# Contents

Terms ...................................................................................................................... 3
Related Documents.................................................................................................. 3
Overview .................................................................................................................. 3
Remote Support - Onsite .......................................................................................... 4
  Remote Device Monitoring (RDM) ......................................................................... 4
  Remote Data Collection (RDC) .............................................................................. 4
  Remote Device Access (RDA) .............................................................................. 4
HPE Remote Support - Communications .............................................................. 6
  Insight Remote Support User Interface ................................................................. 6
  HPE OneView Remote Support ............................................................................ 7
  HPE Insight Remote Support Email Adapter ......................................................... 7
  HPE Insight Remote Support Device Discovery ................................................... 7
Communication Services ....................................................................................... 10
HPE Active Health System .................................................................................... 14
Insight Remote Support ......................................................................................... 14
  Event Management ............................................................................................. 14
  Data Collections ................................................................................................ 14
Logging ................................................................................................................... 15
Data Sent to HPE .................................................................................................... 15
Email Notifications ............................................................................................... 16
Insight Remote Support at HPE .............................................................................. 18
  HPE Data Centers ............................................................................................. 18
  Data Stored at HPE ............................................................................................ 19
  Data Orchestration ............................................................................................. 19
  Event Processing ............................................................................................... 19
  Event Filtering ................................................................................................... 19
Entitlement ............................................................................................................... 19
Event Correlation ................................................................................................. 20
Collection Processing ........................................................................................... 20
HPE Insight Online ............................................................................................... 21
  HPE Support Center .......................................................................................... 21
  HPE Passport ..................................................................................................... 21
GLOSSARY of Terms ............................................................................................ 22
Terms
Throughout this document, the term “HPE Remote Support” will refer to both “HPE Insight Remote Support”, including Insight Online direct connect and “HPE OneView Remote Support” collectively.

HPE Insight Remote Support is a platform that enables automated remote monitoring and event notification for virtually any HPE hardware product. Automated notification will transmit failure events and relevant device configuration details to HPE for analysis and repair. Learn more about HPE Insight Remote Support here. [https://www.hpe.com/us/en/services/remote-it-support.html](https://www.hpe.com/us/en/services/remote-it-support.html)

HPE OneView is a virtual management appliance that simplifies the management of Hybrid IT environments. For HPE OneView, this document covers only the security capabilities of HPE OneView Remote Support. Learn more about HPE OneView, visit the HPE OneView information page here: [https://www.hpe.com/us/en/integrated-systems/software.html](https://www.hpe.com/us/en/integrated-systems/software.html)

Related Documents

- HPE Insight Remote Support 7.9 Release Notes
- HPE Insight Remote Support 7.9 Upgrade Guide
- HPE Insight Remote Support 7.9 Quick Installation Guide
- HPE Insight Remote Support 7.9 Installation and Configuration Guide
- HPE Insight Remote Support 7.9 Monitored Devices Configuration Guide
- HPE Remote Support Enablement in HPE OneView 4.1 – Frequently Asked Questions
- HPE OneView 4.1 Support Matrix
- HPE 3PAR StoreServ Secure Service Architecture
- HPE Remote Device Access Security Whitepaper

This document describes the security aspects of both the HPE Insight Remote Support and HPE OneView Remote Support solutions and their components. It describes the security features and capabilities of these solutions. Related documents can be found on the Hewlett Packard Enterprise Information Library ([https://www.hpe.com/info/insightremotesupport/docs](https://www.hpe.com/info/insightremotesupport/docs) and [https://www.hpe.com/info/oneview/docs](https://www.hpe.com/info/oneview/docs))

Overview
Today’s IT department plays a central role in meeting business objectives. Leveraging your IT infrastructure investments and improving overall system availability and utilization are crucial in today’s business environment. HPE Remote Support simplifies the management of highly diverse IT environments by providing automated failure detection and reporting as well as advanced analytics for your IT environment. HPE Remote Support can automatically detect and analyze problems in your IT environment. If a repair is necessary, HPE Remote Support will automatically log a support case and dispatch it to HPE Support for resolution.

Today, many security-sensitive transactions—such as e-commerce, stock trades, and online banking—are executed securely over the Internet using the same secure electronic transfer technology utilized by HPE Remote Support.

HPE understands and shares your company’s security and privacy concerns and has leveraged its experience as a technology leader to create a secure remote support solution.

HPE Remote Support provides a multilevel, layered security structure through encryption, authentication, standard security protocols, and industry best practices integrated at the physical, network, application, and operational levels. Interactions between HPE and your enterprise network are restricted and tightly controlled through one or more secure access points.
HPE’s remote monitoring and support capabilities, along with any support information collected, are used only to provide you with world-class HPE support. All data collected by HPE Remote Support is treated as confidential and handled in accordance with HPE’s strict data management policies.

Remote Support - Onsite

HPE Insight Remote Support is a Windows based support application that enhances the support experience by automating routine support tasks. HPE Insight Remote Support requires Windows Administrator credentials to install, configure and manage the application settings. Once installed, HPE Insight Remote Support can be configured to use Active Directory for user authentication. Insight Remote Support provides comprehensive product coverage for a wide range of supported devices. See the Insight Remote Support 7.9 Monitored Devices Support Matrix for a complete list of supported devices. [https://www.hpe.com/info/insightremotesupport/docs](https://www.hpe.com/info/insightremotesupport/docs).

HPE OneView is an Infrastructure Management appliance that has broad infrastructure management capabilities beyond remote support. Similar to HPE Insight Remote Support, HPE OneView Remote Support provides automated support capabilities for devices managed by HPE Oneview. See the HPE Oneview Support Matrix for a complete list of supported devices [https://www.hpe.com/info/oneview/docs](https://www.hpe.com/info/oneview/docs).

HPE Direct Connect (aka Embedded Remote Support) allows supported HPE ProLiant Servers and BladeSystem enclosures to enable remote support by connecting directly (or via an internet proxy) to HPE from an iLO or OA Management Interface. HPE Direct Connect devices can be viewed from anywhere at any time by registering them with HPE Insight Online in the Hewlett Packard Enterprise Support Center.

All of these options have the following three capabilities.

Remote Device Monitoring (RDM)

RDM monitors supported devices in your environment by listening for event messages from the device’s local diagnostic monitors. Diagnostic monitor event messages are analyzed by Remote Support and if it is determined that preventative or corrective action by HPE is needed. Event data is automatically sent to HPE where it will be further analyzed and processed. If further analysis indicates that a response by HPE is necessary, a support case will be created and the appropriate HPE support teams will be immediately notified of the issue. RDM is a required component of HPE Remote Support.

Remote Data Collection (RDC)

Many of the devices in today's IT environment can have complex configurations. HPE Remote Support has the ability to collect configuration information for devices on a scheduled basis and send this information to HPE. HPE can use this information to help restore your device configuration after a hardware component has been replaced. HPE can also use the device configuration information for proactive services, looking for configuration anomalies, and reporting them to you before they result in unplanned downtime. RDC is a required component of HPE Remote Support.

Remote Device Access (RDA)

Remote Device Access gives your IT System Administrators the ability to allow authorized HPE personnel access to your environment in a secure and controlled way. HPE understands that security policies may vary from customer to customer. Therefore HPE offers several secure remote access options to choose from, all of which provide a secure and controlled connection for HPE authorized support personnel into your network. RDA is an optional component for HPE Remote Support. More information about RDA security can be found in the Remote Device Access Security Whitepaper in the Whitepaper section of the HPE Insight Remote Support Information Library.
Figure 1: Insight Remote Support Onsite Architecture
HPE Remote Support - Communications

There are several communication methods used in Insight Remote Support. These include: Device Discovery, Event Management, Data Collection, Data sent to HP, Data Management at HP, and accessing data using Insight Online.

Insight Remote Support User Interface

Active Directory User Authentication

Insight Remote Support provides an optional feature to use Active Directory (AD) authentication to access the Insight RS Console. When not enabled, Insight Remote Support uses the Windows accounts on the local Hosting Device's Windows OS to identify and authenticate Insight Remote Support users.

When Insight RS AD authentication is enabled:

- All login access authentication is controlled by AD rather than the local system accounts on the Insight RS Hosting Device
- You must specify one, and only one, AD group to be recognized as admin users within Insight RS
- You may specify one, and only one, AD group to be recognized as non-admin users within Insight RS
- Any user attempting to log in that is not in one of the two above groups will not be authenticated
- Once the feature is enabled, the local Hosting Device's Windows accounts will no longer be allowed to log in

To configure Active Directory user authentication for a Hosting Device, open an administrator Windows Command window; at the command prompt type the ‘rsadmin’ command below and follow the command line interface (CLI) prompts:

    rsadmin auth -activeDirectory

For more information on configuring Active Directory authentication refer to the HPE Insight Remote Support Installation and Configuration Guide in the HPE Information Library.
Operator Level User Authentication (Windows Authentication Only)
The Insight RS Console allows a system administrator to view configuration details about devices in their enterprise. User access to the Insight RS Console is controlled by the Windows account settings. Users in the Windows Administrator group will have full access in the Insight RS User Interface. Non-Administrator (operator-level) user access is the default setting. Administrator-level access to the Insight RS Console can be granted to all users by checking the box as shown below in the Administrator Settings → Settings tab:

Password management for the Insight RS Console is managed at the Operating System level by default. Password management can be set to use Active Directory/LDAP using the ‘rsadmin’ CLI. When using Active Directory authentication, operator level users cannot be granted administrative access using this setting. Local access passwords are not stored within the application. To access the Insight RS Console, open a browser window (see Release Notes for a full list of supported browsers), and browse to the URL: https://<hosting_device_IP|Full_Domain_Name>:7906 and enter your user credentials in the Username: and Password: boxes.

HPE OneView Remote Support
HPE OneView Remote Support Supports ProLiant servers (Gen 8 and above) and BladeSystem enclosures, and interconnects including Synergy (refer to the HPE OneView Support Matrix for a full list of supported devices). Devices configured to use HPE OneView Remote Support use the same services and protocols as HPE Insight Remote Support. Oneview Remote Support is enabled via the settings menu in HPE OneView. Devices configured to use OneView Remote Support will be automatically unregistered from HPE Insight Remote Support and marked as disabled. If you wish to restore device monitoring to HPE Insight Remote Support, you must disable HPE OneView Remote Support and then re-register the devices in HPE Insight Remote Support. For more information see the HPE OneView Remote Support Enablement in HPE OneView 4.1 FAQ on the HPE OneView Information Library at: https://www.hpe.com/info/OneView/docs.

HPE Insight Remote Support Email Adapter
HPE Insight Remote Support and HPE OneView Remote Support can notify the (default and backup) device contacts via email when certain events occur. Email notification can be configured in the Integration Adapters tab in Administrative Settings menu of the Insight RS Console and under Edit Notifications in the HPE OneView Settings menu.

HPE Insight Remote Support Device Discovery
Device Discovery is used to scan your network, a portion of your network, or discover a single device. Device Discovery searches for potential devices to be included in Remote Device Monitoring (RDM) and the Remote Device Collections
(RDC). Device Discovery uses standard network management protocols (like Simple Network Management Protocol – SNMP and Web-based Enterprise Management – WBEM) to identify devices connected to your network (see: Chapter 3 of the Installation and Configuration Guide). For each device discovered on your network, the discover engine will attempt to communicate with it using all available services (listed in table 1 below). The discovery will identify all possible communication methods and allow the administrator to select the best one for the target device. Network management protocol passwords are encrypted using Advanced Encryption Standard 128 (AES-128) and stored in the Insight Remote Support database on the Hosting Device. These protocols must be configured in the Discovery → Credentials tab prior to discovery in order to properly identify devices on your network. The discovery engine can add devices the following ways:

- Scan using an IPv4 address, a list of IPv4 addresses or range of IPv4 addresses
  - This is the most restrictive method, allowing the administrator to target specific devices or a specific subnet range for device discovery
- Scan using a Windows Domain Group
  - This allows the Hosting Device administrator to discover all devices in a Windows Domain. This option requires the Window Domain administrator username and password to be configured in the discovery engine on the hosting device
- Scan a LAN Subnet or all LAN Subnets
  - This allows the Windows Administrator to automatically discover all devices contained in a LAN Subnet. The Subnet range is defined by the LAN IP/Network Mask. This can be the entire network (or networks) or any subnet network range within your enterprise with IP Routing enabled from the Hosting Device

Device Discovery will scan your network for possible monitored devices using all available management protocols. These include:
Table 1: Device Discovery Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol/Port</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP*</td>
<td>_</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>TCP Ping*</td>
<td>TCP/80</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>DCOM*</td>
<td>TCP/135</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>ELMC</td>
<td>TCP/7920</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>HTTP*</td>
<td>TCP/80</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP/443</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>P4000 CLI API</td>
<td>TCP/5989</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>P6000 CV</td>
<td>TCP/2372</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>REST</td>
<td>TCP 443</td>
<td>Hosting Device</td>
<td>HPE Web API</td>
</tr>
<tr>
<td>RIBCL</td>
<td>TCP/443</td>
<td>Hosting Device</td>
<td>Monitored iLO Device</td>
</tr>
<tr>
<td>SNMPv1*</td>
<td>UDP/161</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>SNMPv2*</td>
<td>UDP/161</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>UDP/161</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>SSH</td>
<td>TCP/22</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>Telnet*</td>
<td>TCP/23</td>
<td>Hosting Device</td>
<td>Monitored Network Device</td>
</tr>
<tr>
<td>VMware vCenter</td>
<td>TCP/443</td>
<td>Hosting Device</td>
<td>VMware vCenter Server</td>
</tr>
<tr>
<td>WS-MAN</td>
<td>TCP/443</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>WS-MAN</td>
<td>TCP/5986</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>WBEM</td>
<td>TCP/5989</td>
<td>Hosting Device</td>
<td>Monitored Device</td>
</tr>
<tr>
<td>WS-MAN</td>
<td>TCP/7905</td>
<td>Monitored Device</td>
<td>Hosting Device</td>
</tr>
<tr>
<td>WMI#</td>
<td>TCP/135</td>
<td>Hosting Device</td>
<td>Monitored Windows Server</td>
</tr>
</tbody>
</table>

*ICMP, TCP Ping, DCOM, HTTP, SNMPv1, SNMPv2 and Telnet are unencrypted protocols

#WMI is a DCOM service to configure your firewall to support DCOM services see: [http://support.microsoft.com/kb/832017](http://support.microsoft.com/kb/832017). To restrict WMI to a specific port see: [http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447%28v=vs.85%29.aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447%28v=vs.85%29.aspx)
Communication Services
The following services are used by HPE Remote Support for one or more of the following tasks: Remote Device Monitoring (Device Discovery and Event Notification); Remote Data Collection; Remote Device Access.

DCOM
The Distributed Component Object Model (DCOM) is a Windows protocol that enables software components to communicate directly over a network. Previously named “Network OLE”, DCOM is designed for use across multiple network transports, including Internet protocols such as HTTP and WMI (Windows Management Instrumentation).

DCOM allows processes to be efficiently distributed to multiple computers so that the client and server components of an application can be placed in optimal locations on the network. Processing occurs transparently to the user because DCOM handles this function. Thus, the user can access and share information without needing to know where the application components are located. If the client and server components of an application are located on the same computer, DCOM can be used to transfer information between processes.

ELMC
The Event Log Monitoring Collector (ELMC) is a proprietary management service included with Insight Remote Support. ELMC is platform-specific and provides error condition detection on the monitored endpoint system on which it is installed. It communicates these events to Insight RS on the Hosting Device, which can be running either on the same system as the ELMC system or another system on the same TCP/IP network. Different ELMC packages exist for the same ELMC version, depending on the operating system and hardware platform.

ESP
Encapsulating Security Payload (ESP), or IP protocol 50, is a protocol header inserted into an IP datagram to provide data encryption and authentication. Remote Device Access uses ESP in tunnel mode to establish VPN connectivity. ESP is described in RFC 4303.

HTTP
The Hypertext Transfer Protocol (HTTP) is an application-layer protocol used for exchanging data. HTTP is described in RFC 2616. Its most popular usage is for transferring text, graphic images, sound, video, and other multimedia files to Web browsers. HTTP capabilities are also general enough for non-web applications. HTTP communications are unencrypted. HTTP typically uses Transmission Control Protocol (TCP) port 80. HTTP is used by HPE Remote Support to discover monitored devices and communicate with older network devices that do not support encrypted communications.

HTTPS
HTTPS is HTTP over Transport Layer Security (TLS) or HTTP over Secure Sockets Layer (SSL) for encrypted communications. All communications between the Hosting Device and the HPE Remote Support Data Center are carried out over HTTPS (TLSv1.2). HTTPS is also used for the marshalling and transfer of collected device data between the Hosting Device and the monitored systems. HTTPS typically uses TCP port 443, but other services, like Remote Insight Board Command Language (RIBCL) and Web-Based Enterprise Management (WBEM), may specify a different port number for HTTPS communications. SSL was originally developed by Netscape Communications. It is considered less secure than TLS. Insight Remote Support can support for SSLv3 and TLS 1.0 protocols if required in order to support for older devices. SSLv3 and TLS 1.0 is disabled by default, but can be enabled by a system administrator using the 'rsadmin' command. HTTP over TLS is described in RFC 2818.

ICMP
Internet Control Message Protocol is a network status reporting protocol used by network devices to report back to the source IP address the status of IP packets. Occasionally a gateway or destination host will communicate with a source host, for example, to report an error in datagram processing. ICMP is used for this purpose. ICMP is an integral part of the IP Protocol and is implemented in every module. HPE Remote Support uses ICMP echo request packets for device discovery and host availability status. ICMP is described in RFC 792.
**IPSec**

IP Security, or IPSec, is a suite of protocols for securing IP communications. IPSec operates in two modes. In transport mode it can be configured to provide end-to-end security of all communications between two systems. In tunnel mode, IPSec can be used to provide Virtual Private Network (VPN) connectivity over insecure networks. A typical IPSec deployment uses two protocols: Internet Security Association and Key Management Protocol (ISAKMP) and either Encapsulating Security Payload (ESP) or Authentication Header (AH), both of which are IP protocols. AH is seldom used as it does not provide encryption. IPSec is described in [RFC 4301](https://www.rfc-editor.org/rfc/rfc4301).

**IKEv2**

Internet Key Exchange version 2 performs mutual authentication between two parties and establishes an IKE security association (SA) that includes shared secret information that can be used to efficiently establish SAs for Encapsulating Security Payload (ESP) [see: RFC 4303] and/or Authentication Header (AH) [see: RFC 4302] and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry. In this document, the term "suite" or "cryptographic suite" refers to a complete set of algorithms used to protect an SA (Security Association). An initiator proposes one or more suites by listing supported algorithms that can be combined into suites in a mix-and-match fashion. IKE can also negotiate use of IP Compression (IPComp) in connection with an ESP and/or AH SA. IKEv2 is described in [RFC 4306](https://www.rfc-editor.org/rfc/rfc4306).

**OCSP**

The Online Certificate Status Protocol (OCSP) [RFC2560] defines a protocol for obtaining certificate status information from an online service. An OCSP responder may or may not be issued an OCSP responder certificate by the certification authority (CA) that issued the certificate whose status is being queried. An OCSP responder may provide pre-signed OCSP responses or may sign responses when queried. OCSP is described in [RFC 6277](https://www.rfc-editor.org/rfc/rfc6277).

**P4000 SAN**

The P4000 Storage Area Network (SAN) Solution (SAN/iQ) protocol is the command line interface that is used to interface with the P4000 Storage Systems from the Hosting Device. The P4000 Command Line Interface (CLI) is installed with Insight Remote Support.

**P6000 CV**

P6000 Command View is the storage management software used to monitored HPE Enterprise Virtual Array (EVA) devices. Insight Remote Support uses ELMC to monitor the array controllers for new log entries and communicates this information back to the Hosting device. The Hosting Device communicates with P6000 CV10 over TCP port 2374 (prior versions use TCP 2372) to query the software for configuration and event details.

**RIBCL**

Remote Insight Board Command Language is an HPE Proprietary Extensible Markup Language (XML) based command language for managing HPE ProLiant Servers via the Integrated Lights Out (iLO) interface. Insight RS uses RIBCL to communicate with iLO 4 & iLO 5 interfaces to gather configuration information and event details for monitored devices. RIBCL communicates using HTTPS (TCP port 443).

**SNMPv1**

Simple Network Management Protocol version 1 is a protocol developed to manage nodes (servers, routers, switches, and hubs) on an IP network. SNMPv1 is described in [RFC 1157]. SNMPv1 is an unencrypted communication service that communicates over UDP port 161. SNMPv1 is a simple request/response protocol (responses are not acknowledged). The Hosting device issues a request and a monitored device returns a response.
SNMPv2

Simple Network Management Protocol version 2 or more specifically, SNMPv2C (a subset of SNMPv2), is an extension of SNMPv1. It also is an unencrypted communication service that communicates over UDP port 161. SNMPv2 is described in RFC 1901 and includes enhanced protocol operations to the SNMPv1 protocol that include the GetBulk operation (to retrieve large blocks of data) and the Inform operation (allowing one Network Management System to send trap information to another Network Management System and receive a response or acknowledgement). If Inform operation responses are not acknowledged, the SNMP agent will resend the Inform message.

SNMPv3

Simple Network Management Protocol version 3 is an extension of SNMPv2 with additional enhancements including transport encryption capabilities and improved remote configuration and administration capabilities. SNMPv3 is widely used for management of network devices. An overview of SNMPv3 is described in RFC 3410.

SSH

The Secure Shell (SSH) protocol is an application-layer protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted, and authenticated connection between an SSH client and an SSH monitored server. SSH provides data integrity checks, prevents eavesdropping, and modification of sensitive data transferred between the Hosting Device and monitored systems. SSH typically uses TCP port 22, but alternative port numbers may be assigned to the SSH server. SSH is described in RFC 4251.

Although the SSH protocol is typically used to log into a remote machine and execute commands, it also supports tunneling, forwarding arbitrary TCP ports and X Windows System, version 11 (X11) connections. It can transfer files using the associated Secure File Transfer Protocol (SFTP) or Secure Containment Protocols (SCP).

The SSH protocol exists in two versions. Several security vulnerabilities have been identified in the original SSH protocol version 1 (SSHv1), therefore it should be considered insecure and should not be used in a secure environment. Its successor, SSH protocol version 2 (SSHv2), strengthened security by changing the protocol and adding Diffie-Hellman key exchange and strong integrity checking via message authentication codes. HPE Remote Support uses SSHv2 for all SSH connections.

TCP Ping

TCP Ping is a TCP base alternative to ICMP (Ping). TCP Ping sends a directed request to a TCP port (default port is 80) on a target IP address to determine if the host (port) is available. HPE Remote Support uses TCP Ping for host and device discovery and availability status in environments where ICMP is disabled.

TLS

Transport Layer Security (TLS) protocols are application-layer protocols which provide data encryption and authentication. TLS protocols use X.509 certificates, also known as “digital” certificates, for authentication. Although most users are accustomed to working only with server certificates, TLS can be configured to require client-side certificates which provides password-less two-way authentication. The Hosting Device and monitored devices authenticate using X.509 certificates. Also, all communications between the client browsers and the Hosting Device are protected by TLS encryption. HPE Insight Remote Support can be configured to support SSL V3 if needed, however SSv3 and TLS 1.0 are disabled by default and must be enabled by the system administrator as they are considered vulnerable to specific network base attacks. TLS protocols are most ubiquitous in HTTPS on TCP port 443. Other protocols and applications also utilize TLS for security. HPE Remote Support supports TLS 1.1 and 1.2 by default.

Telnet

Telecommunications Network (Telnet) is an application-layer protocol that was developed for providing remote terminal sessions. Some older storage devices, routers, switches, and other devices will support only telnet for network access. Although it is insecure and disabled by default, Insight Remote Support can use this protocol to provide support for these legacy devices. Telnet does not provide encrypted transport of data and is considered to be an insecure communication
service. Today, most operating systems use SSH in place of telnet as the standard terminal communication protocol. Telnet is described in RFC 854. Telnet has been assigned to TCP port 23, however it may be configured to run on other ports.

**VMware vCenter**
VMware vCenter Server provides centralized management of vSphere virtual infrastructure. VMware vCenter provides IT administrators the ability to ensure security and availability, simplify day-to-day tasks, and reduce the complexity of managing virtual infrastructure. HPE Insight Remote Support uses VMware vCenter to obtain a CIM ticket for authenticating to VMware ESXi hosts operating in lockdown mode.

**WBEM**
Web Based Enterprise Management (WBEM) is an initiative based on a set of management and Internet standard technologies developed by the Distributed Management Task Force (DMTF) to unify the management of enterprise computing environments. WBEM is really a collection of Internet standards and DMTF open standards: Common Information Model (CIM) infrastructure and schema, CIM-XML, CIM operations over HTTP, and Web Services for Management (WS-Management). The Common Information Model (CIM) provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. WS-Management is a specification of a SOAP-based protocol for the management of servers, devices, and applications. WBEM can be encapsulated inside either HTTP or HTTPS. HPE Remote Support does not support unencrypted WBEM communications. All Insight Remote Support WBEM traffic is encrypted using HTTPS on TCP port 5989.

**WS-MAN**
WS-MAN or Web Services Management is a DMTF open standard defining a SOAP based protocol for the management of servers, devices and applications. HPE Remote Support uses WS-MAN to communicate with the Superdome 2 Onboard Administrator.

**WMI**
Windows Management Instrumentation (WMI) is the Microsoft proprietary implementation of WBEM. WMI runs as a DCOM (Distributed Component Object Model) service which in turn uses RPC (Remote Procedure Call) and other associated DCOM services. The WMI Mapper is an application that provides a two way translation interface between DCOM and WBEM. WMI Mapper is required for any Windows monitored system supporting WBEM Indications to be monitored by HPE Remote Support Active Health System.
HPE Active Health System
HPE Active Health System (AHS) tracks configuration changes, events and telemetry information on ProLiant Gen8 and Gen9 servers with iLO 4 and ProLiant Gen10 servers with iLO 5 Integrated Lights-Out interfaces (iLO), enabling you to eliminate time spent running diagnostics, reproducing problems, and describing errors to HPE support engineers. Changes to the device configuration are reported to HPE Insight Remote Support or HPE OneView Remote Support using a secure (HTTPS) connection between the ProLiant Server iLO interface and the Remote Support Host. HPE Remote Support will package and forward the configuration changes to HPE over a secure HTTPS connection. Active Health System information contains no business or personal data and is not viewable locally on the remote support host. Active Health System collections may be sent to HPE regardless of the collections setting on the Remote Support Host. Device Administrator contact information is appended to AHS data prior to being sent to HPE.

Insight Remote Support
HPE Insight Remote Support stores information in specific locations on the Hosting Device. Permissions on these directories are set to deny access to all users except Hosting Device System Administrators and the Windows System account. The Installer can change the default locations for these directories during installation. The standard (default) locations for Insight Remote Support are as follows:

- Data: C:\ProgramData\HP\RS\DATA
- Log Files: C:\ProgramData\HP\RS\LOG
- Configuration Files: C:\ProgramData\HP\RS\CONFIG
- Executable Files: C:\Program Files\HP\RS

Event Management
Insight Remote Support relies on the onboard diagnostic monitors to detect hardware events on monitored devices. When events are detected, notification is sent to the Remote Support Host (and any other configured host) via one of the management protocols listed in Table 1 above. The management protocol used is determined by platform and policy. HPE Remote Support supports many device platforms (refer to the Monitored Devices Configuration Guide to determine the supported protocol for your devices).

When the Hosting Device receives an event from the managed device, the Insight Remote Support software on the Hosting Device will screen the event to determine whether or not the event may require action by HPE to address. If the analysis determines that action by HPE may be necessary, the event will be packaged with the associated device contact information stored in the Host Device configuration database and sent to HPE via HTTPS (TCP/443).

Data Collections
Insight Remote Support collects configuration information about devices in your environment. This data may be used to aid in restoring your device to production status. Depending on your support agreement with HPE, it can also be analyzed and compared with information in HPE’s knowledge database to provide recommendations to improve performance, or to avoid potential unwanted downtime. Data is collected using management agents (like WBEM) to query the device and report data back to the Hosting Device. This information is packaged by the Hosting Device and sent to HPE via HTTPS (TCP/443). Data collections are not stored or accessible on the local system.
Logging
The Hosting Device keeps a record of Insight Remote Support activities in the following (default) location:

- Log Data
  C:\ProgramData\HP\RS\LOG\{Log_Name}.log

Data Sent to HPE
This section describes HPE Remote Support data sent to HPE. Some ProLiant Gen8/Gen9/Gen10 and c-Class BladeServers have the ability to send data directly to HPE.

Data sent to HPE can be sent directly or via a proxy server. If a proxy server is used, the proxy settings are configured using the Insight Remote Support User Interface: Administrator Settings → Settings tab. In HPE OneView proxy settings are configured via the OneView -> Settings -> Proxy page. If a proxy username and password are required, the password is encrypted and stored locally in a binary format file. If the proxy username and password are changed at the proxy, they must also be changed in the Remote Support device console to ensure connectivity to HPE is uninterrupted. All transport sessions to HPE are encrypted using TLSv1.2 over HTTPS. Connections are always initiated by the Hosting Device or HPE OneView appliance outbound to HPE and are authenticated using X.509 Digital Certificates and a Global Unique Identifier (GUID) that is unique to the Hosting Device / OneView appliance. All data sent to HPE is via an HTTPS connection to a single destination URL (https://api.support.hpe.com/v1/). This destination is a virtual IP address that is automatically routed to an active server in one of the HPE Corporate Data Centers (see figure 2).

Note: Insight Remote Support can allow TLS 1.0, SSLv3 and SSLv2 connections from Monitored Devices to ensure compatibility with older platforms. These protocols must be specifically enabled by the Insight Remote Support Host system administrator. All Remote Support connections to HPE require strong encryption (TLSv1.2 or higher) to ensure the best possible security during the transport of event and collection data to HPE.

Data Sent to HPE contains configuration information about devices in your environment. Some of this information may be viewable using HPE Insight Online. Examples of data collected include diagnostic sense information, firmware information, electronic model number, electronic serial number, and other device configuration data. Due to the nature of the configuration collection utilities, some potentially sensitive configuration details may be collected and sent to HPE as part of the event or data collection. This could include IP Address, Fully Qualified Domain Name, MAC address, DNS Configuration, and Windows Domain Details. HPE treats all collection data as HPE Confidential while at HPE. Access to this information is restricted to authorized HPE personnel with a valid business reason for accessing this information. Device Administrator contact details such as system administrator name, phone number, and email address will also be added to the event or collection data prior to transport to HPE. This is done to ensure HPE has the necessary contact information in case a response from HPE is required to affect a repair or to recommend a configuration change to avoid potential downtime.

Configuration and Device Administrator contact information will be sent to HPE as part of scheduled configuration collections, as part of event telemetry data or as part of a Remote Support device metrics collections.

All information collected by HPE Remote Support and sent to HPE is used in accordance with the Insight Remote Support Terms and Conditions (see note below) and the HPE Privacy Statement.

Note: For receiving remote support:
Installing HPE Remote Support enables your IT devices to be remotely monitored and to securely send support or service events, IT configuration information, diagnostic, configuration, and telemetry information to HPE, together with your support contact information. No other business information is sent to HPE.
Automated Connections to HPE
HPE Insight Remote Support and HPE OneView Remote Support will automatically open a HTTPS communication channel to HPE for the submission of service events, data collections and automatic device registrations and periodic device health metrics. In addition to these messaging events, HPE Remote Support Client installations will send periodic ‘Heartbeat’ messages to the HPE Data Center periodically to verify connectivity. Remote Support Heartbeats can be used to verify that communication with HPE is functioning properly. If there are open service events or pending data collections, the Remote Support Client will automatically connect to the HPE Data Center every 10 minutes to check for status updates or to confirm the successful submission of pending data collections. If there are no open service events or pending data collections the Remote Support client will connect to HPE every 6 hours to send a heartbeat message and check for and retrieve routine messages and updates.

Connection Retries
If an Internet connection fails to connect to HPE, it will automatically retry the connection after two minutes. If the connection still fails, continue attempting to connect on the following schedule (in minutes): 2, 4, 8, 16, 30, 1440, 1440, 20160. After 10 failed connection attempts (16 days 2 hours), connection attempts will cease until the next system restart.

Email Notifications
HPE Remote Support has the capability of sending email notifications to the default and device contacts when certain events occur. You can enable email notification on the Administrator Settings → Integration Adapters tab, enabling email notification in the Insight RS Console, or in the OneView -> Settings -> Email Notifications allowing you to receive email notification for any or all of the following events:
### Table 2: Email Notifications

<table>
<thead>
<tr>
<th>Notification State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Submitted</td>
<td>Primary 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</td>
</tr>
<tr>
<td>Case Opened</td>
<td>Primary 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</td>
</tr>
<tr>
<td>Case Closed</td>
<td>Primary and backup contacts notified when a case is closed in HPE data center. Emails are also sent for service events generated by test events</td>
</tr>
<tr>
<td>Collection Sent</td>
<td>Primary and Backup contacts notified each time data collected about a device is sent to HPE</td>
</tr>
<tr>
<td>Software Management Updates</td>
<td>Primary contact notified whenever there is a new software update is available</td>
</tr>
<tr>
<td>Entitlement Expiration</td>
<td>Primary and Backup contacts notified when a warranty or contract is about to expire. Notifications are sent at 90, 60, 30 and 0 days prior to expiration</td>
</tr>
<tr>
<td>New Device Discovered</td>
<td>Primary and Backup contacts notified when a new device has been discovered</td>
</tr>
<tr>
<td>Device Health Status</td>
<td>Primary 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</td>
</tr>
<tr>
<td>Hosting Device Threshold Exceeds %</td>
<td>Primary and backup contacts notified when the Hosting Device's capacity exceeds the specified percentage of devices that Insight RS can support</td>
</tr>
</tbody>
</table>

**NOTE:** Email messages may contain device IP Address and Fully Qualified Domain Name. This information is sent from the Hosting Device and may be unencrypted. HPE does not recommend sending unencrypted email notification messages to email destinations outside of your company domain.
Insight Remote Support at HPE

HPE Data Centers
All customer data received by HPE is treated as “HPE Confidential” and treated in accordance with HPE’s Data Handling guidelines for HPE Confidential information.

Customer data is stored at one of the HPE Global Data Centers (DC)—located in Houston Texas. Each DC zone has a site-to-site business continuity and disaster recovery capability. The DCs operate continuously (24x7) in a lights-out computing environment with strict physical and logical access control mechanisms. HPE corporate data centers are concurrently maintainable and are designed to meet or exceed the American National Standards Institute / Technology Industries Association (ANSI/TIA) 942 Tier III Data Center standards.

Figure 2: HPE Corporate Network
Data Stored at HPE
Remote Support Data transmitted to HPE is received by the Remote Support Data Center (RSDC) Application Web Servers in the HPE Data Center. The Application Web Servers are responsible for the initial processing of data and routing it to the appropriate destination. There are two primary types of data transmitted to HPE from HPE Remote Support: event data and collection data. Event data is any data that is the result of a hardware or software event that occurs on a monitored device that is sent to HPE. Collection data contains configuration details about monitored devices in your enterprise. Configuration information may be used to restore device configuration parameters after a hardware component has been replaced. It can also be used for proactive data analysis. Proactive analysis compares your device configuration information against HPE’s known problem database in order to identify potential configuration issues that could impact production and/or performance.

Note: The RSDC servers support Global Server Load Balancing (GSLB) and Site-to-Site failover.

Data Orchestration
When Insight Remote Support event data is received at HPE, the first step is to determine the type of data coming in and route it to the correct parsing engine. Event data is forwarded to the event processing engine (see Figure 3) and collection data is forwarded to the collection processing engine (see Figure 4).

Event Processing
Every device monitored by Insight Remote Support is assigned a unique identifier called a Global Device Identifier (GDID). The event processing looks at the GDID in the event to determine if there is a record for this device in the Application Database. Event processing will also parse the data so it can be analyzed.

Event Filtering
Event Filtering uses smart analytics to determine whether or not an event requires action by HPE. This is done by comparing the event to a rules engine to determine if the event meets all of the requirements necessary to open a new service request or match the event to an existing service request.

Entitlement
If an event passes the initial event filtering process, it will go through entitlement analysis (denoted by the ‘Create Workflow Case?’ decision box above). Entitlement analysis checks the device entitlement parameters (serial number, model number, contract identifier) against the HPE entitlement database to determine the appropriate Service Level
Agreement (SLA) for the device. If a valid entitlement is found, the event is forwarded to Event Correlation. If no valid entitlement is found, the event is closed with a status of no entitlement.

**Event Correlation**

Once an event is entitled, it goes through one final correlation check. All currently open service requests for this device are checked to determine if the event matches the description of an open service request. If no match is found, a new service request is opened in the workflow system and routed to the appropriate support team for resolution. If a match is found, the event is marked as a duplicate event and correlated with the open workflow case.

**Figure 4: Configuration Collection Data Flow at HPE**

**Collection Processing**

Collection data, like event data, is parsed to obtain the device GDID and entitlement information. The GDID is used to identify the device for which the collection information originated. The entitlement information is used to determine if the device is covered under a support agreement that authorizes collection information to be stored and analyzed by HPE. If collection processing determines that collections are supported for this device’s GDID, the collection data will be sent to the Support Automation Database (SADB).
HPE Insight Online

HPE Support Center
HPE Insight Online is a cloud-based IT Management and support solution. HPE Insight Online lets you view, monitor, and support devices in your enterprise from the HPE Support Center portal. Data collected from your devices can be viewed online using HPE Support Center. HPE Insight Online allows customers (and optionally, HPE Authorized Resellers and Authorized Support Providers) with HPE Remote Support to monitor the status and support details of devices in their enterprise. Refer to the HPE Insight Remote Support and HPE Insight Online Setup Guide for HPE ProLiant Servers and HPE BladeSystem c-Class Enclosures for information about enabling HPE Insight Online. Remote Support Administrators can verify access to HPE Support Center from the Insight RS Console by entering their HPE Passport Username and Password in the setup wizard or on the Administrator Settings tab. The HPE Passport username is retained in the RS Host administrator settings; however the HPE Passport password is passed to HPE Passport for authentication only and is not retained in the Insight RS Console.

HPE Passport
Access authentication for HPE Insight Online is managed by HPE Passport.

HPE Passport maintains access information for most HPE online applications, HPE Passport stores basic personal information (e.g., user id, password, name, e-mail address, country, and language preferences) in an encrypted database. This information is managed according to HPE’s strict privacy policies. If the HPE Passport account used by HPE Remote Support changes, the information in HPE Insight Online must be updated to match the HPE Passport Account username and password.
# GLOSSARY of Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>DCOM</td>
<td>Distributed Component Object Module</td>
</tr>
<tr>
<td>EDW</td>
<td>Enterprise Data Warehouse</td>
</tr>
<tr>
<td>ELMC</td>
<td>Event Log Monitoring Collector</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>GDID</td>
<td>Global Support Identifier</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface (same as UI)</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hyper Text Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper Text Transfer Protocol Secure</td>
</tr>
<tr>
<td>IKEv2</td>
<td>Internet Key Exchange version 2</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>OSCP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>RDA</td>
<td>Remote Device Access</td>
</tr>
<tr>
<td>RDC</td>
<td>Remote Data Collection</td>
</tr>
<tr>
<td>RDM</td>
<td>Remote Device Management</td>
</tr>
<tr>
<td>RIBCL</td>
<td>Remote Insight Board Control Language</td>
</tr>
<tr>
<td>RS</td>
<td>Remote Support</td>
</tr>
<tr>
<td>RSDB</td>
<td>Remote Support Database</td>
</tr>
<tr>
<td>SADB</td>
<td>Support Automation Database</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SNMPv1</td>
<td>Simple Network Management Protocol Version 1</td>
</tr>
<tr>
<td>SNMPv2</td>
<td>Simple Network Management Protocol Version 2</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>Simple Network Management Protocol Version 3</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UDP</td>
<td>Unified Datagram Protocol</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>WEBM</td>
<td>Web-Based Enterprise Management</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Measurement Instrumentation</td>
</tr>
</tbody>
</table>
Learn more at the Hewlett Packard Enterprise Information Library
hpe.com/info/insightremotesupport/docs