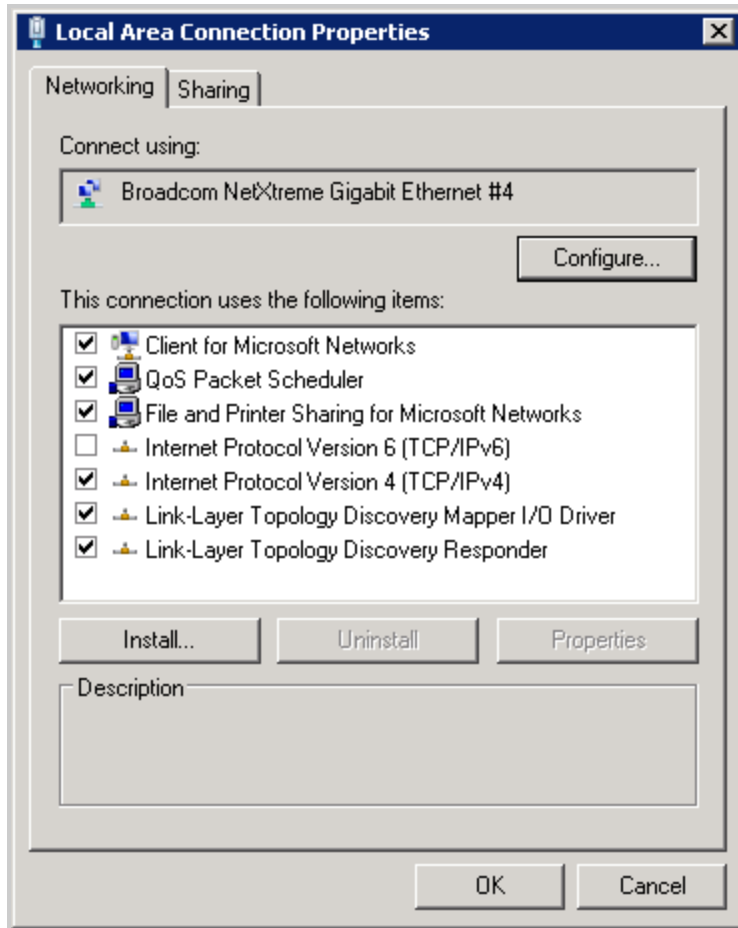
- **Port 443 (HTTPS)**—Insight RS communicates over HTTPS/443 to submit incidents to and retrieve warranty and contract information from HPE. HTTPS provides encryption for confidentiality of software configuration data collected from the Hosting Device and transferred to HPE. HPE recommends you configure your firewall before installing Insight RS.
- **api.support.hpe.com**—Set your firewall rules to allow access to HPE using the alias `api.support.hpe.com`. All data sent to HPE is through an HTTPS connection to the destination `api.support.hpe.com`. This destination is a virtual IP address that is automatically routed to an active server in one of the HPE Data Centers. HPE strongly recommends configuring only the alias. If your policies require IP addresses, see the *HPE Insight Remote Support Security White Paper* for details.

Configure the Hosting Device to use DNS

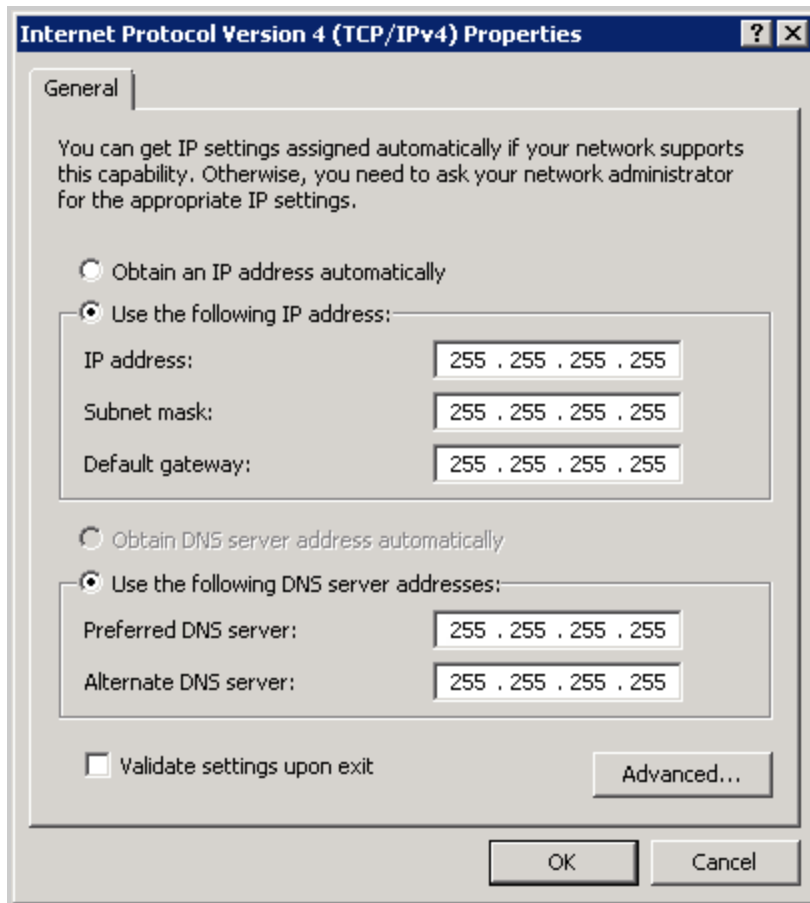
HPE Insight RS uses redundant data centers to provide resiliency and load balancing. Global Server Load Balancing (GSLB) redirects traffic based on server load and availability. GSLB uses Domain Name System (DNS) to return the IP address of an available server. The Hosting Device must use DNS to communicate with the redundant sites. If you configure IP addresses in the hosts file instead of using DNS, you will lose service when the GSLB redirects traffic.

To configure the Hosting Device to use Domain Name System (DNS), complete the following steps:

1. Log on to the system as a member of the Administrators group.
2. Click **Start** → **Control Panel**.
3. In the Network and Internet category, click the **View network status and tasks** link.
4. Click the link for Connections, for example: **Local Area Connection, Ethernet**.
5. Click **Properties**. The Properties screen appears.



6. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. The Internet Protocol Version 4 (TCP/IPv4) Properties screen appears.



7. Click one of the following options:
 - **Obtain an IP address automatically** (if appropriate for the your environment)
 - **Use the following IP address**
8. Specify the Hosting Device's IP address fields and the DNS server(s) available in your environment.
9. Click **OK**, click **OK**, and then click **Close**. Close the Network and Sharing Center.
10. Verify the settings by performing the `nslookup` command in a DOS window:

```
nslookup api.support.hpe.com
```

The output should show the IP address of the DNS server you typed.

Verify Hosting Device connectivity with HPE

HPE recommends verifying connectivity to the HPE Data Center before installing Insight RS to avoid installation failures due to connectivity problems.

During installation, there is no specific connectivity check for Insight RS. The Hosting Device Setup Wizard contains a connectivity test. If there are any problems the first time Insight RS attempts to connect to the HPE Data Center, the test will fail. Therefore, verifying connectivity before installation reduces the chance of connectivity failure.

Perform the following connectivity test:



Important: This test does *not* verify that the Hosting Device or Insight RS configurations will actually submit collections or events, but it does validate that the Hosting Device itself can communicate to HPE's servers before you continue configuring the Hosting Device.

- `api.support.hpe.com`

If you are using a proxy server, verify connectivity between the Hosting Device and the HPE Data Center by using a web browser to connect to the following site: <https://api.support.hpe.com/v1/version/index.html>. The response should be a version number, for example: `##.##.##.##`.



Note: This version number will *not* match the version of the software which you are installing.

If you are not using a proxy server, verify connectivity to `api.support.hpe.com` by using telnet. From a command prompt, type the command `telnet api.support.hpe.com 443`. You will see a connection established, which confirms connectivity.

Configuring communication between the Hosting Device and monitored devices

The firewall settings between the Hosting Device and the monitored devices also need to be opened. This could be the Windows firewall and, if one exists, the firewall between the Hosting Device and the monitored devices. See the *HPE Insight Remote Support Security White Paper* for the ports needed for your device types.

Depending on your monitored device type, your Hosting Device will collect event and configuration data from the monitored device through one or more of the following: SNMP, WBEM, ELMC, and/or P6000 Command View. The instructions to configure SNMP on the Hosting Device are in "[Install SNMP on the Hosting Device](#)" below. The instructions to configure communications on your monitored device are in the chapter specific to the device in the *HPE Insight Remote Support Monitored Devices Configuration Guide*. If you fail to configure these protocols properly, events and configuration collections will not reach the Hosting Device and therefore will not be communicated by the Hosting Device to HPE for support.

Install SNMP on the Hosting Device

SNMP is required for Insight RS to monitor device types that use SNMP for communication (see the *HPE Insight Remote Support Monitored Devices Configuration Guide* for specific devices). SNMP *must* be installed on the Hosting Device. SNMP is provided by Microsoft and, if not already installed on your Hosting Device, can be installed through the Server Manager.

To install SNMP on your Hosting Device, complete the following steps:

1. On the Hosting Device, open the **Server Manager**.
2. In Server Manager, do one of the following:
 - For Windows 2008, go to **Action** → **Add Features**.
 - For Windows 2012, go to **Manage** → **Add Roles and Features**.
3. Scroll down to **SNMP Service**. If it is not selected, select the check box and click **Next**. Follow the wizard to install the service.

Configure Traps

Once you have SNMP installed on your Hosting Device, configure it to receive packets from your monitored devices by completing the following steps:

1. On the Hosting Device, click **Start** → **Administrative Tools** → **Services**.
2. Double click **SNMP Service** to open the Properties window.
3. On the **Traps** tab, make sure a community string is listed, and make sure localhost and 127.0.0.1 exists as a trap destination.
4. On the **Security** tab, choose one of the following options:
 - **Accept SNMP packets from any host.**
 - **Accept SNMP packets from these hosts** and use the **Add** feature to add your monitored devices to the list.
5. Click **OK** to save your changes and close the SNMP Service Properties configuration window.

Set SNMP Trap service startup type

Insight RS requires the SNMP Trap service to start automatically upon boot. Configure the SNMP Trap service by completing the following steps:

1. On the Hosting Device, click **Start** → **Administrative Tools** → **Services**.
2. Double click **SNMP Trap** to open the Properties window.
3. Click the **General** tab.
4. From the **Startup type** drop-down list, select **Automatic**.
5. If the service is not running, click **Start**.
6. Click **OK** to save your changes and close the SNMP Trap Properties configuration window.

Update WMI Mapper to monitor Windows Server 2012 devices

If you want to take advantage of Insight RS 7.6's support for monitored devices running Windows Server 2012, you need to ensure that the WMI Mapper is updated to version 7.2.3 or later. This version of WMI Mapper is included in recent SIM distributions, and it is also available as a package which can be installed from the Insight RS Software Updates screen.

To make sure you have a supported version of WMI Mapper, complete the following steps:

1. To verify the installed version of WMI Mapper, navigate to **Start** → **Control Panel** → **Programs and Features**. Check the **Installed** column for the package **Pegasus WMI Mapper**. If version 7.2.3 or later is installed, no further action is required. If 7.2.3 or later is not installed, proceed to the next step.
2. To install or upgrade WMI Mapper from the Insight RS Console:
 - a. Log on to the Insight RS Console.
 - b. In the Insight RS Console, navigate to **Administrator Settings** → **Software Updates**.
 - c. Select the WMI Mapper package in the table.

- d. Select the **Available Version** tab below the table, and then click **Install**. Note that the Insight RS service will be stopped during and restarted after the WMI Mapper installation, so the web interface will indicate the need to log out.

Monitor the Hosting Device

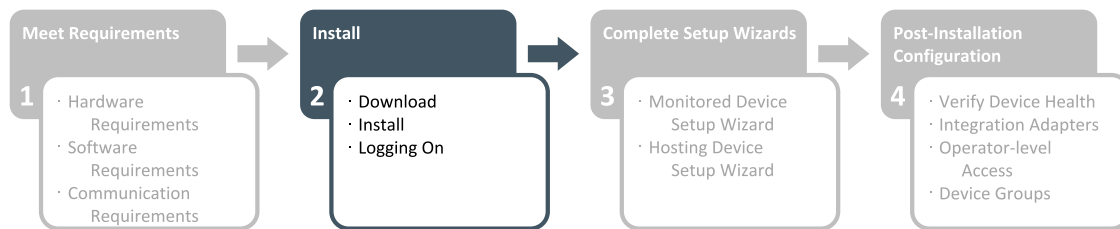
Monitor the physical server that the Insight RS software is installed on. The software required to monitor the Hosting Device depends on the ProLiant generation and operating system installed. For information about configuring your Hosting Device for monitoring, see the *HPE Insight Remote Support Monitored Devices Configuration Guide*.

Chapter 2: Installing Insight Remote Support for the first time

This chapter guides you through the Insight RS installation process.

At this point, step 1 below is complete. Perform step 2 to install and configure Insight RS on your Hosting Device.

If a previous version of Insight RS is installed on your Hosting Device and you want to upgrade, see the *HPE Insight Remote Support Upgrade Guide*.



Download and install Insight Remote Support

Before beginning the Insight RS installation, you need to download the Insight RS software package from the HPE Software Depot at:

h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=REMOTESUPPORT.

To download Insight RS, complete the following steps:

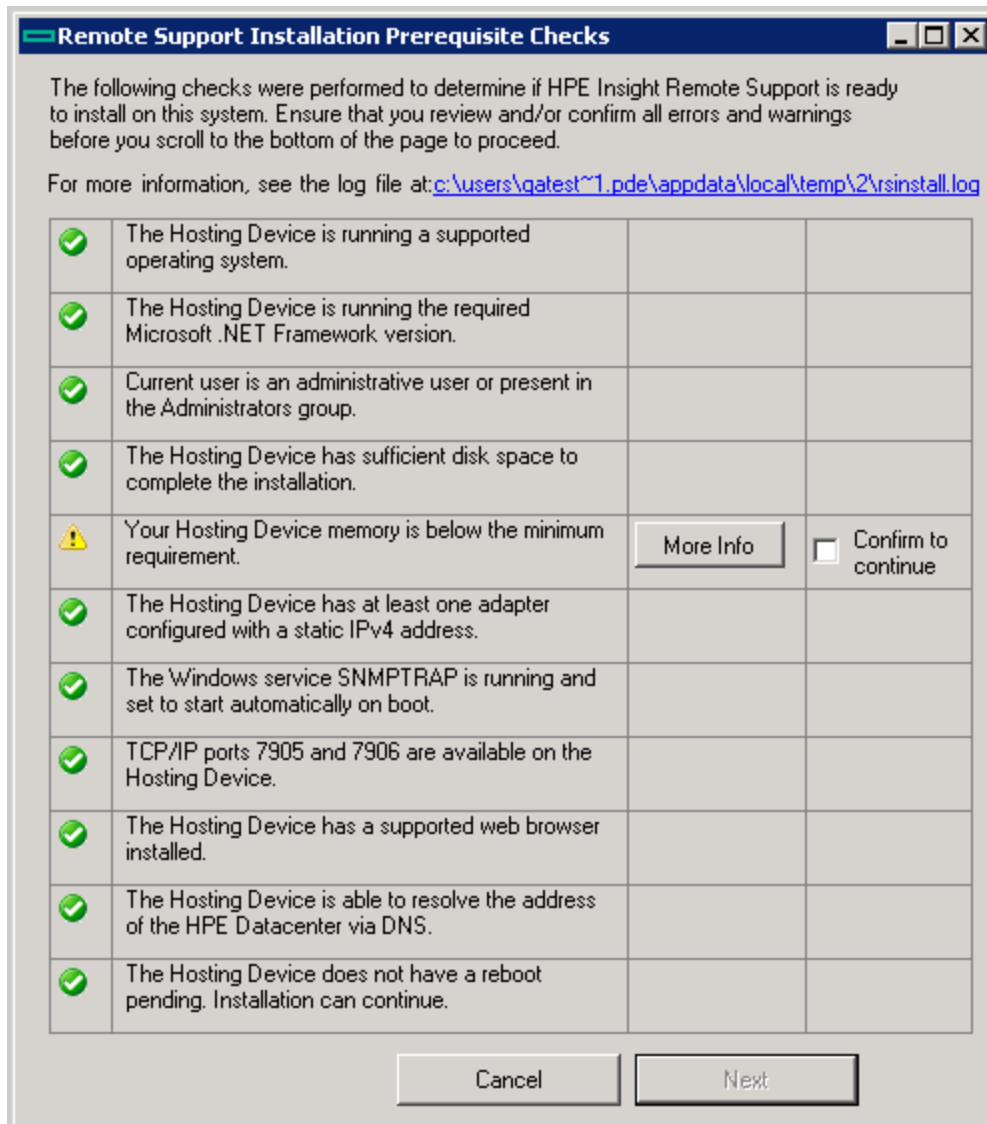
1. Log on to your Hosting Device using an Administrator account. You must log on as an Administrator or as a user that is a direct member of the Hosting Device's Administrators group.
2. Download the .exe file containing the Insight RS installation files from the HPE Software Depot.



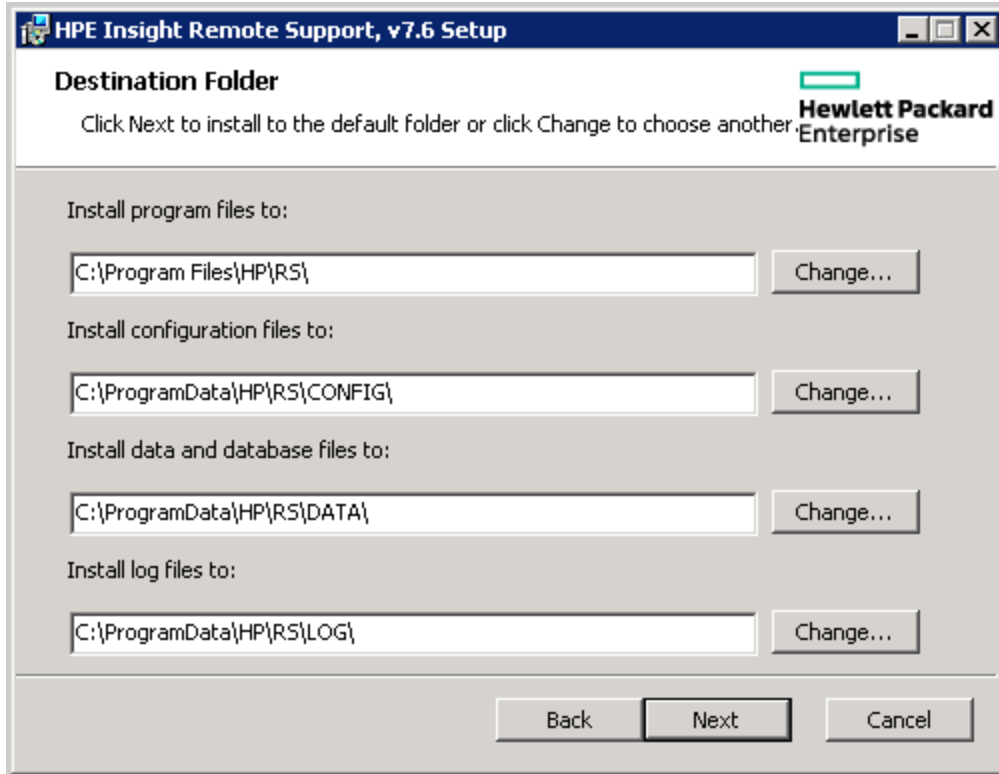
Important: If you use any process monitoring tools to monitor the status of the HPRS services on the Insight RS Hosting Device, HPE recommends you pause the monitoring of HPRS services before installing or upgrading Insight RS. If left enabled, the monitoring tool may restart the HPRS services before the install or upgrade completes, resulting in a corrupted Insight RS install.

To begin the installation, complete the following steps:

1. On the Hosting Device, right-click the self-extracting .exe file that you downloaded from the HPE Software Depot, and choose **Run as administrator**. After the files are extracted, the installation wizard launches and performs a prerequisite check.



2. If all of the prerequisites are met, click **Next**. If any prerequisites are not met, do one of the following:
 - If the problem is a critical failure, exit the installer, resolve the issue, and then restart the installer.
 - If the problem is a warning, either exit the installer to resolve the issue or check the **Confirm to continue** check box and click **Next**.
3. On the Welcome screen, click **Next**.
4. Review the license agreement, select the **I accept the terms in the License Agreement** check box, and click **Next**. The Destination Folder section of the wizard appears.



5. On the Destination Folder screen, you can change the default locations for program files, configuration files, database files, and log files. Do one of the following:
 - To install Insight RS to the default destination folders, click **Next**.
 - To install files to other folders, click **Change**, select a new destination folder, and click **OK**. Repeat for any install folder you want to change, and when finished, click **Next**.

Installation directories must be seen by Microsoft Windows as local drives and not network drives. Insight RS cannot be executed from a single shared disk by multiple computers.



Note: If you have a large number of devices to monitor, HPE recommends you configure the destination folder for the database and log files to be on different volumes to increase the performance of Insight RS.

6. Click **Install**. When the installation is nearing completion, the following message appears: *Install complete. Waiting up to 600 seconds for the Insight RS Console to become available.*
7. When the installation completes, click **Finish** to exit the installation wizard.



Important: After installation, if the `rsadmin` command is not recognized when run from a command prompt, log off then log back on to Windows. This forces Windows to apply the new modified PATH variable. A reboot is *not* required.

Locating log files

If you encounter any problems during installation, view the `rsinstall.log` and the `hprs_msi_install-0.log` files. During installation, these log files are located in the `%TEMP%` folder. After a successful installation,

these log files are copied to the C:\ProgramData\HP\RS\LOG\ folder. This is the default log file location, and it will be different if you chose a different log file location during installation.



Note: The C:\ProgramData folder is a hidden folder, so you may need to set your folder options to show hidden folders.

Logging on to the Insight RS Console

After installation, wait a few minutes before attempting to log on to the Insight RS Console to make sure the hosting device is ready for registration. If you try to log on immediately, you will be prompted by a message informing you that the system is starting up and to try again later. If you do this, you must force a refresh on the Insight RS Console (or open a new browser window) to avoid the browser cache.

Point your browser to: `https://<hosting_device_ip_or_fqdn>:7906`.

Log on as an Administrator or as a user that is a direct member of the Hosting Device's Administrators group. The first time you log on to the Insight RS Console you need to log on as an Administrator, but you can enable access for any system account. For more information, see "[Enable operator-level user authentication](#)" on [page 59](#).

Users must be allowed to log on locally or they will not be able to access the Insight RS Console; this is true in a domain or in a workgroup environment.



Important: The `rsadmin` command is a powerful tool that can be used to manage the Insight RS application. The `rsadmin` command is executable by any local users on the Hosting Device. HPE recommends that you restrict access to the Hosting Device to only authorized users to prevent unwanted changes to the Insight RS configuration on the Hosting Device.

If the account is not an Administrator account you will not be able to access the Administrator Settings, Discovery or Solution Manager screens in the Insight RS Console.

Note that after 30 minutes of inactivity the Insight RS Console times out the session and the user is logged off.



Important: Your web browser language settings determine the language displayed in the Insight RS Console. When connecting to Insight RS Console from a remote system, configure your web browser language settings to match the language you used when you installed Insight RS.

Known issue: Cannot log on to the Insight RS Console as an administrator

Issue: You are using a domain user account. This account is a member of a domain group which in turn is a member of the domain Administrators group. User Account Control (UAC) is turned on.

Example:

You cannot log on to the Insight RS Console with user `MYDOMAIN\myusername` and,

- `MYDOMAIN\myusername` is a member of the group `MYDOMAIN\specialusers`.
- `MYDOMAIN\specialusers` has been added to the `MYDOMAIN\Administrators` group.
- UAC is turned on.

Suggested action:

Any of the following actions enable you to log on as an Administrator:

- Turn off UAC on the Hosting Device.
- Add your user account to a local Administrators group on the Hosting Device. For example, add MYDOMAIN\myusername to the local HostingDevice\Administrators group.
- Add your user account directly to the domain Administrators group. For example, add MYDOMAIN\myusername to the MYDOMAIN\Administrators group directly.
- Create a new local Administrators account and use that to log on to the Hosting Device. For example, create an Administrative account named HostingDevice\AdminAccount and log on with that.

Resolve certificate warning

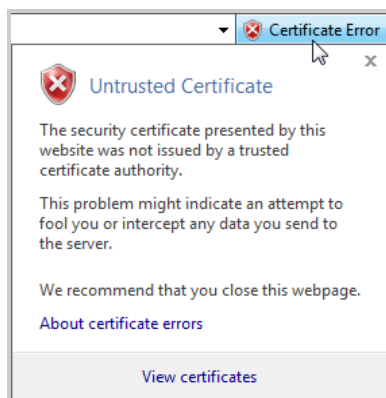
When you point your browser (Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome) to the Insight RS Console, a certificate error message appears. To resolve the security warning for your Internet browser, complete the following steps:



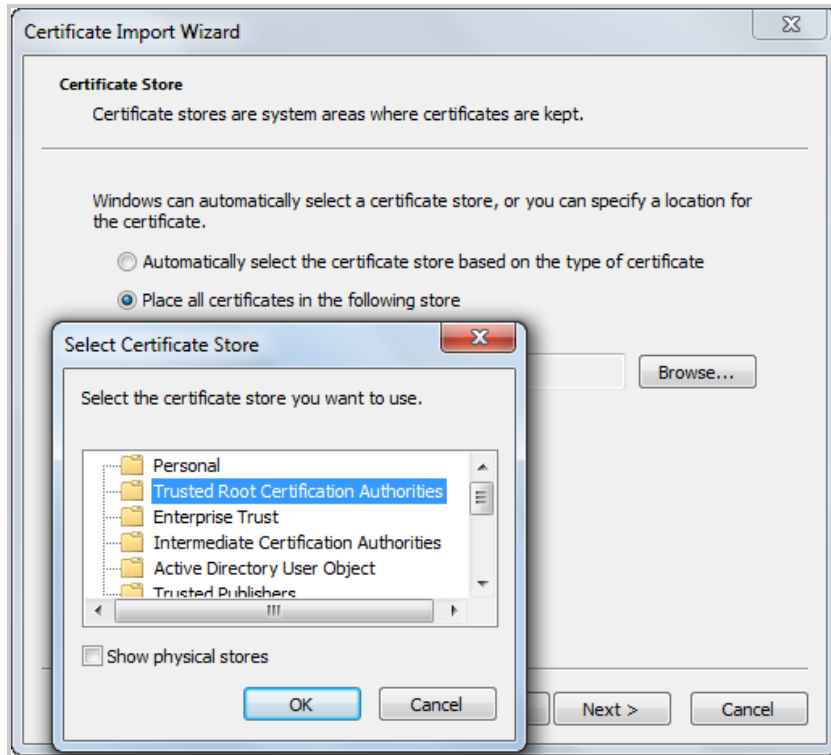
Note: The desktop shortcut installed on the Hosting Device points to the localhost. If using the desktop shortcut to start the Insight RS Console, change the properties of the shortcut to use the Hosting Device's IP address or FQDN for the certificate steps below to work correctly.

Internet Explorer

1. Click the **Continue to this website (not recommended)** link.
2. In the address bar, click **Certificate Error**. The Untrusted Certificate window appears.



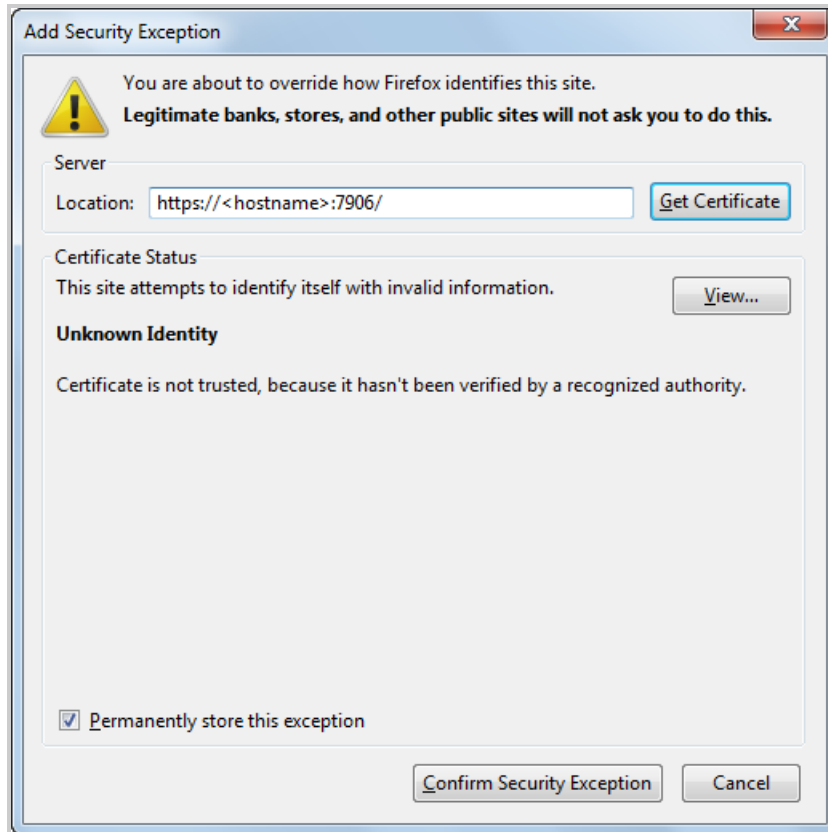
3. Click **View certificates**.
4. In the Certificate dialog box, click **Install Certificate**.
5. In the Certificate Import Wizard, click **Next**.
6. Click the **Place all certificates in the following store** option.
7. Click **Browse**. The Select Certificate Store window appears.



8. Select **Trusted Root Certification Authorities** and click **OK**.
9. Click **Next** and **Finish**. The Security Warning dialog box appears.
10. Click **Yes** to confirm you want to install the certificate.

Mozilla Firefox

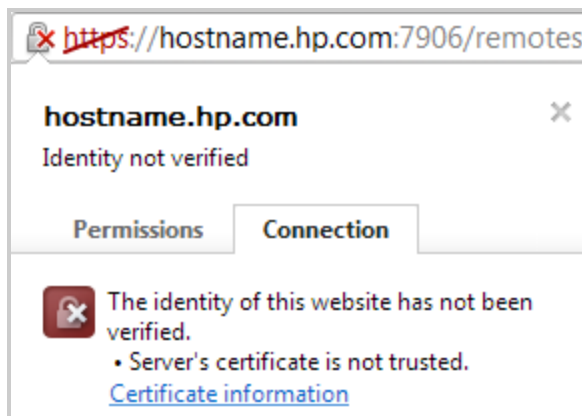
1. Click the **I Understand the Risks** link to expand the section and click **Add Exception**.
2. In the Add Security Exception dialog box, type `https://<hosting_device_ip_or_fqdn>:7906/` into the Location field or continue to the next step if the information is correct.



3. Click **Confirm Security Exception** to resolve the security warning.

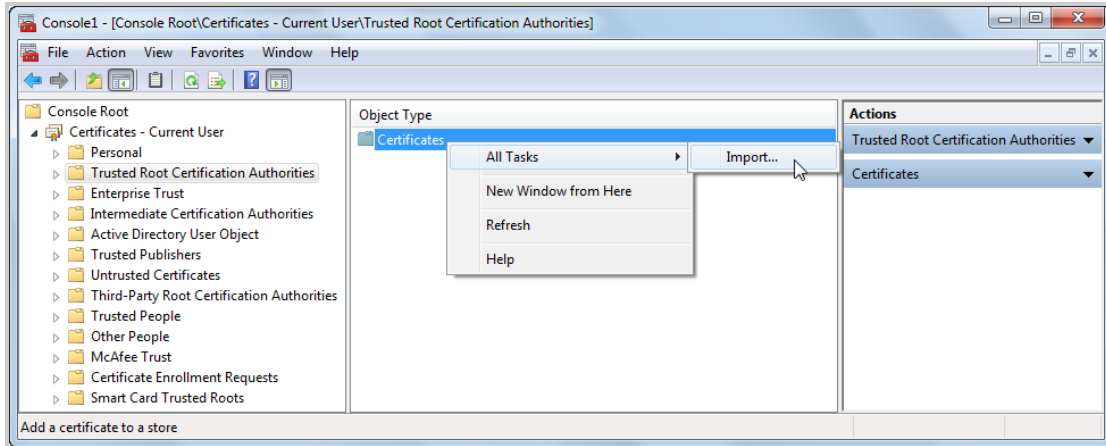
Google Chrome

1. On the *Privacy error* screen that appears, click the “lock with the red X” icon in the menu bar, and choose “Certificate information”.

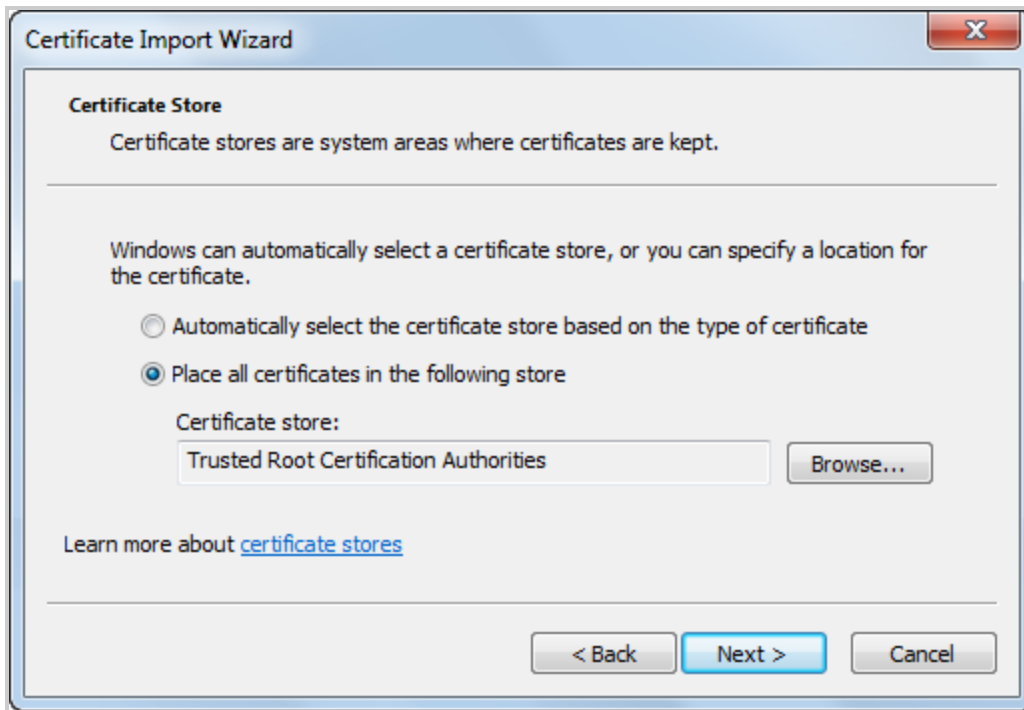


2. In the Certificate dialog box, click the **Details** tab and then click **Copy to File**. The Certificate Export Wizard appears.
3. Proceed through the wizard and save the certificate. When complete, click **OK** to close the Certificate dialog box.
4. Use the Microsoft Management Console to import the certificate as a trusted root certificate:

- a. On the Start menu, click **Run**, type **MMC**, and then click **OK**. Microsoft Management Console opens with an empty console.
- b. From the console, choose **File** → **Add/Remove Snap-in**.
- c. In the **Available snap-ins** pane, select **Certificates** and click **Add**.
- d. In the **Certificates snap-in dialog box**, select how you want to manage certificates and click **Finish** and then click **OK**.
- e. In the left menu, select **Trusted Root Certification Authorities**. In the **Object Type** pane, right-click **Certificates** and choose **All Tasks** → **Import**.



The Certificate Import Wizard appears.

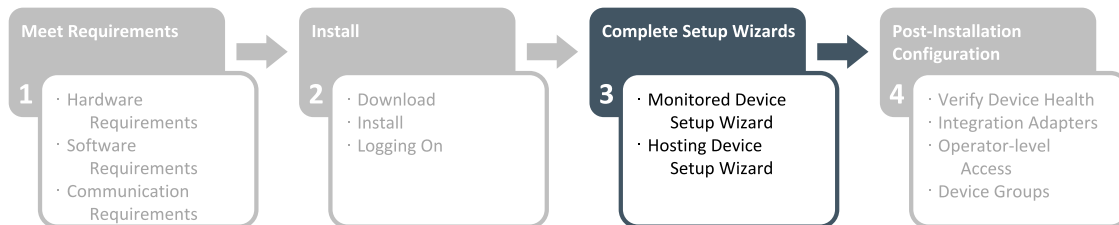


- f. In the **Certificate Import Wizard**, import the certificate you saved in step 3. Place the certificate in the **Trusted Root Certification Authorities** store.
- g. Click **Finish**.

Chapter 3: Completing the Setup Wizards

This chapter guides you through the Insight RS setup process.

At this point, steps 1 and 2 below are complete. Perform step 3 to complete the setup wizards.



When you first open the Insight RS Console, you must complete the Setup Wizards. There are two Setup Wizards: the Monitored Device Setup Wizard checks the readiness of the devices you want to monitor, and the Hosting Device Setup Wizard allows you to enter default settings about your environment. HPE recommends you complete the Monitored Device Setup Wizard first and let it run in the background while you complete the Hosting Device Setup Wizard.

Access the Insight RS Console through a web browser at: https://<hosting_device_ip_or_fqdn>:7906. Log on to the Insight RS Console using an Administrator account. You can log on to the Insight RS Console using any system account, but if the account is not an Administrator account you will not be able to access the Administrator Settings, Discovery or Solution Manager screens in the Insight RS Console.

Important: The Setup Wizards are not available in the main menu after you complete them. You can update the settings elsewhere in the Insight RS Console if necessary. If you need to access the wizards again, use the following URL: https://<hosting_device_ip_or_fqdn>:7906/remotesupport/command/viewWizards/.

On the Insight Remote Support Setup Wizard screen, you can:

- Complete the Monitored Device Setup Wizard to discover the devices you want to monitor. For more information, see "[Complete the Monitored Device Setup Wizard](#)" below.
- Complete the Hosting Device Setup Wizard to configure the Hosting Device. For more information, see "[Complete the Hosting Device Setup Wizard](#)" on page 40.

Complete the Monitored Device Setup Wizard

The Monitored Device Setup Wizard checks whether Insight RS can communicate with devices in your environment based on the configured credentials and verifies the devices are ready to be monitored by HPE Insight Remote Support. The Monitored Device Setup Wizard can be left unattended for large environments. The results can be viewed in the final screen of the wizard or on the Discovery screen in the Insight RS Console.

The left pane displays each step in the wizard and highlights the current step in green. Complete the information in each step and click **Next** to continue. Return to any step in the wizard by clicking **Previous** until you reach the desired step.

Insight RS checks every device's warranty and contract to make sure it has a valid HPE warranty or contract. If a device has no HPE warranty or contract, the monitoring health indicator in the Insight RS Console will be red. If this is red, then no service events will be analyzed or sent to HPE.

Configure your devices

Before your devices can be monitored by Insight RS, they need to be configured to communicate with the Hosting Device. For information about configuring your specific device type, refer to the *HPE Insight Remote Support Monitored Devices Configuration Guide* at: www.hpe.com/info/insightremotesupport/docs.

Configure protocol access credentials

On the Discovery Access Credentials screen, configure protocol credentials for the devices in your environment.



Note: This information can be modified on the **Discovery** → **Credentials** tab.

Each device in your environment requires protocols that Insight Remote Support uses to communicate with the device. Each of these protocols must have associated credential information.

During discovery, protocol credentials are used to gather information about the device such as warranty and contract information. If the protocol credentials are not supplied, the device may be discovered, but all of the relevant information about the device may not be detected, preventing Insight Remote Support from monitoring the device.

See the *HPE Insight Remote Support Monitored Devices Configuration Guide* for the protocols required for each device type.



Important: Set up discovery credentials *before* attempting device discovery. If devices are discovered without protocol credentials, then the warranty and contract information is not detected by Insight Remote Support.



Important: Insight RS requires administrator access to the monitored devices. Discovery and collections require privileged access in order to retrieve information about the monitored devices.

Priority	Type	Summary	Name
No data available in table			

To add a new protocol credential, complete the following steps:

1. Experienced users can choose a protocol directly from the Select and Configure Protocol drop-down list, but less experienced users can filter the protocols to determine the necessary protocol for a given device type. To filter the list of available protocols, do one of the following:
 - To choose from a list of all available protocols (regardless of device), select **All Device Types** in the Select Type drop-down list.
 - To filter the list of available protocols, select the type of device for which you want to configure

access credentials in the Select Type drop-down list. You can also identify a sub device type in the Select Sub-Type drop-down list to further filter the list of protocols.

The Select and Configure Protocol drop-down list is filtered according to your selection(s).

2. From the Select and Configure Protocol drop-down list, select the appropriate protocol.
3. Click **New**. The New Credential dialog box appears with fields for the protocol you selected.

4. Complete the fields in the New Credential dialog box.



Note: The available fields depend on the protocol that you select.

The following table describes the different fields you will see when working with different protocols:

Credential field	Description
Priority	Select a priority from the drop-down list. Credentials with a higher set priority will be attempted before credentials with a lower set priority. For example, a set of credentials with a priority of 1 will be executed first during the discovery process.
Type	Select a credential type from the drop-down list. For example, Username Password Credential, Certificate Credential, Anonymous Credential. Selecting a new credential type changes the available fields in the window.
Port	Contains the default port number.
Use default	Clear this check box if you do not want to use the default port number. Type the appropriate port number in the Port field.
Named Credential	If you have created a named credential for the device type, you can select it here. Insight Remote Support populates the access fields with the login details specified in the named credential. By default, the protocol uses the Named Credential that is assigned to the

Credential field	Description
	selected device. If no named protocols exist, then <i>None</i> is selected in the Named Credential drop-down list.
Username	Type the username used to access the device type.
Password	Type the password used to access the device type.
Confirm Password	Re-type the password you typed in the Password field.
File Upload	Click the Browse button to locate the certificate and upload it.
Certificate Alias	If the certificate you are identifying for access has an alias, type the alias here.

- After completing the fields, click **Add**.

The credential is added to the list of credentials for the protocol.



Note: Each protocol can have multiple credentials configured. Select a protocol in the Select and Configure Protocol drop-down list to view the list of credentials for that protocol.

- Repeat steps 1 - 5 to add additional protocol credentials.
- To update or delete a protocol credential, select the credential in the table and modify the information in the Existing Credential dialog box.
- Click **Next** to continue to the next screen of the wizard.

Insight Remote Support saves the credential information.

Discovery sources

On the Discovery Sources screen, configure which devices on your network you want discovered.

Device discovery identifies devices on your network to be monitored by Insight Remote Support.

There are three ways to tell Insight RS which devices on your network to discover, and they can be used individually or in combination: IP addresses, Windows domains, and local networks.



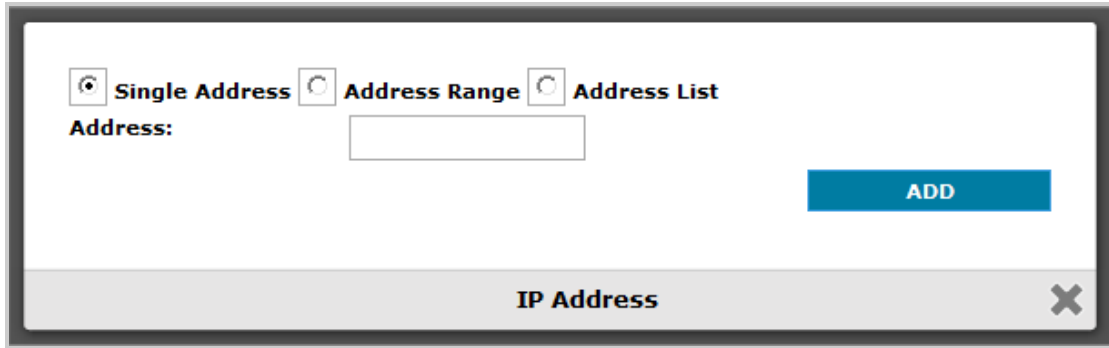
Important: If you have more than 30 devices on your network, depending on your network speed, it may take a considerable time to discover all of the devices at once. Unless you have a very small network, HPE advises that you specify discovery settings before starting device discovery.

To configure discovery sources, complete the following steps:

- Add IP addresses to be discovered. You can discover a single device by typing its IP address or discover multiple devices by typing a range or list of IP addresses.

To discover devices by IP address, complete the following steps:

- Click the **IP Addresses** pane.
- Click **New**. The IP Address dialog box appears.



- c. Do one of the following:
 - o To discover a single monitored device, type the device's IP address in the Address field.
 - o To discover a range of devices, select the **Address Range** option. In the Start Address field, type the IP address of the first device in the range. In the End Address field, type the IP address of the last device in the range.
 - o To discover a list of devices, select the Address List option. In the Comma-Separated List box, type the IP addresses of the devices separated by commas.

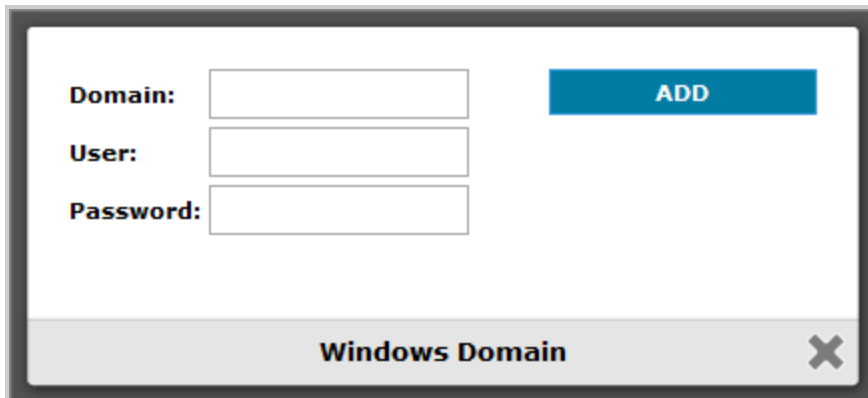
- d. Click **Add**.

The IP address or addresses appear in the table. IP address ranges appear in the Start Address and End Address columns. Single IP addresses display only in the Start Address column.

- 2. Add Windows domains to be discovered. You can discover devices by typing a Windows domain name and log on credentials.

To discover devices by Windows domain, complete the following steps:

- a. In the main menu, select **Discovery**.
- b. Click the **Sources** tab.
- c. Click the **Windows Domains** pane.
- d. Click **New**. The Windows Domain dialog box appears.



- e. In the Domain field, type the domain name.
- f. In the User field, type the username of the domain administrator.
- g. In the Password field, type the domain administrator's password.

1. After configuring your protocol credentials and discovery source(s), click **Start Discovery**. Insight Remote Support displays the progress:

Discovery Status: Running

Number of discovery operations to be run during this cycle: 1 Number of discovery operations completed during this cycle: 0

As discovery runs, Insight Remote Support adds discovered devices to the All Devices table. A device's Status column shows whether or not the device is ready to be monitored.

If you exit the Discovery screen, discovery continues in the background.

2. Review your discovered device(s). Discovered devices display in sets of 10. If Insight Remote Support discovers more than 10 devices, use the buttons at the bottom of the table to navigate to the other sets of devices.

If a device displays an error icon (❌) for its status, hover over the icon to view more details about why discovery was not successful for the device.



Note: The results table shows all devices that have been discovered by Insight RS, not just devices that have been discovered with the current settings, so you may see more devices than expected with your current settings.

Discovery Status: Stopped

Number of discovery operations to be run during this cycle: 2 Number of discovery operations completed during this cycle: 2

All Devices Search: <input type="text"/>			
Device Name	Product	Product Category	Status
hostname1.hp.com		SERVER	✔
hostname2.hp.com		SERVER	✔
hostname3.hp.com		DISK_ARRAY	✔
hostname4.hp.com		DISK_ARRAY	✔
hostname5.hp.com		DISK_ARRAY	❌
hostname6.hp.com		DISK_ARRAY	✔
hostname7.hp.com		DISK_ARRAY	✔
hostname8.hp.com		COMPUTER	❌
hostname9.hp.com		COMPUTER	❌
hostname10.hp.com		SWITCH	❌

Showing 1 to 10 of 13 entries First Previous 1 2 Next Last

3. Click **Finish** to close the wizard.

Verification is complete, and successfully discovered devices are ready to be monitored.

Export health report

You can export a health report of the devices in your environment to determine how many are ready to be monitored by Insight RS, and also let HPE or your Channel Partner to determine the effort it would take to configure your devices and deploy Insight RS in your environment.

To export a health report, complete the following steps:

1. In the main menu, select **Devices**.
2. Below the devices table, click **Export Report**.
3. Open or save the report.

The report pulls the device information from the local database and lists all of the devices covered by your discovery settings and shows why they may or may not have been successfully discovered. You can share the report with your HPE representative or Channel Partner to determine the effort required to configure the devices in your environment and deploy Insight RS.

Note that when this report is generated from the Monitored Device Setup Wizard, Insight RS has not yet connected to HPE, so will not be able to populate the report with warranty and contract information. Run the report from the Discovery or Devices screens in the Insight RS Console to see warranty and contract information.

Complete the Hosting Device Setup Wizard

The Hosting Device Setup Wizard guides you through the initial configuration of Insight Remote Support. In the Hosting Device Setup Wizard you set up default contact, site, and Channel Partner information, connect to HPE, and connect Insight Remote Support to Insight Online.

The left pane displays each step in the wizard and highlights the current step in green. Complete the information in each step and click **Next** to continue. Required fields are marked by an asterisk (*). Return to any step in the wizard by clicking **Previous** until you reach the desired step.

Receiving remote support

On the Receiving Remote Support screen, enable notifications and configure software updates.

Complete the following sections:

Optimize environment

Through Insight Remote Support, you can allow (or deny) HPE and its partners to contact your organization with products and services recommendations, pricing, and delivery information.

In the **Choosing to optimize my environment** section, do one of the following:

- To allow HPE and HPE Authorized Resellers to contact your organization, select the **Yes, I consent to having HPE or my HPE authorized reseller contact me to discuss optimizing my environment** check box.
- To deny HPE and HPE Authorized Resellers from contacting your organization, clear the **Yes, I consent to having HPE or my HPE authorized reseller contact me to discuss optimizing my environment** check box.

CHOOSING TO OPTIMIZE MY ENVIRONMENT

Yes, I consent to having HPE or my HPE Authorized Reseller contact me to discuss optimizing my IT environment. [More info.](#)



Note: Click the **more Info** link to read details about the different communications HPE and HPE Authorized Resellers send to clients.

This setting can be updated at any time on the **Application Settings** → **Settings** screen.

Remote support software updates

Choose how you want to receive software updates. The following table describes the available options:

Option	Action
Automatically Download and Install	Select Automatically Download and Install to automatically download and install a group's packages. This is the default setting, and is the recommended setting because new product support and product improvements are installed automatically.
Automatically Download	Select Automatically Download to automatically download a group's packages without installing them. These packages can be installed on the Downloaded Version tab.
Manually Apply	Select Manually Apply to manually download and install a group's packages. Install packages on the Available Version tab.

This setting can be updated at any time on the **Application Settings** → **Software Updates** screen.

Contact information

On the Contact Information screen, configure the default contact for your environment. This contact is assigned to newly discovered devices.

Additional contacts, or updates to the default contact, can be configured on the **Company Information** → **Contacts** screen.

Important: Provide correct contact details

To optimize the handling of incidents, it is important that you supply and maintain complete, accurate, and up-to-date contact information in HPE Insight RS for the monitored devices. Once an incident is automatically submitted and logged, HPE uses the specified contact information for further troubleshooting or for initiating on-site intervention, which always involves contacting the customer.



HPE will make reasonable efforts to establish contact as per the specified information, however if no contact is possible HPE shall not be liable for any delays resulting from incomplete, inaccurate, or out-of-date information; unavailability of the designated customer contact; or any other related causes outside of HPE's responsibility.

Make sure that all your contact information for all monitored devices is correct and kept up to date at all times. This will enable HPE to promptly react to any reported incidents, speed up troubleshooting and expedite necessary corrective actions in the quickest possible time.

To add a default contact, complete the following steps:

1. Complete the following fields:



Note: Required fields are marked by an asterisk (*).

Field	Action
Company Name	Type the company name.

Field	Action
First Name	Type the contact's first name.
Last Name	Type the contact's last name.
Email	Type the contact's email address. See "Enable and configure email notifications" on page 53 .
Additional Email(s)	Type additional email addresses, if desired. These email addresses will be copied on emails sent to the contact. Separate the email addresses by a comma, semicolon, or space.
Preferred Language	Select the contact's language from the drop-down list. The 🗇 character denotes that emails will be sent in the chosen language if the Email Adapter is enabled.
Primary Phone Number	Type the contact's primary phone number.
Alt Phone Number	Type the contact's secondary phone number (optional).
Special instructions for support delivery	Type special support delivery instructions in this free form text field. Text typed here is included with service events and is visible to people working cases that Insight RS submits to HPE. Example of a message that could be typed in this field: <i>If you get an event from my site on New Year's Day, call my pager instead, at +1-555-555-5555.</i>

2. Click **Next**.

The system creates the default contact.

Site information

On the Site Information screen, configure site details for your environment. The information configured here is used as the default site information for your environment and is assigned to newly discovered devices. Keep the site information current because this specifies the location where support services will be delivered.

Additional sites can be configured on the **Company Information** → **Sites** screen.



Important: Make sure you type the correct address details, as the service is delivered to the address details provided.

To add a default site, complete the following steps:

1. Complete the following fields:



Note: Required fields are marked by an asterisk (*).

Field	Action
Site Name	Type the site name.
Address Line 1	Type the site's address. Use Address Line 2 if necessary.
City	Type the site's city.

Field	Action
State/Province	Type the site's state or province.
Postal Code	Type the site's postal code.
Country	Select the site's country from the drop-down list.
Time Zone	Select the time zone from the drop-down list.

2. Click **Next**.

The system creates the default site.

Registering HPE Insight Remote Support

On the Registering Insight Remote Support screen, configure your proxy settings, test your connectivity to HPE, and register your Hosting Device with HPE.

Complete the following sections:

Test connectivity to HPE

Test your connection to HPE to make sure the Hosting Device can communicate with HPE. If your company uses a web proxy server, configure the web proxy settings so Insight Remote Support can connect to HPE through your web proxy server.

To configure your web proxy settings and test your connection to HPE, complete the following steps:

1. Select the **Use Web Proxy to access Internet** check box to activate the fields.
2. Complete the following fields:
 - Web Proxy Server
 - Web Proxy Port
 - Web Proxy User Name
 - Web Proxy Password
3. Click **Test Connection**.



Note: Clicking **Test Connection** saves the web proxy settings.

Register with HPE

Registration confirms that the Hosting Device can reach HPE. If for some reason HPE cannot be reached, Insight Remote Support will continue to retry registration until HPE can be reached. If you prefer to manually attempt to register, return to the Register Hosting Device screen of the Hosting Device Setup Wizard and click **Register with HPE**.

To register your Hosting Device with HPE, complete the following steps:

1. Click **Register With HPE**.

The status of your registration appears next to the **HPE Registration Status** field. Once your registration status is *Registered*, the **Register With HPE** button grays out so you can only register once, and the **Next** button enables.

If registration fails, return to the previous section and test your connection to HPE.

Insight Remote Support is registered with HPE and can send information to HPE.

2. Click **Next**.

Integrate Insight RS with HPE Insight Online

On the Integration with HPE Insight Online screen, connect to HPE Insight Online, if desired.

HPE Insight Online provides one stop, secure access within the HPE Support Center (www.hpe.com/support/hpesc) portal to product and HPE support information personalized to your IT environment with warranty or HPE contractual services. You can link Insight Remote Support to HPE Insight Online and get automatic updates of device health, service events, and associated support cases. Integrating with HPE Insight Online automatically associates any devices monitored by Insight Remote Support with the HP Passport account in HPE Insight Online. The device details displayed in HPE Insight Online reflect the configuration information and event details transmitted automatically from Insight Remote Support.

Additional users can be configured to have a shared view of these devices within HPE Insight Online. If you configure HPE Authorized Channel Partners, those Channel Partners will also be able to log on to HPE Insight Online with their own HP Passport account to view your device information. If you selected in the Receiving Remote Support screen to have your HPE Authorized Channel Partner contact you to discuss optimizing your IT environment, then the device information available in HPE Insight Online will also be viewable to your preferred HPE Authorized Channel Partner.



Important: Insight Online supports a maximum of 1,500 devices per HP Passport ID. When integrating with Insight Online, make sure each Insight RS installation monitors no more than 1,500 devices.



Note: There is no communication from HPE Insight Online to Insight Remote Support.

To enable Insight Remote Support to send data to HPE Insight Online, complete the following steps:

1. Type your HP Passport user name and password in the provided fields.

HPESC Registration Status:	Not Registered
HP Passport User Name:	<input type="text"/>
HP Passport Password	<input type="password"/>



Note: If you do not have an HP Passport Account, click **Do not have a HP Passport Account?** and create one.

These settings can be updated at any time on the **Application Settings** → **HPE Insight Online** screen.

2. Click **Register With HPE Insight Online**.

The HPESC Registration Status changes to Registered, and Insight Remote Support uses your HPE Support Center credentials when sending data to HPE Insight Online.

3. Click **Next**.

HPE Authorized Channel Partners

On the HPE Authorized Channel Partners screen, set your channel partner.

The default HPE Authorized Service Partner and HPE Authorized Reseller/Distributor will be used for any newly discovered devices. Additional HPE Authorized Resellers and Service Partners can be specified for each device, if required, on the **Company Information** → **Channel Partners** screen once this setup is complete.

The HPE Authorized Channel Partners screen contains the following sections:

- **Default HPE Authorized Service Partner** – HPE Authorized Channel Partner who sells HPE products and services, and is also authorized to deliver services and support on behalf of HPE.
- **Default HPE Authorized Reseller/Distributor** – HPE Authorized Channel Partner who sells HPE products and services.
- **Default Installer** – The installer of HPE Insight Remote Support.

If your product sales and support services are delivered by Hewlett Packard Enterprise, leave HPE as the default channel partner and click **Next**.

To add default channel partner information, complete the following steps in each section:

1. Click the Partner ID option.
2. Type your partner identification number into the **Partner ID** field. The Partner ID uniquely identifies a partner as an HPE Authorized Partner during the HPE partner registration process.
3. Click **Check ID**. The partner ID is verified and details about the partner appear. Make sure the information about the partner is correct.
4. Repeat steps 1 - 3 for each section.
The system saves the default channel partner information.
5. Click **Next**.

Chapter 4: Completing post-installation configuration tasks

This chapter guides you through optional configuration tasks you may want to perform after installing Insight RS. Perform these tasks after the Hosting Device Setup Wizard device discovery is complete.

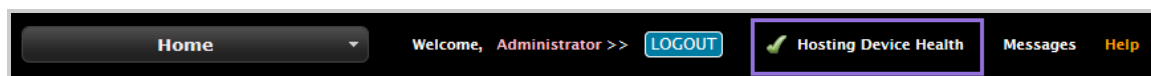


Verify Hosting Device health

Make sure the installation is successful by confirming your Hosting Device is healthy. A green check mark appears at the top of the screen when the Hosting Device is healthy.

To verify the Hosting Device's health, complete the following steps:

1. Log on to the Insight RS Console.
2. Confirm a green check mark appears next to **Hosting Device Health** at the top of your screen.



3. If the green check mark does not appear, click the **Hosting Device Health** link to find out which component is not functioning correctly. See the Online Help for more information about resolving health issues.

Verify warranty and contract information

Entitlement information is required to route your managed system's hardware events to the appropriate HPE support program based on your contract and support level. Without the necessary and correct entitlement information, events from your managed systems cannot be received and the systems cannot be supported.

In Insight RS every device has its entitlement checked to see if it is in HPE warranty or contract and Insight RS displays that device's entitlement. If the device has no HPE entitlement the health status indicator will be red, and no incidents will be analyzed or sent to HPE.

To verify a device's warranty and contract information, complete the following steps:

1. In the main menu, select **Devices**.
2. Locate the device and click the device name. The Device Details screen appears.
3. Click the **Device** tab.
4. Expand the Hardware section and verify the Acquired Serial Number and Acquired Product Number are correct for your device.

With the exception of EVA, P4000 and multivendor devices, the serial number and product number should be returned correctly from your device during discovery. For other devices, if these values are not correct, check the protocol credentials assigned to the device on the **Credentials** tab. If the credentials are incorrect, fix them and rediscover the device.

- Expand the Warranty & Contract section and verify the Support Type and Support Identifier are correct for your device. These values are returned from HPE based on the device's Serial Number and Product Number, so make sure those values are correct first before modifying these values. If these values are not correct, enter the correct values.

The device will use the new warranty and contract information.

Verify device status

After discovery completes, select **Devices** in the main menu. Check that the device information has been discovered correctly. If it has not, verify your credential settings and run discovery again for that device.



Note: Discovery will always assign any valid credentials to a device that have been configured in the discovery settings, even if you have manually assigned invalid credentials to the specific device on the device's Credentials tab.

After discovery, an overview of the device status appears. The Status column shows whether Insight RS can monitor your devices. Verify the Status column shows a success icon (🟢). If the Status column shows an error icon (🔴), then there are one or more issues with the device's warranty and contract, monitoring and collections information, or its eligibility to receive remote support.

Insight RS checks every device's warranty and contract to make sure it has a valid HPE warranty or contract. If a device has no HPE warranty or contract, the monitoring health indicator in the Insight RS Console will be red. If this is red, then no service events will be analyzed or sent to HPE.

Insight RS does not immediately gather collections after discovering a new device. The first collection for a device occurs when the collection schedule normally triggers. To clear any status issues, HPE recommends you manually run the collection schedule on the **Collection Services** → **Collection Schedules** tab.

If an error icon appears for any devices, hover your pointer over the icon, and a dialog box appears showing an overview of the status issue.

Discovery Status: Stopped

EXPORT REPORT SHOW CONFIGURATION OPTIONS START DISCOVERY

Number of discovery operations to be run during this cycle: 2 Number of discovery operations completed during this cycle: 2

Device Name	Product	Product Category	Status
hostname1.hp.com		SERVER	🔴
hostname2.hp.com		SERVER	🟢
hostname3.hp.com		DISK_ARRAY	🟢
hostname4.hp.com		COMPUTER	🟢
hostname5.hp.com		SERVER	🟢

Showing 1 to 5 of 5 entries

Overall Status:
 Eligible: Yes
 Monitoring & Collections: FAILURE
 Warranty & Contract: Not Entitled
 Enabled: No

To resolve device status issues, see ["Resolve monitored device status issues"](#) on the next page.

Resolve monitored device status issues

Insight RS checks every device's warranty and contract to make sure it has a valid HPE warranty or contract. If a device has no HPE warranty or contract, the monitoring health indicator in the Insight RS Console will be red. If this is red, then no service events will be analyzed or sent to HPE.

To resolve the status issue, complete the following steps:

1. In the main menu, select **Devices**.
2. On the **Device Summary** tab, the Status column shows the overall health of the device and should match the status on the discovery screen. View the Warranty & Contract, Monitoring & Collections, and Eligible columns for areas where errors occurred.

Device Summary									
Status	Device Name	Product	OS Name	Warranty & Contract	Monitoring & Collections	Open Service Events	Eligible	Enabled	
✓	hostname1.hp.com	ProLiant DL360 G3	Linux - Red Hat Enterprise Linux	✓	✓	None	✓	Yes	
✓	hostname2.hp.com	StorageWorks MSA2324i		✓	✓	None	✓	Yes	
✗	hostname3.hp.com	NSM2060	SAN/iQ	✗	✗	None	✓	Yes	
✓	hostname4.hp.com	ProLiant ML350 G3	Windows Server	✓	✓	None	✓	Yes	

3. Check the following if any columns show the error icon:

- **Warranty & Contract**—This column shows if a device has valid warranty and contract information. If an error icon appears, this can mean the device does not have a warranty contract, that there was a problem with the Serial Number or Product Number, or that this information was not gathered from the device correctly during discovery.

In Insight RS every device has its entitlement checked to see if it is in HPE warranty or contract and Insight RS displays that device's entitlement. If the device has no HPE entitlement the health status indicator will be red, and no incidents will be analyzed or sent to HPE.

To resolve the error, complete the following steps:

- i. Click the device name and on the **Device** tab expand the Hardware section.
- ii. Check the values for the Serial Number and Product Number. If they are not correct, check the protocol credentials assigned to the device on the **Credentials** tab. If the credentials are incorrect, fix them and rediscover the device.

For some device types, such as EVA and P4000 devices, the Serial Number and Product Number need to be entered manually. Enter the values in the Override Serial Number and Override Product Number fields, and click **Save Changes**.

- iii. Return to the **Devices** → **Warranty & Contract** tab, select the device and click **Actions** → **Refresh Warranty & Contract**. If the success icon does not appear, return to first step and verify your Serial Number and Product Number.
- **Monitoring & Collections**—This column shows if device monitoring and collections are working correctly. To resolve the error, complete the following steps:

- i. Click the **Monitoring & Collections** tab and hover over the error icon in Monitoring, Basic Collection, or SAN/Storage Collection column for details or click the error icon for more information about why the failure occurred.
 - ii. Resolve the failures shown in the information window.
 - iii. If the device still displays an error icon in one of its status columns, the failures may need to be cleared. See "[Clear status errors](#)" below for more information.
- **Eligible**—This column shows whether the device is eligible for Insight RS. If the device is not eligible for remote support, then it cannot be monitored.

Send test events and generate collections

For each device you register with Insight RS, send a test event and generate a collection to Insight RS to verify the device is communicating with the application.

View the *HPE Insight Remote Support Monitored Devices Configuration Guide* to learn how to send test events and generate collections for specific devices.



Important: When viewing events and collections in the Insight RS Console, any time displayed converts to the time zone set in the web browser. This is to make sure users see the event timing using their local time zone. If there are discrepancies between the event time and the event processed time, then check the time and time zone setting on the monitored device. If the time is set externally from a time server or via DHCP, make sure these are connected and set to the appropriate time. The time discrepancy will not affect the efficient delivery of service by HPE or an HPE Authorized Service Partner, as the Hosting Device time is used as a reference for service delivery.

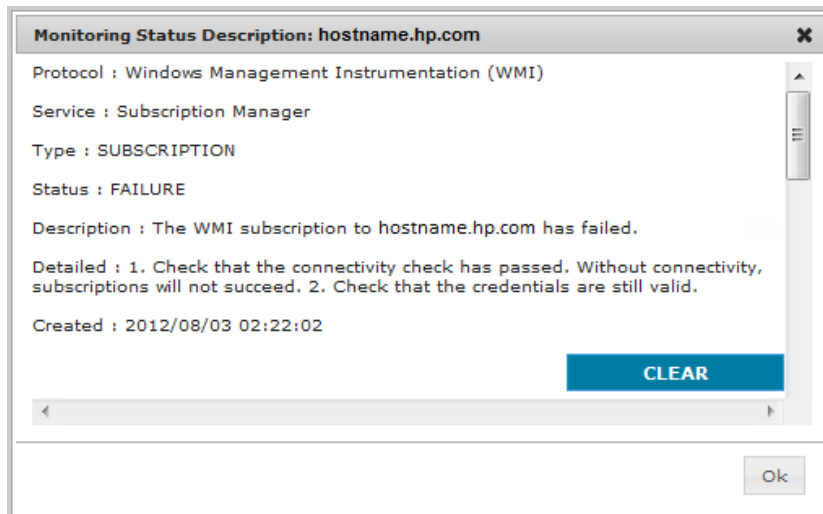
Clear status errors

Even when collections and events have been processed successfully, an error icon (❌) may appear under the Monitoring & Collections column for a device on the **Devices** → **Device Summary** screen. An error icon indicates that a failure occurred during event or collection processing. Even after an event or collection succeeds, the error icon persists until errors associated with the device are cleared.

To remove the error icon from the display so that a success icon (✅) appears instead, all errors associated with monitoring or collections must be cleared.

To clear status errors, complete the following steps:

1. From the **Devices** screen, select the **Monitoring & Collections** tab.
2. For the device in question, click the error icon under the **Monitoring, Basic Collections** and/or **SAN/Storage Collection** column to get more information. A window appears listing previous and current uncleared failure and success messages for the device. Use the scroll bar on the right to view the entire window contents.



- For each failure message, click **Clear**. All of the failure messages must be cleared before the error icon will be replaced by a success icon.



Note: If only Unknown status messages remain in the window after the failure messages are cleared, a gray box icon (☐) appears instead of a success or error icon.

Configure the backup settings

If you want to change the default settings, configure the backup target location and number of backups to retain.

Set the backup target location

The default target location is: C:\ProgramData\HP\RS\DATA\backup

HPE recommends that you change the target location to a non-default storage device or network share so that backups are not stored on the same device as the original data. HPE also recommends that you set the Insight RS and system-level backup target locations to a device that contains removable media or to a remote network share so that backups can be physically stored off-site for disaster-recovery purposes.

To change the backup target location, run the following command from a command prompt:

```
rsadmin backup -now -target \\home\backups
```

This command runs the backup immediately and directs the backup to the network share: \\home\backups.

Because the **-now** option is used, the network share has to be accessible at the time this command is run. If the **-now** option is not used, it is not required that the share location be accessible at the time the command is executed, but it must be accessible whenever the next scheduled or commanded backup is run.



Important: The target directory is cleared every time the backup runs so that only the results of the backup exist in that directory. Use caution when specifying the output directory. If you do not use the **-now** option, Insight RS verifies the directory exists and is accessible, but it is not be cleared until the regularly scheduled backup time.

Set the number of backup versions

The default number of backups Insight RS retains, and the recommended setting, is 2.

To change the number of backups retained, run the following command from a command prompt:

```
rsadmin backup -versions <number_of_backups>
```

where <number_of_backups> is the number of backup data sets to be retained at the target location.

Integrate with HPE SIM

If you want to share information about your service events between SIM and Insight RS, install the HPE SIM Adapter through the Insight RS Console. If SIM was installed on the Hosting Device *before* installing Insight RS, then the HPE SIM Adapter is automatically installed. If SIM was installed *after* installing Insight RS, then the HPE SIM Adapter needs to be manually installed.



Important: You may need to enter additional credentials, such as RIBCL, in Insight RS that are not available in SIM. Additionally, values such as Serial Numbers and Product Numbers that you manually entered in SIM must be manually entered in Insight RS as well.

For information about supported versions of SIM, see the *HPE Insight Remote Support Release Notes* at: www.hpe.com/info/insightremotesupport/docs.

For information about installing SIM, see the *HPE Systems Insight Manager Installation and Configuration Guide for Windows* at: <http://www.hpe.com/info/insightmanagement/docs>.



Important: SIM must be installed on the Hosting Device *before* installing the HPE SIM Adapter. If SIM is *not* installed, the SIM Adapter installation will fail and you will not see the HPE SIM Adapter on the Administrator Settings screen.

Before you can enable the HPE SIM Adapter pane, you must install the HPE SIM Adapter:

Install the HPE SIM Adapter

To install the HPE SIM Adapter, complete the following steps:

1. Log on to the Insight RS Console.
2. In the main menu, select **Administrator Settings**.
3. Click the **Software Updates** tab.
4. Click the **HPE Systems Insight Manager (HPE SIM) Adapter** link in the table.
5. Click the **Available Version** tab in the lower pane.

Settings | HP Insight Online | Integration Adapters | **Software Updates** | Schedules

Automatic Update Level: CHECK FOR NEW UPDATE SCHEDULE UPDATE START UPDATE

Group	Package	Installed	Downloaded	Available
▼ UCA_V1				
	Event Log Monitoring Collector (ELMC)	6.4.0.17	6.4.0.17	6.4.0.17
	HP Operations Manager (HPOM) Adapter			7.0.6.6427
	HP Systems Insight Manager (HP SIM) Adapter			7.0.5.169

Installed Version | Downloaded Version | **Available Version**

Name: HP Systems Insight Manager (HP SIM) Adapter **Description:** This management platform adapter allows synchronization of events between HP Insight Remote Support and HP Systems Insight Manager (HP SIM), including the case id and its status of all hardware incidents sent to HP. You can also optionally configure synchronization of devices and credentials from HP SIM. This adapter requires HP SIM to be installed on the same Hosting Device before this adapter is installed and subsequently configured in the Integration Adapters tab. INSTALL DOWNLOAD

Version: 7.0.5.169

ID: HpSimAdapterNonPlugin

Group: UCA_V1

Status: Available

Package Dependencies: None

- Click **Install**. The HPE SIM Adapter downloads and installs onto the Hosting Device.
- When the installation is complete, select the **Integration Adapters** tab to enable and configure the HPE SIM Adapter. See ["Configure the HPE SIM Adapter" below](#) for more details.

Important: To install updates to the HPE SIM Adapter through the **Software Updates** tab, you must first disable the HPE SIM Adapter on the **Integration Adapters** tab.

The HPE SIM Adapter installs and is ready to be enabled and configured.

Configure the HPE SIM Adapter

If your company uses SIM, configure Insight Remote Support to share information with SIM through an included adapter.

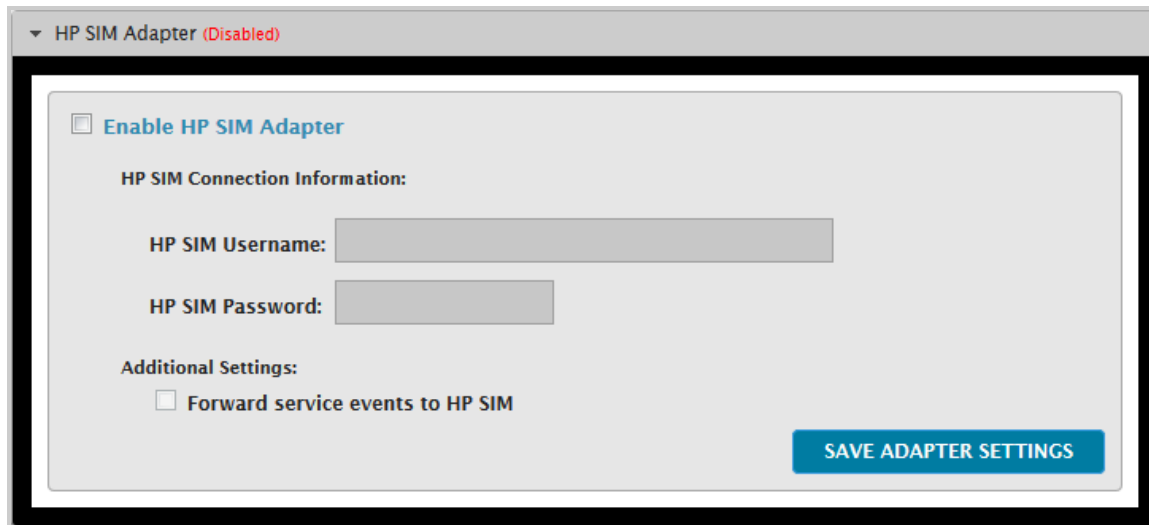
To install the HPE SIM Adapter, see ["Install the HPE SIM Adapter" on the previous page](#).

Important: You may need to enter additional credentials, such as RIBCL, in Insight RS Console that are not available in SIM. Additionally, values such as Serial Numbers and Product Numbers that you manually entered in SIM must be manually entered in Insight RS Console as well.


To configure the HPE SIM Adapter, complete the following steps:

- In the main menu, select **Administrator Settings**.
- Click the **Integration Adapters** tab.
- Click the **HPE SIM Adapter** heading to expand the HPE SIM Adapter pane.

The pane is divided into two sections: SIM Connection Information and Additional Settings.



4. Select the **Enable HPE SIM Adapter** check box.
5. In the HPE SIM Connection Information section, type the HPE SIM username and password.


 **Tip:** Use an SIM-specific account with a password that does not expire. This will help you to avoid issues if the account is tied to an individual person's account that could be disabled or locked out.

6. In the Additional Settings section, select the **Forward service events to HPE SIM** check box to forward any service events relating to SIM-specific devices to SIM.
7. Click **Save Adapter Settings**.

Insight Remote Support saves the HPE SIM Adapter configuration. **(Enabled)** now appears next to the HPE SIM Adapter to indicate it is enabled.

Enable and configure email notifications

Insight Remote Support sends email notifications when certain system events occur. You can enable or disable some or all of these notifications.

 **Note:** HPE highly recommends that you enable the Email Adapter and, at the minimum, select the following notifications: *Case Opened*, *Entitlement Expiration*, and *Device Change*.

To enable email notifications, complete the following steps:

1. In the main menu, select **Administrator Settings**.
2. Click the **Integration Adapters** tab.
3. Click the **Email Adapter** heading to expand the Email Adapter pane.

4. Select the **Enable Email Notifications** check box to activate the Notification States check boxes.
5. Under Notifications States, select one or more of the following check boxes:

Notification state	Description
Event Submitted	Default and backup contacts notified when a service event is submitted to the HPE data center. An email is sent for all events that are submitted to the HPE data center, including test events.
Case Opened (Events)	Default and backup contacts notified when a case is opened in the HPE data center. Note that service events generated by test events are never opened so an email will not be sent for test events.
Case Closed (Events)	Default and backup contacts notified when a case is closed in the HPE data center. Emails are also sent for service events generated by test events.
Collection Sent	Default and backup contacts notified each time data collected about a device is sent to HPE.
Software Management Updates	Default contact notified whenever there is a new software update available.
Entitlement Expiration	Default and backup contacts notified when a warranty or contract is about to expire. Notifications are sent at 90, 60, 30, and 0 days before expiration.
New Device Discovered	Default and backup contacts notified when a new device is discovered.

Notification state	Description
Device Health Status	<p>Default and backup contacts sent a CSV file that contains current and previous health status for all devices. The CSV file contains information about the status and, when applicable, a description of the problem to assist in troubleshooting. Note that when the schedule runs for the first time, email will not be sent because there is not yet a record of device health history.</p> <p>The daily schedule is visible on the Settings tab. Expand Advanced Schedules → Device Health Status Notification to modify the schedule or manually run the schedule.</p>
Hosting Devices Exceeds %	Default and backup contacts notified when the Hosting Device's capacity exceeds the specified percentage of devices that Insight RS can support.



Note: Case Opened, Case Closed, Collection Sent, Entitlement Expiration, and Device Change notifications are sent to the user identified as the default Insight Remote Support contact, as well as any configured backup contacts. Application Failure and Software Management Updates notifications are sent to the user identified as the Hosting Device contact.

6. Under Mail Server Settings, type the sender's email address, and the SMTP server name and port. The sender's email address prevents the anonymous email from being classified as spam by your email system.
7. From the Encryption drop-down list, do one of the following:
 - If your company does not use an encryption method, select **None**.
 - If your company uses an encryption method, select the appropriate encryption type: Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
8. Select the **Send test email to default Hosting Device contact** check box.
9. Click **Save Adapter Settings**.



Important: To install updates to the Email Adapter through the **Software Updates** tab, you must first disable the Email Adapter on the **Integration Adapters** tab.

Insight Remote Support saves the email notification settings. (Enabled) appears in the Email Adapter pane's heading. The Hosting Device contact receives a test email. If the contact does not receive the test email, return to the Email Adapter pane and check the mail server settings for errors.

Forward service events to another management application

The SNMP Service Event Adapter allows you to forward a hardware event to another management application when a service event is sent to HPE. The SNMP Service Event Adapter only forwards events that need intervention to stop failures, which have already automatically been logged at HPE.

The service event and support case information displayed in the Insight RS Console can also be communicated through an SNMP trap to your receiving application. To properly interpret the trap, your receiving application must be configured to use the cpqService MIB, which is available for download in the

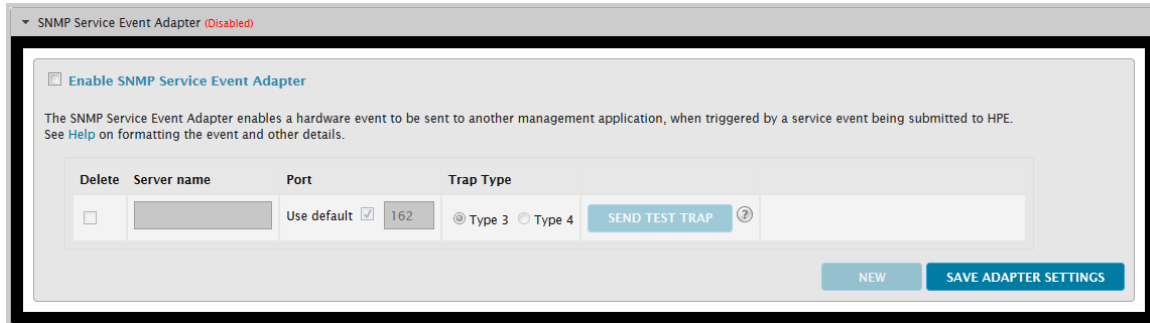
HP Systems Insight Manager - MIB Kit at:

http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04272529.

The cpqService MIB defines the Type 3 or the Type 4 SNMP service trap. The cpqService MIB references other MIBs.

To forward service events to another server, complete the following steps:

1. In the main menu, select **Administrator Settings**.
2. Click the **Integration Adapters** tab.
3. Click the **SNMP Service Event Adapter** heading to expand the Service Event Adapter pane.



4. Select the **Enable Service Event Adapter** check box.
5. Edit an existing server or click **New** to add a new server.
6. Type an IP address or fully qualified domain name in the **Server name** field.
7. Use the existing port or clear the **Use default port** check box and type a port number in the **Port** field.
8. Determine which Trap Type you want to use.

- The Type 3 trap is the default. Type 3 traps are sent only when the service event case status is Submitted, and Type 3 does not include the case ID in the trap. The event case status is defined by the cpqService3IncidentStatus variable.

Type 3 traps will display cpqService3Information as the event OID name.

- The Type 4 traps are sent when the status of the service event case changes, and also include the case status and case ID in the trap. The event case status is defined by the cpqService3Incident7Status variable and will be one of the following states: error(0), pending(1), submitted(2), received(3), open(4), closed(5). The case ID is defined by the cpqService3CaseIdentifier variable.

The Type 4 MIB definition includes the Type 3 definition plus additional definitions to include the Case ID and Case Status.

Type 4 traps will display cpqService4Information as the event OID name.

Trap type variables and descriptions

Variable	Description	Type 3	Type 4
2	<p>cpqService3IncidentStatus</p> <p>The status of the service incident.</p> <p>Syntax=INTEGER { other(1), intransit(2), delivered(3), undelivered(4), assigned(5), closed(6), submitted_to_ISEE(7) }</p>	X	
3	<p>cpqService3IncidentInformation</p> <p>Provides the URL to the event analysis report.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
4	<p>cpqService3IncidentEvent</p> <p>Brief description of the event that initiated the service incident.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
5	<p>cpqService3IncidentUniqueID</p> <p>Unique Event Analysis Identifier assigned to the incident.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
6	<p>cpqService3IncidentTimeofOriginalEvent</p> <p>Time of the original event this service event relates to.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
7	<p>cpqService3IncidentSourceSystemName</p> <p>Name of the system this service event relates to.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
8	<p>cpqService3IncidentIPAdressOfSource</p> <p>IP Address of the system this service event relates to.</p> <p>Syntax=IpAddress</p>	X	X
9	<p>cpqService3ISEEIncidentInformation</p> <p>This is a URL pointing to the Service Incident status in ISEE if available.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
10	<p>cpqService3IncidentIdentifier</p> <p>Service Incident Identifier assigned to the incident report by the ISEE client.</p> <p>Syntax=DisplayString (SIZE (0..255))</p>	X	X
11	<p>cpqService3IncidentReceiveTrapOID</p> <p>The ID of the originally received event.</p> <p>Syntax=OBJECT IDENTIFIER</p>	X	X

Variable	Description	Type 3	Type 4
14	cpqService3RecommendedAction1	X	X
15	cpqService3RecommendedAction2		
16	cpqService3RecommendedAction3 Recommended action. Syntax=DisplayString (SIZE (0..255))		
17	cpqService3CustomerSelfRepairInstructionURL A URL pointing to additional repair information. Syntax=DisplayString (SIZE (0..255))	X	X
18	cpqService3EventSeverity The severity of the service incident. Syntax=INTEGER { critical(1), major(2), minor(3), warning(4), informational(5) }	X	X
19	cpqService3AnalyzerSystemName Name of the system this service event was analyzed on. Syntax=DisplayString (SIZE (0..255))	X	X
20	cpqService3FRUList1	X	X
21	cpqService3FRUList2		
22	cpqService3FRUList3		
23	cpqService3FRUList4 Replaceable Unit information. Syntax=DisplayString (SIZE (0..255))		
24	cpqService3Location1	X	X
25	cpqService3Location2 Replaceable Unit location. Syntax=DisplayString (SIZE (0..255))		
26	cpqService3Incident7Status The status of the service incident for IRS 7.x. Syntax=INTEGER { error(0), pending(1), submitted(2), received(3), open(4), closed(5) }		X
27	cpqService3CaseIdentifier Unique Case Identifier assigned to the incident if a case is opened in the data center. Syntax=DisplayString (SIZE (0..255))	X	X

9. To make sure the settings are correct, click **Send Test Trap**. A test SNMP trap is sent to the specified management application server where its receipt can be checked.

10. Click **Save Adapter Settings**.

The system saves the server, and SNMP events received by Insight RS will be forwarded to the server where its arrival can be checked.

Enable operator-level user authentication

Password management for the Insight RS Console is managed at the operating system level. Users that are members of the operating system's Administrators group are automatically granted *administrator-level* access in Insight Remote Support. Automatic administrator-level authentication cannot be disabled.

You can choose to grant *operator-level* access to any user authenticated by the operating system, regardless of group membership. With *operator-level* access disabled, non-Administrative users cannot access the Insight RS Console console. *Operator-level* access can be enabled or disabled.



Note: Administrator-level users can access all areas of Insight Remote Support, including Administrator Settings, Discovery, and Solution Manager. Operator-level users cannot access Administrator Settings, Discovery, Solution Manager or the setup wizards, but have access to the rest of Insight Remote Support.

To enable operator-level access, complete the following steps:

1. In the main menu, select **Administrator Settings**.
2. Click the **Settings** tab.
3. In the User Authentication pane, select the check box to enable automatic operator-level user authentication:

User Authentication

You can choose to grant operator-level access to any user authenticated by the operating system by selecting the check box.

Administrator-level users can access all areas of Insight Remote Support, including Administrator Settings.

Operator-level users cannot access the Administrator Settings, of Discovery, but have access to the rest of Insight Remote Support.

Allow all users authenticated by the operating system to access the Insight RS Console as operators, regardless of group membership



Note: You can clear this check box at any time to disable automatic operator-level user authentication.

4. Click **Save Settings**.

Automatic operator-level user authentication is enabled or disabled.

Enable SSLv3 (if required)

SSLv3 is disabled by default in Insight RS. With SSLv3 disabled, Insight RS uses Transport Layer Security (TLS) for communication. For more details about Insight RS communication, see the *HPE Insight Remote Support Security White Paper* or the *HPE Insight Remote Support Security Presentation*.

The `rsadmin config` command can be used to enable SSLv3, disable SSLv3, or disable Padded Ciphers for SSLv3.

Padded Ciphers are susceptible to POODLE attacks. Reference the following HPE Support Communication:

<http://h20565.www2.hp.com/hpsc/doc/public/display?docId=c04496345>



Important: Some older monitored devices can only communicate with Insight RS through SSLv3. Disabling SSLv3 will prevent Insight RS from monitoring those devices.



Important: Communication with the HPE backend over the Internet will not allow SSLv3 communication.

Execution of these options impacts Insight RS server ports 7905 (event indications) and 7906 (Insight RS Console).

In addition, these `rsadmin` commands impact outbound protocols: RIBCL, WBEM, WMI (DCOM), WS-Man, HTTPS, ELMC, and VMWare. Discovery and collections will be impacted in the following ways:

- If the `rsadmin` command is executed after devices have already been discovered and appear on the Devices page, collections may begin to fail.
- If discovery is executed against any new device that only uses SSLv3, the new device may fail to be discovered properly.

To determine if your devices are affected by SSLv3 disablement, see "[Determine which devices are affected by SSLv3 disablement](#)" on the next page.

The `-disableSslv3PaddedCiphers` option will allow communication through SSLv3, but with a shorter list of usable ciphers:

- Port 7905:
 - TLS_ECDHE_RSA_WITH_RC4_128_SHA
- Port 7906:
 - RSA_WITH_RC4_128_MD5
 - RSA_WITH_RC4_128_SHA
 - TLS_ECDHE_RSA_WITH_RC4_128_SHA

If the monitored devices cannot use these ciphers for the ports listed, then `-enableSslv3Completely` is recommended.

When these options are executed, the command line will inform you if the Insight RS processes need to be restarted. For example, if the same command is executed a second time after a restart, the user will be informed that a restart is not required.

Table 4.1 SSLv3 rsadmin commands

Command	Description
<code>rsadmin config -disableSslv3Completely</code>	Completely disable support of SSLv3.
<code>rsadmin config -disableSslv3PaddedCiphers</code>	Allow SSLv3 but without Padded Ciphers.
<code>rsadmin config -enableSslv3Completely</code>	Enable full support of SSLv3.

Determine which devices are affected by SSLv3 disablement

After you install the 7.6 patch release, SSLv3 is disabled by default. You can identify which devices were impacted by the patch by viewing the device health status report, which runs on a weekly schedule or you can run it manually. You can view the report results either through email notifications or through the Insight RS Console. Note that regardless of which option you choose to view the health report, all of the device health checks must have been run after installing the patch.

You can wait for the health checks to run on their weekly schedule, but it may take up to a week before they are next scheduled to run. You can also run the health check manually:

1. In the main menu, select **Administrator Settings**.
2. Click the **Schedules** tab.
3. In the schedules table expand the Advanced Schedules section.
4. Look for the schedules for device health checks:

Name	Frequency	Day	Time	Next Scheduled Time	Enabled
Network Collection Health Check	Every Week	Saturday	03:01	7/23/2016, 3:01:00 AM	✓
Performance Data Collection Schedule	Every Month	Day 8	13:53	8/8/2016, 1:53:00 PM	✗
Resource Monitor Schedule	Every Hour		Minute 0	7/19/2016, 11:00:00 AM	✓
SAN Configuration Collection Health Check	Every Week	Sunday	02:05	7/24/2016, 2:05:00 AM	✓
Server Basic Collection Health Check	Every Week	Sunday	03:15	7/24/2016, 3:15:00 AM	✓
Storage Collection Health Check	Every Week	Sunday	04:15	7/24/2016, 4:15:00 AM	✓
StoreVirtual (P4000) Collection Health Check	Every Week	Saturday	04:05	7/23/2016, 4:05:00 AM	✓

5. Manually run the health checks for the device types you have in your environment. For example, if you have servers in your environment, run the Server Basic Collection Health Check:
 - a. Click on the name of the schedule.

✕
Schedule

SAVE
START NOW

Name: Server Basic Collection Health Check

Frequency: Every Week

Day and Time: Every Sunday at 03 : 15

Next Scheduled Time: 7/24/2016, 3:15:00 AM

Comment: Runs weekly checks that Server Basic Collections are working correctly and communication with the device is functional.

- b. Click **Start Now**.
 - c. This executes connectivity checks to the monitored devices. This schedule can take some time to complete.
6. After the health check completes, you can view the results in one of two ways:

- **Option 1: Through email notification**

If you have email notifications enabled (**Administrator Settings** → **Integration Adapters** → **Email Adapter**) and have selected to receive the *Device Health Status* notification you will receive a daily email with current health status of each device in your environment. The notification email contains a CSV report that can be opened in a program like Excel to view issues.

- **Option 2: Through the Insight RS Console**

- i. In the Insight RS Console, navigate to the **Devices** → **Device Summary** tab, and check for red health indicators in the Monitoring & Collections column.

Status	Device Name	Product	OS Name	Warranty & Contract	Monitoring & Collections	Open Service Events	Eligible	Enabled
	hostname1.hp.com	ProLiant DL360 G3	Linux - Red Hat Enterprise Linux	✓	✗	None	✓	Yes

- ii. Click the red health indicator to go to the Monitoring & Collections tab. Then click the red health indicator to view detailed information about the health. The following message appears when the SSLv3 disablement issue happens:

This device is attempting to use an unsupported SSL protocol or cipher. The device may need a firmware/BIOS update. Or, you can enable additional protocols/ciphers on this IRS host. See the rsadmin documentation.

When this message is displayed, it means this device used SSLv3 to communicate with Insight RS and now that has been disabled. Refer to the *Installation and Configuration Guide* for how to re-enable SSLv3.

Disable SNMP automatic discovery

By default, if an SNMP provider on a monitored device has been configured with the Hosting Device as a trap destination, Insight RS tries to discover the device when it receives a trap. You can disable this behavior if you want to prevent Insight RS from automatically discovering these devices.

Disabling this behavior prevents Insight RS from starting unexpected discovery operations, which in some environments can prove problematic in terms of performance and can delay processing of real service events.

To disable SNMP auto-discovery, complete the following steps:

1. On the Hosting Device, open a DOS window with administrative rights.
2. Run the following command:

```
rsadmin config -set analysis.autodiscovery.disabled=true
```

Add device groups

You can group the devices in your environment into logical categories to make administration of settings easier.

Insight RS contains default device groups created when devices are discovered. Devices belonging to these groups are automatically assigned to these device groups. Create additional device groups to further group your devices based on your individual needs.

To create a custom device group, complete the following steps:

1. In the main menu, select **Device Groups**.
2. In the List of Device Groups pane, click **Add New Group**.
3. In the Create New Device Group pane, type a name for the group in the Device Group Name field.
4. In the Custom Delivery ID field, type the optional alphanumeric value if one has been supplied to you by your HPE representative. This field allows you to assign a Custom Delivery ID to a group of devices rather than assigning the ID to devices individually.
5. Click **Save Group Name**. The system creates and displays the new device group in the List of Device Groups pane. The assigned devices table appears where you can assign devices to the new device group.
6. Assign devices in the assigned devices pane. The default view shows devices not assigned to the device group. To show additional devices, click the **Not Assigned to this Device Group** or **All Devices** options. To show devices in a specific device group, select a device group from the **Filter by device group** drop-down list. To search for a specific device, type the device name into the **Search** box. The table displays the devices based on your filter and search criteria.
 - To add a device, select the check box next to the device in the devices table.
 - To remove a device, clear the check box next to the device in the devices table.
7. Click **Save Devices**.

The system creates and displays the device group in the List of Device Groups pane.

Chapter 5: Restoring from backup

Insight Remote Support provides a built-in capability to backup the Insight RS application and associated data and configuration files. The built-in Insight RS backup capability is intended to provide non-disruptive backups of the running Insight RS system using minimal resources.

The backup files can be used to restore Insight RS configuration information if the application encounters a problem and needs to be reinstalled, to recover data if it is lost, or to revert to a previous configuration as the result of a support call.

The Insight RS backup capability does not replace an OS-level backup utility such as Windows Backup. Direct restoration of Insight RS data from a system-level backup using a third party utility like Windows Backup may not be successful if the backup is taken while Insight RS is running. This is because such utilities cannot maintain time-consistency of data, particularly database data, while executing the backup if the files being backed up are concurrently being updated by the program. As a result, such utilities may be designed to block themselves or block running programs, causing user interfaces to freeze during backup. Otherwise they may capture backups that are internally inconsistent and that may not actually be useful when restored because of those inconsistencies. The built-in Insight RS backup is designed to address these issues by quickly capturing a time-consistent snapshot of its own data without disrupting its own operations.

You may wish to use a standard backup utility to backup the entire system that hosts Insight RS or to copy the Insight RS backup data sets to another location.

For information about using the backup capability, see ["Manually run backup schedules" below](#).

For information about restoring from backup, see ["Restoring Insight RS from backup" on the next page](#).

Insight Remote Support also provides a capability to export your device configuration data to a comma separated value (CSV) file. This file can be used to restore device information or to change device configuration data for multiple devices.

For information about using the export capability, see ["Export and import of device information" on page 70](#).

Manually run backup schedules

On the Administrator Settings → Schedules → Advanced Schedules section, you can run the Application Backup Schedule to backup/restore data, such as device details and configuration history. After the initial install, backups are automatically scheduled to run daily at 3:33 AM and data is restored to the selected location.

To run the Application Backup Schedule, complete the following steps:

1. In the main menu, select **Administrator Settings**.
2. Click the **Schedules** tab.
3. In the Schedules table expand the Advanced Schedules section, and click **Application Backup Schedule**. The Application Backup Schedule dialog box appears.

Schedule

Name: Application Backup Schedule

Frequency: Every Day

Time: 03 : 33

Next Scheduled Time: 12/4/2015, 3:33:00 AM

Comment: Creates scheduled backup copies of your Insight Remote Support configuration history and device details. To change the frequency, backup directory or to disable backup (not recommended), please see help.

SAVE **START NOW**



Note: To run the schedule at a different time, select the required time from the Time field and click **Save**.

4. In the Application Backup Schedule dialog box, click **Start Now**.

Insight Remote Support runs the schedule.

Viewing successful backup information

You can view the date and time of the last successful backup on the About Insight Remote Support screen of the Insight RS Console.

Identifying backup failures

If a backup fails, then a message appears on the Message Board section of the Home page of the Insight RS Console. View the error log files for details on the backup failure.

Restoring Insight RS from backup

The Insight RS restore function restores Insight RS dynamic data from a backup data set. For this to happen, Insight RS must be installed so that the correct restore target location can be determined, but Insight RS must not be running so that normal operations and restore operations will not interfere with one another. After the backup data is restored, Insight RS can be restarted.

To run the Application Backup Schedule, complete the following steps:

1. Open a command prompt window on the Hosting Device.
2. Stop the Insight RS services:


```
net stop hprsreceivers
net stop hprsmain
```
3. Restore your backup data set:


```
rsadmin restore -source <backup_data_set>
```

where *backup_data_set* is the location of your backup data set.

The default backup location is C:\ProgramData\HP\RS\DATA\backup. If you change the source location, then make sure you include the time stamp folder name, for example, E:\backup\1350683403365.

4. Restart the Insight RS services:

```
net start hprsmain
```

```
net start hprsreceivers
```

After restarting the Insight RS services, the database re-initializes with the backup data. Note that the re-initialization takes a few minutes, and the Insight RS Console will not be accessible during this time.

Chapter 6: Uninstalling Insight RS

You can use the Windows Programs and Features control panel to uninstall Insight RS.

Insight RS leaves behind configuration, monitored device, and log file information when it is uninstalled. This allows the application to be uninstalled and reinstalled under the guidance of HPE Support without losing data. Deleting this data recovers the disk space and allows a clean re-installation of Insight RS. The default locations for the data files are shown in the figure on page 27. Once Insight RS has been uninstalled, these folders can be deleted. Insight RS does not leave behind data in the registry when uninstalled.

Make sure you disable the Hosting Device in the Insight RS Console before uninstalling Insight RS to prevent any issues with Hosting Device registration if you ever reinstall Insight RS on the same Hosting Device.

To uninstall Insight RS, complete the following steps:

1. If you use HPE Insight Online, make sure your device data is removed from HPE Insight Online. See ["Disable Insight Online"](#) below.
2. ["Uninstall the Insight RS software"](#) on page 69.
3. If you believe any remaining data may be left, you can completely clean your Hosting Device by performing the steps in ["Cleanup Hosting Device"](#) on page 69.

Disable Insight Online

If you use HPE Insight Online, you need to perform the following steps to make sure your support cases and devices are removed from Insight Online before you disable the connection to Insight Online.

Close support cases

Make sure you close all support cases associated with the Hosting Device so the support case are removed from Insight Online.

To view and close service events for a device, complete the following steps:

1. In a web browser, log on to the Insight RS Console.
2. In the main menu, select **Service Events**, and click the Event Status column to sort the results to show open service events.
3. Record the Case ID, which you will need to close the support case.
4. Close any open support cases:
 - Use the HPE Support Center Support Case Manager and request that open cases be closed. Note that cases are not automatically closed as the result of a request. A support agent closes the case after reviewing the request.
 - Contact your support representative to close open support cases.

Delete devices from Insight RS Console

Uninstalling the Insight RS software does not remove your devices from HPE Insight Online. You must manually delete your devices in the Insight RS Console, which also removes the devices from HPE Insight Online. Deleting a device removes all event and configuration collection history from the Hosting Device and disables the device in HPE Insight Online, if configured.

To delete a device, complete the following steps:

1. In a web browser, log on to the Insight RS Console.
2. In the main menu, select **Devices**, and then click the **Device Summary** tab.
3. Select the check box in the far left column for all devices.
4. Click **Actions** → **Delete Selected**, and click **OK** in the confirmation dialog box.



Note: When a monitored device sends an SNMP packet to the Hosting Device, the Insight RS automatically attempts to re-register the monitored device. To make sure this does not happen before uninstalling Insight RS, remove the Hosting Device as a trap destination on your monitored devices or disable the SNMP receiver service on the Hosting Device.

Disable connection to HPE Insight Online

Disabling the HPE Insight Online integration removes all details of remotely supported devices in HPE Insight Online for the registered HPE Passport account. This also disables the same device details for any users for which this data was shared as well as the view of your HPE Authorized Channel Partner, if configured.

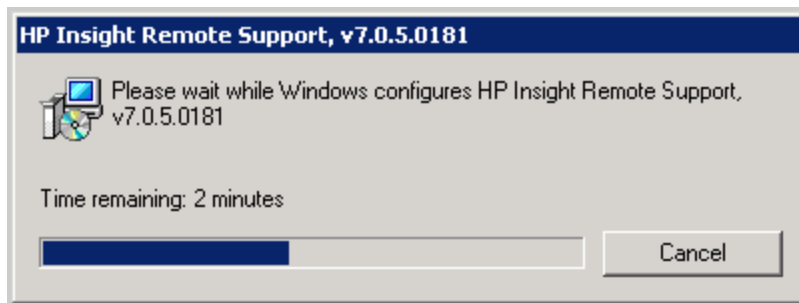
To disable Insight Remote Support from sending data to Insight Online, complete the following steps:

1. In a web browser, log on to the Insight RS Console.
2. In the main menu, select **Administrator Settings**.
3. Click the **HPE Insight Online** tab.
4. Click **Disable Insight Online View**.
5. In the Confirm Disable dialog box, click **OK** to confirm.
6. Log on to your HPE Insight Online account and make sure that the devices no longer appear on the dashboard.

Uninstall the Insight RS software

To uninstall Insight RS, complete the following steps:

1. On the Hosting Device, navigate to **Start** → **Control Panel** → **Programs and Features**.
2. Select **HPE Insight RS, v7.x** and click **Uninstall**.
3. Click **Yes** to confirm that you want to uninstall Insight RS. The HPE Insight RS, v7.x uninstall window appears showing the progress of the uninstall.



When it completes, Insight RS is removed from the Programs and Features window.

4. Delete the Insight RS data files, if desired. The default locations for the data files are shown in the figure on page 27.


Cleanup Hosting Device

After uninstalling HPE Insight RS, HPE recommends the following cleanup to make sure any monitored device or company information is removed from the server. Complete these steps to make sure the Hosting Device no longer contains any of your company information.

1. Wipe the attached storage devices following your security policy.
2. Reset the BIOS and firmware to factory defaults.

Appendix A: Export and import of device information

The bulk upload functionality allows you to submit monitored device configuration information for multiple devices through a scripted process, rather than updating each individual system through the Insight RS Console. The bulk upload file stores the required information for selected monitored devices. When the file is imported, this information is used to supply unique information (including warranty and contract information) for each monitored device. Provide the monitored device information in a comma separated value (CSV) file, one device per line.

 **Important:** For security reasons, protocol credential information is not saved in the CSV file. After loading the CSV file, protocol credential information must be reconfigured for each device.

Export a bulk CSV file

To export a bulk CSV file, complete the following steps:


1. Open a command prompt window on the Hosting Device.
2. Export the CSV file using the following command and the path to where you want to save the CSV file:


```
rsadmin unload -file C:\[filepath]\[filename].csv
```

The system downloads the devices from Insight RS and saves them to a CSV file.

Import a bulk CSV file

You can import previously edited bulk CSV files. See ["Edit a bulk CSV file" on the next page](#) for information about editing bulk CSV files.

 **Important:** Make sure you register Insight RS in the Hosting Device Setup Wizard before performing this command. Running this command before registration can lead to data integrity issues during the registration process.


 **Important:** A hard line break (carriage return) is required at the end of each series of system fields. If one of the fields does not apply, leave the field empty, but do not delete the comma delimiter.

To upload a bulk CSV file, complete the following steps:

1. Open a command prompt window on the Hosting Device.
2. Import the CSV file using the following command and the full path to the CSV file:

```
rsadmin load -file C:\[filepath]\[filename].csv
```

The system uploads the devices from the CSV file and lists them in the Insight RS Console.

 **Note:** If attempting to use the `rsadmin` command right after installing Insight RS, the path environment may not immediately be updated. If the `rsadmin` command is not found, and you just completed the installation, you may need to log off and then log on to the Hosting Device to make sure the needed environment variables have been updated.

Edit a bulk CSV file

You can edit the bulk CSV file that you exported from Insight RS and then import the information. The file can be edited with a text editor or a spreadsheet program. The table below shows the structure of the of bulk CSV file.



Important: If any of the values in the CSV file contain commas, you need to wrap the value in quotation marks, otherwise the comma will cause the CSV file to not load properly, resulting in an error.

Table A.1 CSV file data fields (in the order in which they should be provided)

Field	Description
SYSTEM_NAME	Fully qualified host name of the monitored device.
SYSTEM_IP	IP address for the monitored device.
SERIAL_NUMBER	Serial number for the monitored device.
PRODUCT_ID	Product number for the monitored device.
COUNTRY_CODE	Country code for the location where the support contract was initiated. You can find your country code at the International Organization for Standardization web site at: http://www.iso.org/iso/home/standards/country_codes.htm .
ENTITLEMENT_TYPE	The contract type. Possible options are: 'SAID,' 'Warranty.'
ENTITLEMENT_ID	The contract ID.
CUST_DELIVERY_ID	A vendor or HPE provided identifier.
CUST_SERIAL_NUM	A customer serial number different from that provided by the system itself.
CUST_PRODUCT_ID	A customer product number different from that provided by the system itself.
SITE_NAME	The location where the monitored device is located. If you have a large campus it might be a facility nickname or other identifying factor for the site location.
SITE_ADDRESS1	Address for the site of the monitored device.
SITE_ADDRESS2	Suite for the site of the monitored device.
SITE_CITY	City for the site of the monitored device.
SITE_STATE	State or province for the site of the monitored device.
SITE_COUNTRY	Country code for the location where the monitored device is physically located. You can find your country code at the International Organization for Standardization web site at:

Table A.1 CSV file data fields (in the order in which they should be provided), continued

Field	Description
	http://www.iso.org/iso/home/standards/country_codes.htm .
SITE_POSTALCODE	Postal Code for the site of the monitored device.
SITE_TIMEZONE	Timezone for the site of the monitored device.
CONTACT1_ROLE	Role of primary contact supporting this monitored device. Must be text 'Primary Contact.'
CONTACT1_FIRSTNAME	Primary contact's first name.
CONTACT1_LASTNAME	Primary contact's last name.
CONTACT1_EMAIL	Primary contact's email address.
CONTACT1_PHONE	Primary contact's primary phone number.
CONTACT1_ALTPHONE	Primary contact's alternate phone number.
CONTACT1_HOURS	Available hours to reach primary contact.
CONTACT1_SALUTATION	Mr., Mrs., Ms., Dr., etc.
CONTACT1_LANGUAGE	Primary contact's preferred language.
CONTACT1_TIMEZONE	Timezone for the area where the primary contact lives.
CONTACT1_OTHER	Free text notes about the primary contact.
CONTACT2_ROLE	Role of secondary contact supporting this monitored device. Must be text 'Secondary Contact.'
CONTACT2_FIRSTNAME	Secondary contact's first name.
CONTACT2_LASTNAME	Secondary contact's last name.
CONTACT2_EMAIL	Secondary contact's email address.
CONTACT2_PHONE	Secondary contact's primary phone number.
CONTACT2_ALTPHONE	Secondary contact's alternate phone number.
CONTACT2_HOURS	Available hours to reach secondary contact.
CONTACT2_SALUTATION	Mr., Mrs., Ms., Dr., etc.
CONTACT2_LANGUAGE	Secondary contact's preferred language.
CONTACT2_TIMEZONE	Timezone for the area where the secondary contact lives.
CONTACT2_OTHER	Free text notes about the secondary contact.
SUPPORT_CHANNEL_PARTNER_NAME	Name of HPE Authorized Service Partner.
SUPPORT_CHANNEL_PARTNER_ID	ID of HPE Authorized Service Partner.
SUPPORT_CHANNEL_PARTNER_CITY	City of the HPE Authorized Service Partner.

Table A.1 CSV file data fields (in the order in which they should be provided), continued

Field	Description
SUPPORT_CHANNEL_PARTNER_COUNTRY	Country of the HPE Authorized Service Partner.
SERVICE_CHANNEL_PARTNER_NAME	Name of Authorized Reseller.
SERVICE_CHANNEL_PARTNER_ID	ID of Authorized Reseller.
SERVICE_CHANNEL_PARTNER_CITY	City of the Authorized Reseller.
SERVICE_CHANNEL_PARTNER_COUNTRY	Country of the Authorized Reseller.
ENTITLEMENT_IS_ENTITLED	True or false value for whether the monitored device is entitled for remote support.
ENTITLEMENT_PACKAGE	The Service Level Agreement (SLA) that covers the monitored device.
ENTITLEMENT_OFFER_START_DATE	The start date of the device's warranty or contract.
ENTITLEMENT_OFFER_END_DATE	The expiration date of the device's warranty or contract.
ENTITLEMENT_COVERAGE_DAYS	Days covered in a week.
ENTITLEMENT_COVERAGE_HOURS_DAY_1_TO_5	Coverage hours for days 1 to 5, Monday through Friday.
ENTITLEMENT_COVERAGE_HOURS_DAY_6	Coverage hours for Day 6, Saturday.
ENTITLEMENT_COVERAGE_HOURS_DAY_7	Coverage hours for Day 7, Sunday.
ENTITLEMENT_COVERED_HOLIDAYS	True or false value for whether the monitored device's warranty or contract coverage includes holidays.

Glossary

A

Agentless Management Service (AMS)

iLO 4 Agentless Management uses out-of-band communication for increased security and stability. With Agentless Management, health monitoring and alerting is built into the system and begins working the moment a power cord is connected to the server. This feature runs on the iLO hardware, independent of the operating system and processor. The separately installed AMS collects additional operating system data.

C

CDID

See Custom Delivery ID.

Central Management Server (CMS)

The CMS is a system in the management domain that executes the HPE Systems Insight Manager software. All central operations within HPE Systems Insight Manager are initiated from this system.

Centralized Management Console (CMC)

The CMC is used to configure and manage the P4000 Storage Systems.

CLIQ

Legacy term for the LeftHand OS command line interface. See P4000 CLI.

cluster

A cluster is a grouping of storage nodes that create the storage pool from which you create volumes.

collection schedules

The frequency in which collections are run. The schedule is configurable in the Insight RS Console.

collections

The term within HPE SIM for grouping system or event searches. While HPE SIM uses the term collection in reference to a group of monitored devices, Insight Remote Support uses the term configuration collection in reference to data collected from a monitored device. This data is communicated to HPE for proactive analysis.

configuration collection

HPE Insight Remote Support uses the term configuration collection in reference to data collected from a monitored device. This data is sent to HPE for proactive analysis.

Custom Delivery ID

The Custom Delivery ID is a free text field that can be individually populated for each monitored device. Unless a specific value is specified within the documentation relating to configuring a particular device, the field should be left blank. In some very specific circumstances, this field may also be populated by an HPE Representative to allow customized handling/routing of reported incidents. In those instances, the field must be populated with a unique value associated with the customized handling that is required. Determination of the unique value must be done by the HPE Representative working with the HPE Automation Team TS that sets up the customizations. Failure to follow this guidance could result in incorrectly handled incident reports.

D

device groups

Configurable groups of devices within the Insight RS Console that helps users organize the devices in their environment.

discovery

A feature within a management application that finds and identifies network objects. In HPE management applications, discovery finds and identifies all the devices within a specified network range.

E

Enterprise Virtual Array (EVA)

An EVA is a high performance, high capacity and high availability virtual RAID storage solution for high-end enterprise environments.

entitlement

The process of authorizing a request for support based on the contents of warranty or support contracts held by the customer, normally with respect to a specific Object of Service (OOS) such as a hardware or software component. Your level of entitlement is determined by your HPE Support contract. Contact your HPE Account Team for more details.

event

A general term for all types of notifications from one process to another.

Event Log Monitoring Collector (ELMC)

ELMC provides error condition detection of the event log and communicates these events to Insight RS.

H

hardware event

A specific type of event that suggests that a specific hardware component may be in trouble. Hardware events may result in a service event.

Health Check

The LeftHand Networks Health Check Utility is used to send monitoring log file information from customer sites to LeftHand Networks for troubleshooting and proactive health monitoring. See Service Console.

Hosting Device

The Hosting Device is a supported Windows ProLiant server that hosts the Insight Remote Support software. When used with HPE Systems

Insight Manager, the Hosting Device can act as a Central Management Server (CMS).

Hosting Device Setup Wizard

Step-by-step screens that helps users with the initial configuration of their Hosting Device.

HPE Authorized Reseller/Distributor

Channel partners who sell hardware and services.

HPE Authorized Service Partner

Channel partners who deliver services and/or installation service on HPE's behalf.

HPE Passport

HPE Passport single sign-in service lets you use one user ID and password of your choice to sign-in to all HPE Passport-enabled Web sites.

I

identification

An aspect of the discovery process that identifies the management protocol and type of system.

iLO

Integrated Lights-Out. Embedded server management technology that delivers web-based remote management that is always available.

iLO Remote Insight Board Command Language (RIBCL)

Communication protocol required for Insight Remote Support to communicate with ProLiant Gen8 servers.

Insight Online

HPE Insight Online provides one-stop personalized, secure access to support the devices in your IT environment. It is integrated into HPE Support Center for your IT staff who deploy, manage and support systems, plus HPE Authorized Channel Partners who support your IT infrastructure. Insight Online can automatically discover devices remotely monitored by HPE

(requires Insight Remote Support 7.0 or later). Depending on your support model you or your HPE Authorized Channel Partner can easily organize your devices into groups and have the flexibility to efficiently monitor, track and service your HPE devices.

Insight Remote Support

HPE Insight Remote Support provides proactive remote monitoring, diagnostics, and troubleshooting to help improve the availability of supported HPE servers and storage systems in your data center. HPE Insight Remote Support reduces cost and complexity through support of systems. HPE Insight Remote Support securely communicates hardware incident information through your firewall and/or web proxy to the HPE Data Center for reactive support. Additionally, based on your support agreement, system information can be collected for proactive analysis and services

Insight RS Console

The Insight Remote Support user interface that is installed on the Hosting Device.

Insight RSA

Insight Remote Support Advanced. Previous version of Insight Remote Support that integrates with HPE SIM to provide proactive remote monitoring, diagnostics, and troubleshooting of devices.

M

management group

A collection of one or more storage nodes which serves as the container within which you cluster storage nodes and create volumes for storage.

Management Information Base (MIB)

The data specification for passing information using the SNMP protocol. An HPE MIB is also a database of managed objects accessed by network management protocols.

management protocol

A set of protocols, such as WBEM, HTTP, or SNMP, used to establish communication with discovered systems.

monitored device

Any device monitored by HPE Insight Remote Support, such as servers, storage systems, and switches. To monitor a device, some type of management protocol (for example, SNMP or WBEM) must be present on the device.

Monitored Device Setup Wizard

Step-by-step screens that helps users discover devices in their environment to be monitored. Users specify the range of devices to be discovered and the corresponding credentials.

O

OA

Onboard Administrator. The Onboard Administrator for the BladeSystem enclosures is the intelligence of the c-Class infrastructure. The Onboard Administrator provides both local and remote administration of BladeSystem c-Class enclosures.

P

P4000 CLI

The P4000 CLI is the command line interface that is used to interface with the P4000 Storage Systems from the Hosting Device. The P4000 CLI is installed with Insight Remote Support. Note that the P4000 CLI is sometimes referred to as cliq, which is the name of the command used within the P4000 CLI.

R

Remote Support Eligible Systems

Systems that are eligible for Remote Support, and when enabled will submit events to the HPE Data Center for incident resolution. Systems

must also be entitled to Remote Support, otherwise submitted events will be closed. You can verify that an eligible system is actually supported by using the Remote Support Entitlement Check.

Remote Support Entitlement Check (RSEC)

The RSEC is a check against the HPE entitlement datastore for the current obligation status of a particular system. The Entitlement window displays the results of the Remote Support Entitlement Check.

RIBCL

See iLO Remote Insight Board Command Language.

S

Secure Sockets Layer (SSL)

Secure Sockets Layer is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

Service Console

The Service Console is the legacy software that enabled remote hardware and software support for P4000 Storage Systems. This functionality is now provided by Insight Remote Support. See Health Check.

service event

Insight RS monitors a customer's hardware environment for service events that require action from the Service Provider (HPE Channel Partner and/or HPE services team) or customer. For the most part, actionable service events require replacing a failed Field Replaceable Unit (FRU) or Customer Replaceable Unit (CRU) in the monitored hardware. Non-actionable events are filtered out, and actionable service events are forwarded to HPE. Insight RS monitors hardware for hard failures from a major component on the hardware such as CPU, disk, memory, and power supply, and these will trigger a service

event communication to HPE. In addition, Insight RS monitors hardware for soft errors, and in some instances, when the number of soft errors exceeds a specific threshold, an event is sent to HPE. Further details regarding what classifies as an actionable service event is HPE confidential information.

Simple Network Management Protocol (SNMP)

One of the management protocols supported by Insight Remote Support. Traditional management protocol used extensively by networking systems and most servers. MIB-2 is the standard information available consistently across all vendors.

SNMP trap

Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.

Storage Area Network (SAN)

A SAN is a network of storage devices and the initiators that store and retrieve information on those devices, including the communication infrastructure. In large enterprises, a SAN connects multiple servers to a centralized pool of disk storage. Compared to managing hundreds of servers, each with their own disks, SANs improve system administration.

Storage Management Server (SMS)

A system on which HPE Enterprise Virtual Array (EVA) software is installed, including HPE P6000 Command View and HPE Replication Solutions Manager, if used. It is a dedicated management server that runs EVA management software exclusively.

System Fault Management (SFM or SysFaultMgmt)

SFM is the HPE-UX fault management solution that implements WBEM standards. SFM integrates with other manageability applications like HPE SIM, HPE SMH, and other WBEM-based clients.

system health

Health status is an aggregate status all of the status sources (which can be SNMP, WBEM, and HTTP) with the most critical status being displayed.

System Management Homepage (SMH)

System Management Homepage (SMH) is a web-based interface that consolidates and simplifies single system management for HPE servers on HPE-UX, Linux, and Windows operating systems.

Systems Insight Manager (SIM)

SIM is a unified server and storage management platform. From a single management console, administrators can manage their complete HPE server and storage environment with a secure management tool set.

T

Transport Layer Security (TLS)

Transport Layer Security is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

V

virtual node

The P4000 Virtual SAN Appliance uses captive server disk drives to build a virtual iSCSI SAN consisting of Virtual Nodes that create the storage pool from which virtualized volumes are created. Virtual Nodes can be discovered and managed in the same manner as physical Storage Nodes.

volume

A logical entity that is made up of storage on one or more storage nodes. It can be used as raw data

storage or it can be formatted with a file system and used by a host or file server.

W

Web-Based Enterprise Management (WBEM)

This industry initiative provides management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to software and hardware data that is readable by WBEM client applications.

Windows Management Instrumentation (WMI)

Microsoft's implementation of Web-Based Enterprise Management (WBEM).

workflow case

The specific HPE obligation to send a replacement part for a failed customer part.

Index

B

- backup and restore 64
 - restoring Insight RS from backup 65
 - run schedule 64
- bulk CSV file
 - edit a bulk CSV file 71
 - export a bulk CSV file 70
 - import a bulk CSV file 70

C

- certificate warning 29

D

- device groups
 - add 62
- discovery
 - device configuration 34
 - resolving device status 48
 - verifying device status 47, 49

E

- email adapter
 - configure 53
 - enable 53

H

- Hosting Device
 - access requirements 17
 - communicating with monitored devices 22
 - communication requirements 18
 - disk space requirements 11
 - DNS configuration 19
 - memory requirements 11
 - monitoring 24
 - SNMP installation 22
 - system requirements 10
 - verifying connectivity 21
- Hosting Device Setup Wizard 40
 - contact information 41
 - HPE Authorized Channel Partners 45
 - Integrate with Insight Online 44
 - receiving remote support 40
 - registering Insight Remote Support 43
 - site information 42
- HPE SIM Adapter 51
 - configure 52
 - install 51

I

- Insight RS Console 28
 - installing 25
 - downloading software 25
- integration adapters
 - HPE SIM 51

L

- log files 27

M

- Monitored Device Setup Wizard 33
 - discover devices 38
 - discovery access credentials 34
 - discovery sources 36

R

- restoring Insight RS from backup 65

S

- settings
 - enable operator-level authentication 59
- SNMP service event adapter
 - add server 55
- software requirements 16
 - .NET framework 17
 - web browsers 16
- SSLv3
 - disable 59
 - disable padded ciphers 59
 - enable 59
- system requirements 10
 - disk space requirements 11
 - hardware requirements 10
 - memory requirements 11
 - operating system requirements 14
 - software requirements 16

U

- uninstalling 67
- upgrade Insight Remote Support 9