UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

INTELLECTUAL VENTURES II LLC,	)	Civil Action No. 6:22-cv-703
Plaintiffs,	)	
v.	)	
HEWLETT PACKARD ENTERPRISE CO.,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff, Intellectual Ventures II LLC ("IV"), for its complaint against defendant, Hewlett Packard Enterprise Company ("HPE"), hereby alleges as follows:

THE PARTIES

1. Intellectual Ventures II LLC ("Intellectual Ventures II" or "IV") is a Delaware limited liability company having its principal place of business located at 3150 139th Avenue SE, Bellevue, Washington 98005.

2. Upon information and belief, HPE is a Delaware corporation with its principal executive offices located at 11445 Compaq Center West Drive, Houston, Texas 77070.

3. Upon information and belief, HPE has regular and established places of business in this District, including a fifty-two (52) acre campus at 14321 Tandem Boulevard, Austin, Texas, and a lease for another 27,326 square foot office at Paloma Ridge, 13620 FM 620 Austin, Texas 78717. HPE also has an office at 6080 Tennyson Parkway, Suite 400, Plano, Texas 75024.

4. Upon information and belief, HPE's global headquarters is in Houston, Texas.

5. Upon information and belief, HPE may be served with process through its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

JURISDICTION

6. IV brings this action for patent infringement pursuant to 35 U.S.C. § 271, *et seq.* This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

7. This Court has general jurisdiction over HPE because HPE is engaged in substantial and not isolated activity at its regular and established places of business within this judicial district. This Court has specific jurisdiction over HPE because HPE has committed acts of infringement giving rise to this action within this judicial district and has established more than minimum contacts within this judicial district, such that the exercise of jurisdiction over HPE in this Court would not offend traditional notions of fair play and substantial justice.

8. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because HPE maintains regular and established places of business and has committed acts of patent infringement within this judicial district.

FACTUAL BACKGROUND

9. Intellectual Ventures Management, LLC ("Intellectual Ventures") was founded in 2000. Intellectual Ventures fosters inventions and facilitates the filing of patent applications for those inventions; collaborates with others to develop and patent inventions; and acquires and licenses patents from individual inventors, universities, corporations, and other institutions. A significant aspect of Intellectual Ventures' business is managing the plaintiff in this case, Intellectual Ventures II.

10. One founder of Intellectual Ventures is Nathan Myhrvold, who worked at Microsoft from 1986 until 2000 in a variety of executive positions, culminating in his appointment as the

company's first Chief Technology Officer ("CTO") in 1996. While at Microsoft, Dr. Myhrvold founded Microsoft Research in 1991 and was one of the world's foremost software experts. Between 1986 and 2000, Microsoft became the world's largest technology company.

11. Under Dr. Myhrvold's leadership, IV acquired thousands of patents covering many important inventions of the Internet era, including many pertaining to the networked computers that comprise the Internet. Many of these inventions coincided with Dr. Myhrvold's successful tenure at Microsoft.

12. One area of particular and continuing importance in the Internet era is the remote management of networked devices. Device security management specifically, which is the management of devices with the goal of protecting them from harm and unauthorized use, is becoming especially important with every passing year. Secure management of remotely located devices is essential for reliable, dependable, and highly availabile systems that are resilient to attack, responsive to customer's needs and affordable to operate.

13. Historically, the combination of remote management and secure management were not coextensive. As a result, networked devices were traditionally managed by physically isolating them, either individually or in small groups, from other parts of the network. An administrator for example, would typically co-locate several devices and limit physical access of those devices to select authorized employees. Any management of the devices would have to be performed while one of those employees was physically present with the devices. Such solutions became cost-prohibitive, in terms of both time and personnel, as networks grew and expanded over geographically dispersed areas.

14. When it became no longer feasible to have an administrator present at the location of every device in the network, many network administrators began allowing authorized

employees to perform remote maintenance on networked devices. Enabling a device for remote management to avoid the cost and delay of dispatching a person to the remote site, however, could potentially allow a determined intruder to utilize the remote access means for an attack if the remote management solution is not highly secure.

15. Remote management of network devices was performed over either "in-band" or "out-of-band" network connections. "In-band" management occurred over the same network that user data traversed, meaning that management data and user data flowed over the same network. "Out-of-band" management occurred using a means other than the network utilized by user data. Both "in-band" and "out-of-band" management did not have the appropriate level of security to prevent against potential attacks.

16. A disadvantage of out-of-band management arose because it bypassed several important network security systems that were employed by user data networks. These systems included virtual private networks (VPNs), firewalls, access control lists (ACLs) and authentication servers. As a result, out-of-band management made the network and its connected devices more vulnerable against malicious attacks.

17. In-band management also has its challenges. One is the comingling of user data and management data. Comingling of user and management data provides an opportunity for rogues to compromise management data from within the network itself, particularly if the administrator failed to implement a robust authentication scheme for other authorized administrators or employees. VPNs existed, which protected management data while it flowed over the in-band network, but even with VPNs, there was commingling of user data and management data in the device itself. In another example, existing authentication schemes, such as placing sole reliance on HTTPS authentication, were not always as robust as they needed to be.

Problems such as comingling and authentication could be addressed by adding additional devices that implemented these features, which would be placed within or near the managed device. But such other devices would add cost and occupy extra space.

18. To overcome these obstacles, Engedi Technologies ("Engedi"), an early developer of network security solutions focused on secure remote management technology and the original assignee of the patents-in-suit, developed the Secure Remote Management System (SRM). SRM provided an authenticated and encrypted secure tunnel between an SRM appliance co-located with a managed device, and a centralized network management center. These secure network tunnels provided multi-pathed communication capability for the remote management of network devices.[1]

19. SRM provided in-band and out-of-band secured network connections from the SRM appliance to the network management center, thus making available multiple and diverse robust paths for reporting status information to monitoring stations or allowing for remote configuration of the device. Compared to prior designs, the diverse and robust multi-path capability was a significant advantage.

20. Engedi Technologies patented many key features of the SRM between 2002 and 2006.

21. HPE makes, uses, and sells servers and network devices that include embedded secure management processors marketed under the Integrated Lights Out ("iLO") brand, as well as purpose-built software that supports operation of the iLO processors. These iLO processors and

[1] For instance as described by Engedi Technologies at: https://web.archive.org/web/20050309054746/http://www.engedi.net/focus.htm and https://web.archive.org/web/20050130064915/http://www.engedi.net/documents/SecureRemoteManagement_ver2p5.pdf

purpose-built software are embedded in HPE's ProLiant, Apollo, and Synergy servers, among others, as well as other solutions based on the aforementioned servers, such as HPE's SimpliVity offerings and many GreenLake hosted services.

THE PATENTS-IN-SUIT

22. On January 29, 2008, the PTO issued United States Patent No. 7,325,140 ("the '140 patent"), titled SECURE MANAGEMENT ACCESS CONTROL FOR COMPUTERS, EMBEDDED AND CARD EMBODIMENT. The '140 patent is valid and enforceable. A copy of the '140 patent is attached as Exhibit A.

23. Intellectual Ventures II LLC is the owner and assignee of all rights, title, and interest in and to the '140 patent, and holds all substantial rights therein, including the rights to grant licenses, to exclude others, and to enforce and recover past damages for infringement of that patent.

24. The '140 patent is directed to a remote device management communication system including a secure management access controller embedded within and in direct communication with a managed networked device. The system enables a remote administrator to securely access, support and manage networked devices that may be geographically dispersed or otherwise not physically accessible. Further, the management system includes in-band and out-of-band connection capability and employs virtualization to enhance security.

25. On June 25, 2013, the PTO issued United States Patent No. 8,474,016 ("the '016 patent"), also titled SECURE MANAGEMENT ACCESS CONTROL FOR COMPUTERS, EMBEDDED AND CARD EMBODIMENT. The '016 patent is valid and enforceable. A copy of the '016 patent is attached as Exhibit B.

26. Intellectual Ventures II LLC is the owner and assignee of all rights, title, and interest in and to the ’016 patent, and holds all substantial rights therein, including the rights to grant licenses, to exclude others, and to enforce and recover past damages for infringement of that patent.

27. Similar to the ’140 patent, the ‘016 patent is directed to a computer network management apparatus and method for remotely managing a networked device. The apparatus and method incorporate a processor that facilitates secure remote management of a networked device, and that is part of the networked device, in addition to a separate processor that facilitates processing of user data. In enabling secure remote management of a networked device, the ’016 patent further separates management requests from user data requests in the networked device using a multi-bus architecture and cryptography to improve the security of the management request communications.

28. The inventions claimed in the ’140 patent and the ’016 patent were conceived by Jeffrey Alan Carley during his time as CTO and Co-Founder of Engedi. As noted above, Engedi created a secure remote management system to meet the need for a cost saving, highly secure method to access and manage remotely located devices in a distributed network. The system had a particular focus on preventing malicious attacks from insiders and resiliency in the event of one or more path failures. Mr. Carley was an integral part of Engedi’s technology development, architecting and overseeing the entire process, including managing funding, vendor and partner relationships and intellectual property growth. He has over 25 years of experience in the computer networking industry with major strengths in hybrid cloud networking, network architecture design and implementation, and network security and management at companies such as AIS, Pearson, TEKsystems, HPE, Modis, MCI and IBM. Mr. Carley also holds the National Security Agency

(NSA) InfoSec Assessment Management Methodology (IAM) certification and is a member of the IEEE, the Computer Society of the IEEE, the Information Systems Security Association and the Center for Internet Security. He is currently a Cloud Infrastructure Consultant at Applied Information Sciences and resides in Colorado Springs, Colorado.

COUNT I
(HPE's Infringement of U.S. Patent No. 7,325,140)

29. The preceding paragraphs are reincorporated by reference as if fully set forth herein.

30. The inventions claimed in the '140 patent, taken alone or in combination, were not well-understood, routine, or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '140 patent claims and teaches, *inter alia*, an improved way to provide secure remote management for devices by deeply embedding the necessary secure remote management hardware and software in the managed device itself. The inventions improved upon then-existing remote access/management security techniques by combining such hardware with a virtual management interface for logically separating user data from management data when using in-band management techniques. They added critical features to in-band management such as enabling separation of management and user data when administrators used in-band management all the way up to the network port itself. They accomplished this by creating a virtual interface at the physical port that accepts management and user data to keep the two data types segregated from end to end, including within the managed device, and not just on the network. Furthermore, this was accomplished without requiring adding more devices in or around the managed device by embedding the secure remote management hardware and software into the managed device itself. This realized significant costs savings for customers that otherwise would have had to add more devices that took up more space substantially increasing cost. Further security and redundancy

improvements were provided by the establishment of a separate purpose-built network connection interface for the secure remote management of the device over an out-of-band connection.

31. The inventions claimed in the ’140 patent represent technical solutions to an unsolved technological problem. The written description of the ’140 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and also to understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been performed in the industry prior to the inventions of the ’140 patent. More specifically, the claims of the ’140 patent recite a remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network. The system includes one or more network services, one or more secure management access controllers, and one or more managed network devices. Further, the system includes at least one secure management access controller connected to one or more data buses of the managed network device for communication of device management data, as well as an out-of-band access connection means for connecting one or more network services or remote users with the secure management access controller for management of the network device. In addition, the system includes at least one virtual management interface connection means for connecting said one or more network services or remote users with the secure management access controller, where the virtual management connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with the secure management access controller.

32. The system covered by the asserted claims, therefore, differs markedly from the prior systems in use at the time of this invention, which, *inter alia*, lacked the claimed combination of the secure management access controller connected to a managed network device, an out-of-band connection means for connecting one or more network services or remote users with the secure management access controller, and a virtual management interface connection means for providing logical separation of management data and user data and for utilizing user interfaces of the managed device to also connect one or more network services or remote users with the secure management access controller.

33. The ’140 patent is drawn to solving a specific, technical problem arising in the context of secure remote access/management of distributed network devices. Consistent with the problem addressed being rooted in such secure remote access/management technology, the solutions disclosed in the ’140 patent consequently are also rooted in that same technology and cannot be performed with pen and paper or in the human mind.

34. HPE has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claim 1 of the ’140 patent by making, using, testing, selling, offering for sale, and/or importing into the United States products and/or services covered by one or more claims of the ’140 patent. HPE’s products and/or services that infringe the ’140 patent include all products and services that use an iLO 5 embedded processor, which upon information and belief, include but are not limited to, the HPE ProLiant Gen 10 series servers, the HPE ProLiant Gen 10 Plus series servers, the HPE ProLiant e900 series server blades, the HPE Edgeline Converged Edge System, the HPE Apollo 2000, 4000 and 6000 Series Systems, the HPE Apollo Gen 10 series servers, the HPE Apollo Gen 10 Plus series servers, the HPE Edgeline e900 series server blades, HPE SimpliVity Gen 10 series nodes, HPE SimpliVity

2600 series nodes, HPE Synergy Gen 10 series compute modules, the HPE Gen 10 series servers for HPE Ezmeral Container Platform (including when provided as a GreenLake service), the HPE Apollo series and ProLiant series modules for Qumulo, and any hosted or on-demand services offered by HPE using the aforementioned hardware/software, as well as any other HPE products and/or services, either alone or in combination, that operate in substantially the same manner (together the "Accused '140 Products" or "Accused Products").

35. Claim 1 of the '140 patent is reproduced below:

> *1. A remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices, the remote device management system comprising:*
>
> *at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data;*
>
> *an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device; and*
>
> *at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller;*
>
> *wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.*

36. The Accused '140 Products each provide a remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed

computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices. As one non-limiting example, the Accused '140 Products are network devices, modules and/or nodes capable of being configured in a distributed computer network, such as the HPE ProLiant Gen 10 series servers, that include an HPE iLO 5 secure processor for controlling and securing remote management applications and services as well as communications regarding the same, as seen below:

HPE Integrated Lights Out (iLO 5) for Gen10 Servers - Overview

iLO 5

iLO is an embedded technology that ships in HPE servers. It is the core foundation for the intelligence of the HPE servers. This technology is combination of the iLO ASIC that is part of the server-board and the firmware that powers the ASIC. Industry leading features that enhance server administrator productivity are available through optional licenses. The available licenses are iLO advanced premium security edition (Supported only on Gen10 and later servers), iLO advanced, iLO essentials and iLO scale out (Supported on all generation servers)

iLO 5 is a remote server management processor embedded on the system boards of supported HPE servers and compute modules. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely.

iLO access security

You can use the following methods to manage access to iLO:

Local accounts

Up to 12 user accounts can be stored in iLO. This configuration is ideal for small environments such as labs and small-sized or medium-sized businesses.

Login security with local accounts is managed through the iLO Access Settings and user privileges.

Directory services

To support more than 12 users, configure iLO to use a directory service to authenticate and authorize access. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise.

If you plan to use directory services, consider enabling at least one local administrator account for alternative access.

A directory provides a central point of administration for iLO devices and users, and the directory can enforce a strong password policy.

CAC smart card authentication

You can configure common access smart cards together with local accounts and directory services to manage iLO user access.

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

You can use the iLO web interface to access iLO through a supported browser to monitor and configure managed servers.

The HPE InfoSight portal is a secure web interface hosted by HPE that allows you to monitor supported devices through a graphical interface.

iLO clock synchronization

SNTP allows iLO to synchronize its clock with an external time source. Configuring SNTP is optional because the iLO date and time can also be synchronized from the following sources:

- System ROM (during POST only)
- Onboard Administrator (ProLiant server blades only)
- Frame Link Module (Synergy compute modules)

Primary and secondary NTP server addresses can be configured manually or through DHCP servers. If the primary server address cannot be contacted, the secondary address is used.

Embedded System Health for HPE ProLiant

On supported server models, the HPE iLO for ProLiant management processor monitors fans, temperature sensors, power supply sensors and VRMs without having the System Management Driver loaded. The status of these is accessible from all HPE iLO for ProLiant user interfaces (browser, SMASH command line Redfish API, XML scripts and IPMI) independent of the host operating system The intelligence of iLO manages the Sea of Sensors thermal control, directs the Dynamic Power Capping technology and monitors the health of server components.

You can connect iLO to the network through a dedicated management network or a shared connection on the production network.

Dedicated management network

In this configuration, the iLO port is on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the production network. In this configuration, iLO cannot be accessed directly from the production network. The Dedicated management network is the preferred iLO network configuration.

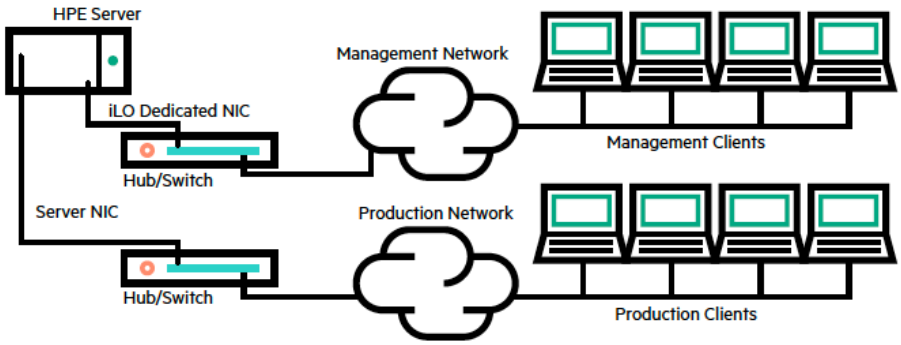
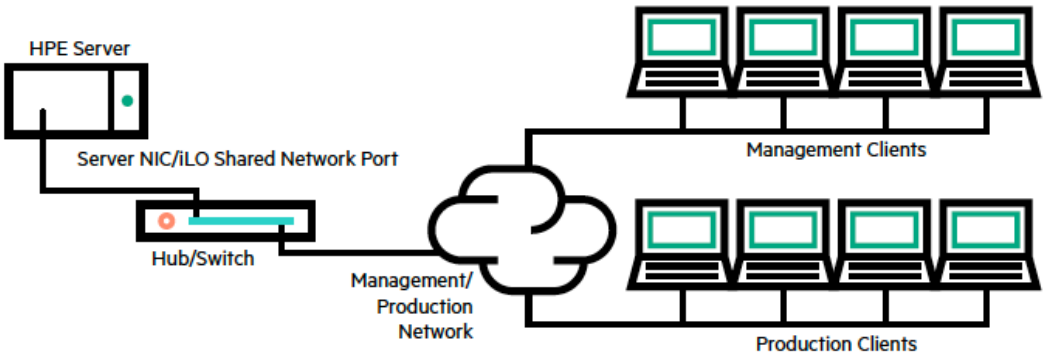


Figure 1: Dedicated management network

Production network

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network. Using a Shared Network Port configuration reduces the amount of networking hardware and infrastructure required to support iLO.



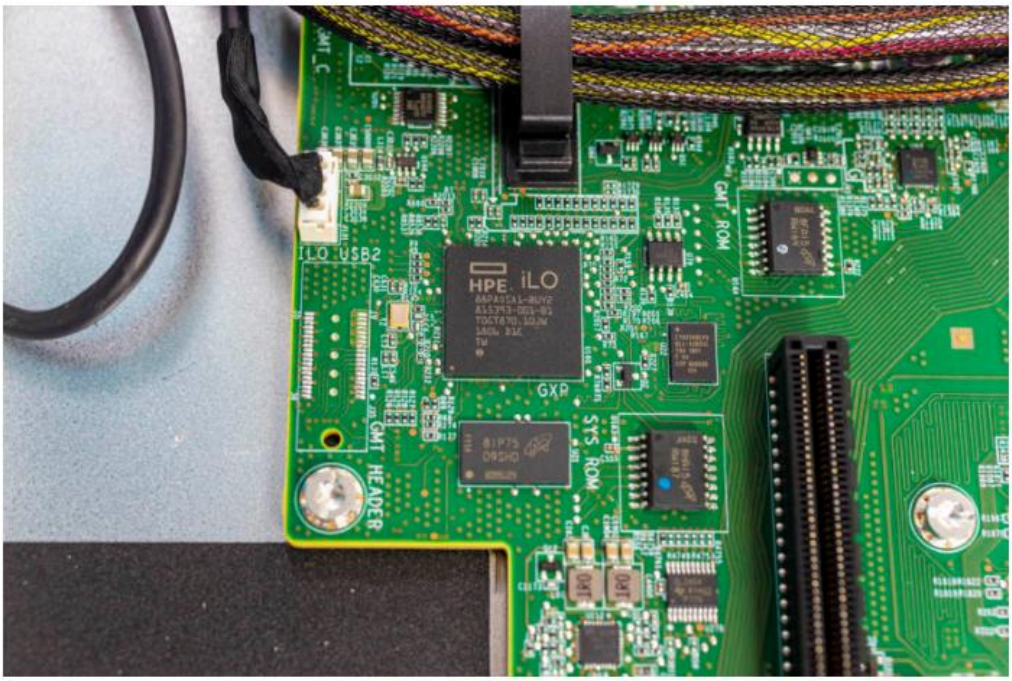
Role access restrictions

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users with dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC to view the **Security** tab.

HPE ProLiant DL325 Gen10 ILO 5 Chip



HPE ProLiant DL325 Gen10 ILO 5 Chip

iLO management for HPE ProLiant	HPE Agentless management 2.0:The base hardware monitoring and alerting capability is built into the system (Running on the HPE iLO chipset) and starts working the moment that a power cord and an Ethernet cable is connected to the server. This means that: • All core management is out-of-band for increased security and stability: no OS software required, no open SNMP port on the OS and zero downtime updates • Monitor and alerting on key internal server components: CPUs, memory, temperatures, fans, Smart Array controllers, hard drives (Including cache modules) and power supplies • HPE SIM can see the system and will give users preview of the system health summary and sub-system details • iLO integrates with HPE OneView
	HPE Active Health System • HPE Active health system is an essential component of the HPE iLO management • It provides users with: Diagnostics tools/scanners wrapped into one; always on, continuous monitoring for increased stability and shorter downtimes; Rich configuration history; health and service alerts; Easy export and upload to service and support
	HPE Active Healthy System Viewer Tool Enables user to read the active health system log files. It will provide errors messages and advises on a resolution. Use can create a support file, simply by uploading users AHS log file from within this tool
	HPE Intelligent Provisioning • Let's users provision and configure a single server without any separate media • No more Smart Start CDs or smart update firmware DVDs are needed
	HPE Embedded Remote Support • Hewlett Packard Enterprise offers embedded remote support that allows a user to enable remote support directly from iLO (Also OA and IP) without installing OS agents on the device, greatly reducing the time to activate remote monitoring • Through insight remote support 7.0.5 and later versions and insight online direct connect capability, users now benefit from 24x7 remote monitoring, auto-generated service events, support cases and anywhere, anytime monitoring with HPE Insight online, a personalized cloud-based IT dashboard

37. Furthermore, the Accused ’140 Products comprise at least one secure management access controller connected to one or more data buses of said managed network device for the communication of device management data. For example, the Accused Products include an iLO processor, which controls remote management functions and communications regarding the same, as seen below:

HPE Integrated Lights-Out (iLO)

Integrated Lights-Out (iLO) is an embedded technology that ships in HPE Servers. It is the core foundation for the intelligence of the HPE Servers. This technology is combination of the iLO ASIC that is part of the server-board and the firmware that powers the ASIC.

iLO 5 is a remote server management processor embedded on the system boards of supported HPE servers and compute modules. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely.

HPE Agentless Management 2.0

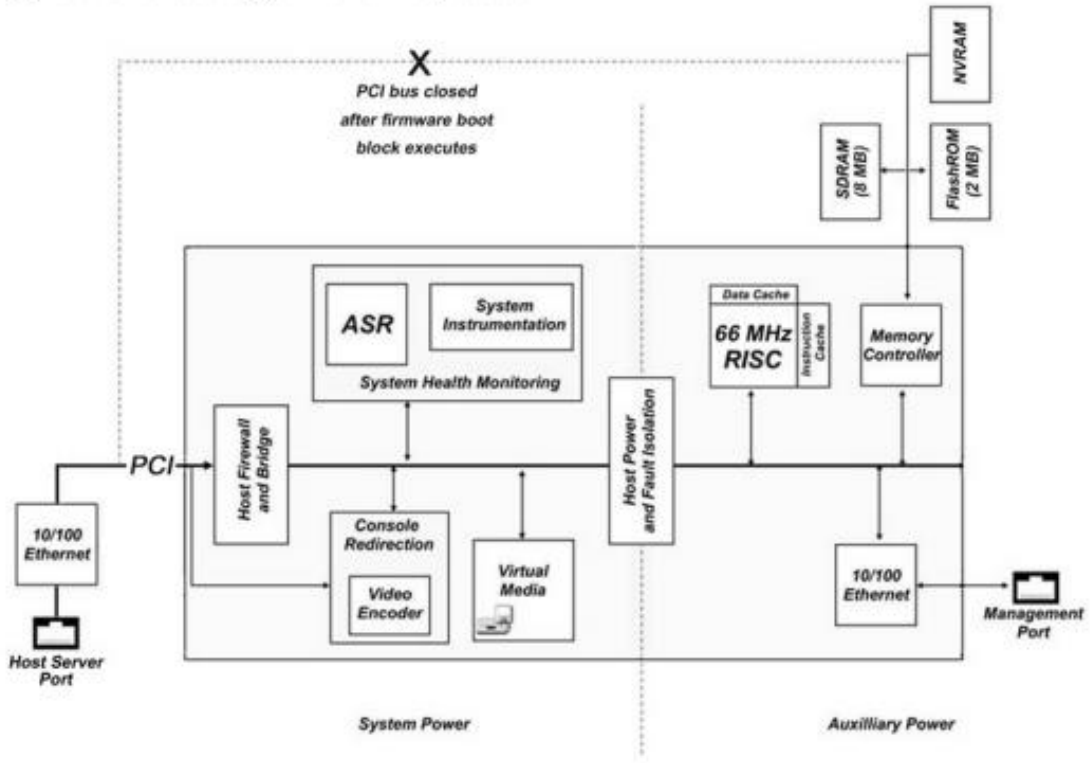
The base hardware monitoring and alerting capability is built into the system (running on the HPE iLO chipset) and starts working the moment that a power cord and an Ethernet cable is connected to the server. This means that:

- All **core** management is out-of-band for increased security and stability: no OS software required, no open SNMP port on the OS and zero downtime updates.
- **Monitor** and Alerting on key internal server components: CPUs, memory, temperatures, fans, SmartArray controllers, hard drives (including cache modules) and power supplies.
- HPE **Systems** Insight Manager (HPE SIM) can see the system and will give customers preview of the System Health Summary and Sub-System Details.
- iLO **integrates** with HPE OneView.

HPE Active Health System

HPE Active Health System is an essential component of the HPE iLO Management. It provides customers with: Diagnostics tools/scanners wrapped into one; Always on, continuous monitoring for increased stability and shorter downtimes; Rich configuration history; Health and service alerts; Easy export and upload to Service and Support.

Figure 1. Schematic diagram of the iLO processor



38. The Accused ’140 Products further comprise an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device. For example, connectivity to the iLO processor for remote device management can be over a dedicated management connection via an embedded dedicated ethernet NIC, giving remote administrators a secure out-of-band management solution, as illustrated below:

Flexible Network Connectivity for HPE ProLiant

HPE Integrated Lights-Out (iLO) for ProLiant provides a choice between two network connection methods to access all functionality:

- **Dedicated connection** - Access HPE iLO for ProLiant via an embedded 10/100-MB (10/100/1000-MB on iLO 4) dedicated Ethernet NIC. This enables remote management over a dedicated, out-of-band management network. In-band SNMP notification of server problems on a real-time basis is also supported without separate telephone connections or modem sharing devices. The dedicated NIC can auto-negotiate speed and duplex options. The iLO Dedicated NIC provides the highest levels of reliability and security.
- **Shared Network Port** - On selected ProLiant server models, HPE iLO for ProLiant supports network connectivity through a new high-speed shared connection via one of the embedded system NICs. The latest version of iLO also supports. Shared network port over the Flexible -LOM providing full accessibility to all HPE iLO for ProLiant functions including browser, Virtual Media and Virtual Keyboard Video and Mouse in graphics mode. The management processor maintains a unique IP address and MAC allowing the network controller to route HPE iLO for ProLiant and host data correctly. With the Shared Network Port, out-of-band management and production data can share the same wire eliminating the separate network connection for each server.

Role access restrictions

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users with dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC to view the **Security** tab.

iLO NIC auto-selection

iLO NIC auto-selection enables iLO to choose between the iLO Dedicated Network Port and the iLO Shared Network Port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common preconfiguration for your ProLiant Gen10 and later servers. For example, if you have several servers, some might be installed in a data center where iLO is contacted through the iLO Dedicated Network Port. Other servers might be installed in a data center where iLO is contacted through the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

Agentless Management and AMS

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.

To collect information from devices and components that cannot communicate directly with iLO, install the **Agentless Management Service (AMS)**.

Integrated Lights-Out (iLO) Management for HPE ProLiant

HPE Agentless Management 2.0

The base hardware monitoring and alerting capability is built into the system (running on the HPE iLO chipset) and starts working the moment that a power cord and an Ethernet cable is connected to the server. This means that:

- All **core** management is out-of-band for increased security and stability: no OS software required, no open SNMP port on the OS and zero downtime updates.
- **Monitor** and Alerting on key internal server components: CPUs, memory, temperatures, fans, SmartArray controllers, hard drives (including cache modules) and power supplies.
- HPE **Systems** Insight Manager (HPE SIM) can see the system and will give customers preview of the System Health Summary and Sub-System Details.
- iLO **integrates** with HPE OneView.

Component	Agentless Management without AMS	Additional information provided when AMS is installed
Server health	• Fans • Temperatures • Power supplies • Memory • CPU • NVDIMM	N/A
Storage	• Smart Array • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array • Smart Storage Energy Pack monitoring (supported servers only) • NVMe drives that support MCTP	• SMART Drive Monitoring (connected to AHCI and Gen10 Smart Array MR) • iSCSI (Windows) • NVMe drives
Network	• MAC addresses for embedded NICs that support NC-SI over MCTP • Physical link connectivity and link up/link down traps for NICs that support NC-SI over MCTP • Fibre Channel adapters that support Hewlett Packard Enterprise vendor-defined MCTP commands	• MAC and IP address for standup and embedded NICs • Link up/link down traps • NIC teaming and bridging information (Windows and Linux) • Supported Fibre Channel adapters • VLAN information (Windows and Linux)

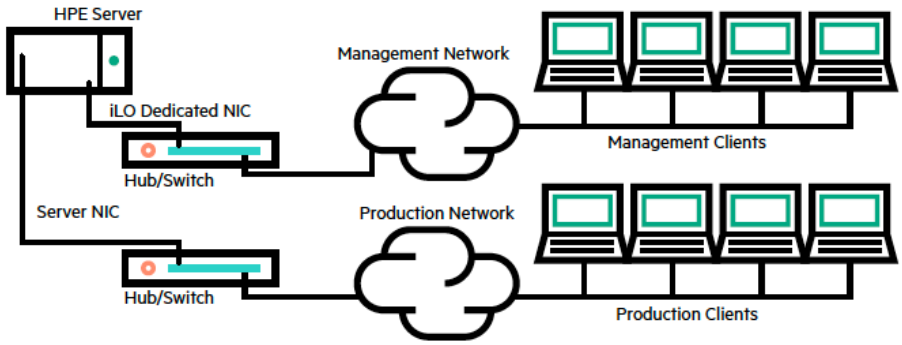


Figure 1: Dedicated management network

39. In addition, the Accused '140 Products include at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management controller. For example, connectivity to the iLO processor for remote device management can be over shared network connections via a shared network port, giving

remote administrators a secure in-band management solution that virtually separates user and management traffic, as illustrated below:

Flexible Network Connectivity for HPE ProLiant

HPE Integrated Lights-Out (iLO) for ProLiant provides a choice between two network connection methods to access all functionality:

- **Dedicated connection** - Access HPE iLO for ProLiant via an embedded 10/100-MB (10/100/1000-MB on iLO 4) dedicated Ethernet NIC. This enables remote management over a dedicated, out-of-band management network. In-band SNMP notification of server problems on a real-time basis is also supported without separate telephone connections or modem sharing devices. The dedicated NIC can auto-negotiate speed and duplex options. The iLO Dedicated NIC provides the highest levels of reliability and security.
- **Shared Network Port** - On selected ProLiant server models, HPE iLO for ProLiant supports network connectivity through a new high-speed shared connection via one of the embedded system NICs. The latest version of iLO also supports. Shared network port over the Flexible -LOM providing full accessibility to all HPE iLO for ProLiant functions including browser, Virtual Media and Virtual Keyboard Video and Mouse in graphics mode. The management processor maintains a unique IP address and MAC allowing the network controller to route HPE iLO for ProLiant and host data correctly. With the Shared Network Port, out-of-band management and production data can share the same wire eliminating the separate network connection for each server.

iLO NIC auto-selection

iLO NIC auto-selection enables iLO to choose between the iLO Dedicated Network Port and the iLO Shared Network Port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common preconfiguration for your ProLiant Gen10 and later servers. For example, if you have several servers, some might be installed in a data center where iLO is contacted through the iLO Dedicated Network Port. Other servers might be installed in a data center where iLO is contacted through the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

Role access restrictions

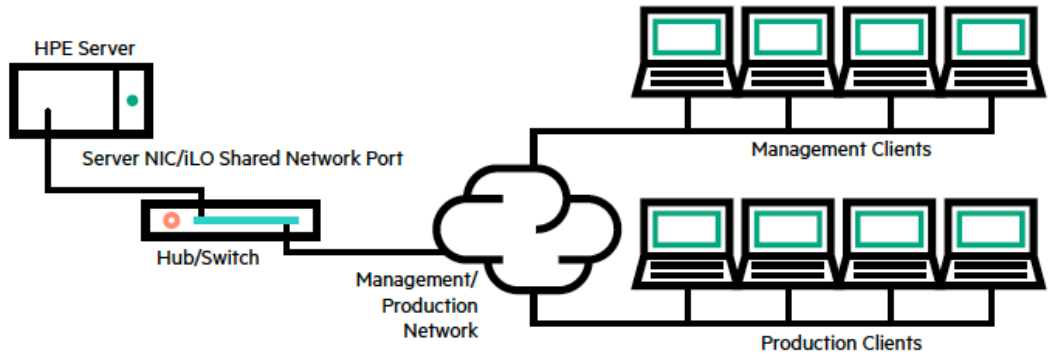
Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users with dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC to view the **Security** tab.

Virtual Private Network (VPN) support for HPE ProLiant

HPE iLO for ProLiant functionality is available securely over the Internet around the world when used in conjunction with VPN technology. VPN is supported on both HPE iLO for ProLiant network connection methods, dedicated and shared network ports.



40. Furthermore, in the Accused '140 Products the virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller. As noted above for example, the shared network port allows remote administrators to communicate management data and logically separate the user data from the management data:

Flexible Network Connectivity for HPE ProLiant

HPE Integrated Lights-Out (iLO) for ProLiant provides a choice between two network connection methods to access all functionality:

- **Dedicated connection** - Access HPE iLO for ProLiant via an embedded 10/100-MB (10/100/1000-MB on iLO 4) dedicated Ethernet NIC. This enables remote management over a dedicated, out-of-band management network. In-band SNMP notification of server problems on a real-time basis is also supported without separate telephone connections or modem sharing devices. The dedicated NIC can auto-negotiate speed and duplex options. The iLO Dedicated NIC provides the highest levels of reliability and security.
- **Shared Network Port** - On selected ProLiant server models, HPE iLO for ProLiant supports network connectivity through a new high-speed shared connection via one of the embedded system NICs. The latest version of iLO also supports. Shared network port over the Flexible -LOM providing full accessibility to all HPE iLO for ProLiant functions including browser, Virtual Media and Virtual Keyboard Video and Mouse in graphics mode. The management processor maintains a unique IP address and MAC allowing the network controller to route HPE iLO for ProLiant and host data correctly. With the Shared Network Port, out-of-band management and production data can share the same wire eliminating the separate network connection for each server.

iLO NIC auto-selection

iLO NIC auto-selection enables iLO to choose between the iLO Dedicated Network Port and the iLO Shared Network Port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common preconfiguration for your ProLiant Gen10 and later servers. For example, if you have several servers, some might be installed in a data center where iLO is contacted through the iLO Dedicated Network Port. Other servers might be installed in a data center where iLO is contacted through the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

Role access restrictions

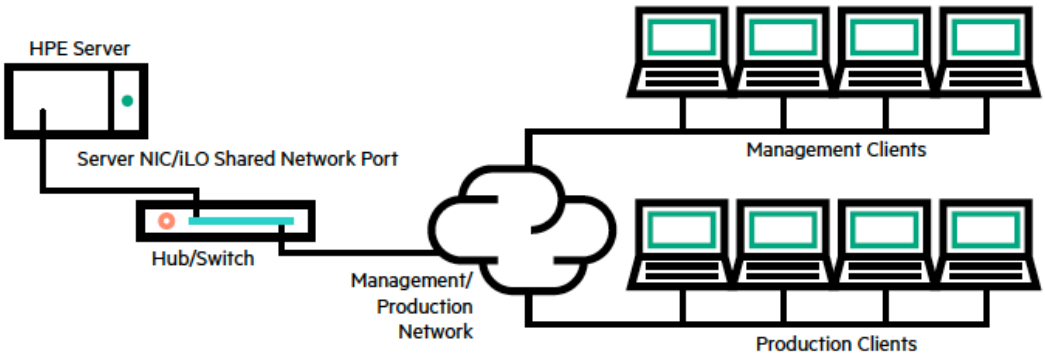
Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users with dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC to view the **Security** tab.

Virtual Private Network (VPN) support for HPE ProLiant

HPE iLO for ProLiant functionality is available securely over the Internet around the world when used in conjunction with VPN technology. VPN is supported on both HPE iLO for ProLiant network connection methods, dedicated and shared network ports.



41. Additionally, HPE has been, and currently is, an active inducer of infringement of the '140 patent under 35 U.S.C. § 271(b) and a contributory infringer of the '140 patent under 35 U.S.C. § 271(c).

42. HPE has actively induced, and continues to actively induce, infringement of the '140 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the '140 patent, including but not limited to, all products and services that use an iLO 5 embedded processor, which upon information and belief, includes but is not limited to, the HPE ProLiant Gen 10 series servers, the HPE ProLiant Gen 10 Plus series servers, the HPE ProLiant e900 series server blades, the HPE Edgeline Converged Edge System, the HPE Apollo 2000, 4000 and 6000 Series System, the HPE Apollo Gen 10 series servers, the HPE Apollo Gen 10 Plus series servers, the HPE Edgeline e900 series server blades, HPE SimpliVity Gen 10 series nodes, HPE SimpliVity 2600 series nodes, HPE Synergy Gen 10 series compute modules, the HPE Gen 10 series servers for HPE Ezmeral Container Platform (including when provided as a GreenLake service), the HPE Apollo series and ProLiant series modules for Qumulo, and any hosted or on-demand services offered by HPE using the aforementioned hardware/software, as well as any other HPE products and/or services, either alone or in combination, that operate in substantially the same manner. HPE provides these products and/or services to others, such as customers, resellers, partners and end-user customers, who, in turn, in

accordance with HPE's design, intent and directions, use, provision for use, offer for sale, or sell in the United States the foregoing products and/or services that directly infringe one or more claims of the '140 patent as described above. HPE's inducement includes the directions and instructions found at one or more of the following links, the provision of which is on-going as of the filing of this Complaint and the content of which is specifically illustrated above:

- https://support.hpe.com/hpesc/public/docDisplay?docId=a00105236en_us
- https://www.hpe.com/psnow/doc/c04154343.html?jumpid=in_lit-psnow-red
- https://www.informatica.us.es/docs/operativa/HP/HP-iLO-Seguridad.pdf
- https://support.hpe.com/hpesc/public/docDisplay?docId=c04530504
- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00026111en_us
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00039732en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00045457en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00026106en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00045462en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00018323en_us

43. HPE has contributed to, and continues to contribute to, the infringement of the '140 patent by others by knowingly providing one or more components, for example the iLO 5 processor, a portion thereof, and/or the software modules responsible for the accused functionality described herein, that, when installed, configured, and used result in systems that, as intended by HPE described above, directly infringe one or more claims of the '140 patent.

44. HPE knew of the '140 patent, or should have known of the '140 patent, but was willfully blind to its existence. Upon information and belief, HPE has had actual knowledge of the '140 patent since at least as early as the receipt of IV's June 29, 2022, notice letter, which

attached a copy of the'140 patent and described the alleged infringement, and service upon HPE of the Complaint in this case.

45. Additionally, upon information and belief, HPE knew or should have known of the '140 patent because the inventor Jeffrey Carley was employed at Hewlett Packard Enterprise Services while simultaneously consulting for his former employer Engedi Technologies, Inc., regarding the prosecution of patent families that were filed when he was CTO at Engedi, including the '140 patent family. More specifically, Mr. Carley co-founded and operated as the CTO of Engedi Technologies from 2002 through 2005, during which time he was named inventor on several patent applications that were assigned to Engedi. From 2005 through 2011 Mr. Carley consulted for Engedi and/or Engedi's successor in interest specifically regarding the prosecution of the patent families that he was involved with while at Engedi. From 2009 through 2014 Mr. Carley was employed by Hewlett Packard Enterprise Services (which would eventually become HPE) as a Senior Network Engineer. Thus, at the time Mr. Carley was hired by Hewlett Packard Enterprise Services and for well over two years thereafter he was aiding in the prosecution of his previously filed patent applications, including continuations of the application that became the '140 patent, which had issued a little over a year before Mr. Carley began working for HPE. Upon information and belief HPE requires approval for continued work outside of HPE employment relating to similar areas of business, particularly involving intellectual property, and therefore, would have (or should have) known of the '140 patent at least as early as April 2009 when Mr. Carley was hired as a result of the disclosures associated with obtaining such approval.

46. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '140 patent.

47. HPE has committed, and continues to commit, contributory infringement by, *inter alia*, knowingly selling products and/or services that when used cause the direct infringement of one or more claims of the '140 patent by a third party, and which have no substantial non-infringing uses, or include one or more separate and distinct components such as hardware/software especially made or adapted for use in infringement of the '140 patent that are not staple articles or commodities of commerce suitable for substantial non-infringing use, such as the iLO 5 processor, a portion thereof, and/or software modules responsible for the accused functionality described herein.

48. As a result of HPE's acts of infringement, IV has suffered and will continue to suffer damages in an amount to be paid at trial.

COUNT II
(HPE's Infringement of U.S. Patent No. 8,474,016)

49. The preceding paragraphs are reincorporated by reference as if fully set forth herein.

50. The inventions claimed in the '016 patent, taken alone or in combination, were not well-understood, routine, or conventional to one of ordinary skill in the art at the time of the invention. Rather, the '016 patent claims and teaches, *inter alia*, an improved way to provide secure access to and management of networked devices by using specialized hardware and software to apply cryptography to management requests and separate those requests from user data requests. The inventions improved upon then-existing secure access/remote management security techniques by utilizing a dedicated processor, distinct from the managed device's main processor, to decrypt management requests. The inventions also improved upon said techniques by utilizing a dual bus architecture including a bus controller that receives encrypted management requests from one bus and conveys them to the dedicated processor over another bus.

51. The inventions claimed in the ’016 patent pioneered a particular bus architecture in managed devices that included secure remote management hardware, that separated management data from user data. This drastically reduced the comingling of user and management data on the managed device thus significantly enhancing device security. By also employing encryption of data comprising management requests, the inventions provided an extremely resilient secure remote management solution that is far less vulnerable to both internal and external threats.

52. The inventions claimed in the ’016 patent represent technical solutions to an unsolved technological problem. The written description of the ’016 patent describes, in technical detail, each of the limitations in the claims, allowing a person of skill in the art to understand what those limitations cover, and therefore what was claimed, and also to understand how the non-conventional and non-generic ordered combination of the elements of the claims differ markedly from what had been performed in the industry prior to the inventions of the ’016 patent. More specifically, the claims of the ’016 patent recite an apparatus, comprising a processor configured to control one or more functions of a network device having a network interface, the network device being configured to receive data requests and an encrypted form of management requests via the network interface, the management requests being from a remote administrator. The apparatus also includes a first bus, and bus controller coupled to the processor via the first bus, the bus controller also being coupled to a second bus of the network device that is distinct from the first bus. The apparatus is further configured such that the bus controller receives the encrypted form of the management requests from the second bus and conveys them to the processor via the first bus for decryption. The claimed network device additionally has a separate processor to

facilitate operation of the network device which is distinct from the processor that receives and decrypts the management requests.

53. The system covered by the asserted claims, therefore, differs markedly from the prior systems in use at the time of this invention, which, *inter alia*, lacked the claimed combination of the two distinct processors including the secure management processor, a dual bus architecture, a bus controller configured to receive and send an encrypted form of management requests to/from the buses respectively, so that the secure management processor can securely receive via a dual bus configuration, and decrypt, the management requests.

54. The ’016 patent is drawn to solving a specific, technical problem arising in the context of secure remote access/management of distributed network devices. Consistent with the problem addressed being rooted in such secure remote access/management technology, the solutions disclosed in the ’016 patent consequently are also rooted in that same technology and cannot be performed with pen and paper or in the human mind.

55. HPE has directly infringed, and continues to directly infringe, literally and/or by the doctrine of equivalents, individually and/or jointly, at least claim 1 of the ’016 patent by making, using, testing, selling, offering for sale, and/or importing into the United States products and/or services covered by one or more claims of the ’016 patent. HPE’s products and/or services that infringe the ’016 patent include all products and services that use an iLO 5 processor, which upon information and belief, include but are not limited to, the HPE ProLiant Gen 10 series servers, the HPE ProLiant Gen 10 Plus series servers, the HPE ProLiant e900 series server blades, the HPE Edgeline Converged Edge System, the HPE Apollo 2000, 4000 and 6000 Series Systems, the HPE Apollo Gen 10 series servers, the HPE Apollo Gen 10 Plus series servers, the HPE Edgeline e900 series server blades, HPE SimpliVity Gen 10 series nodes, HPE SimpliVity 2600 series nodes,

HPE Synergy Gen 10 series compute modules, the HPE Gen 10 series servers for HPE Ezmeral Container Platform (including when provided as a GreenLake service), the HPE Apollo series and ProLiant series modules for Qumulo, and any hosted or on-demand services offered by HPE using the aforementioned hardware/software, as well as any other HPE products and/or services, either alone or in combination, that operate in substantially the same manner (together the "Accused '016 Products" or "Accused Products").

56. Claim 1 of the '016 patent is reproduced below:

> *1. An apparatus, comprising:*
>
> *a processor configured to control one or more functions of a network device having a network interface, wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, wherein the management requests are from a remote administrator;*
>
> *a first bus; and*
>
> *a bus controller coupled to the processor via the first bus, wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus, wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus;*
>
> *wherein the processor is configured to decrypt the encrypted form of the management requests, wherein the network device includes a processor configured to facilitate operation of the network device, and wherein the processor of the apparatus is distinct from the processor included in the network device.*

57. The Accused '016 Products provide an apparatus comprising a processor configured to control one of more functions of a network device having a network interface. As one non-limiting example, the Accused '016 Products are network devices, modules and/or nodes, such as the HPE ProLiant Gen 10 series servers, that include an HPE iLO secure processor with

an embedded ARM (or similar) core for controlling remote management of the Accused '016 Products, as seen below:

HPE Integrated Lights Out (iLO 5) for Gen10 Servers - Overview

iLO 5

iLO is an embedded technology that ships in HPE servers. It is the core foundation for the intelligence of the HPE servers. This technology is combination of the iLO ASIC that is part of the server-board and the firmware that powers the ASIC. Industry leading features that enhance server administrator productivity are available through optional licenses. The available licenses are iLO advanced premium security edition (Supported only on Gen10 and later servers), iLO advanced, iLO essentials and iLO scale out (Supported on all generation servers)

iLO 5 is a remote server management processor embedded on the system boards of supported HPE servers and compute modules. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely.

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

You can use the iLO web interface to access iLO through a supported browser to monitor and configure managed servers.

The HPE InfoSight portal is a secure web interface hosted by HPE that allows you to monitor supported devices through a graphical interface.

Embedded System Health for HPE ProLiant

On supported server models, the HPE iLO for ProLiant management processor monitors fans, temperature sensors, power supply sensors and VRMs without having the System Management Driver loaded. The status of these is accessible from all HPE iLO for ProLiant user interfaces (browser, SMASH command line Redfish API, XML scripts and IPMI) independent of the host operating system The intelligence of iLO manages the Sea of Sensors thermal control, directs the Dynamic Power Capping technology and monitors the health of server components.

Production network

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network. Using a Shared Network Port configuration reduces the amount of networking hardware and infrastructure required to support iLO.

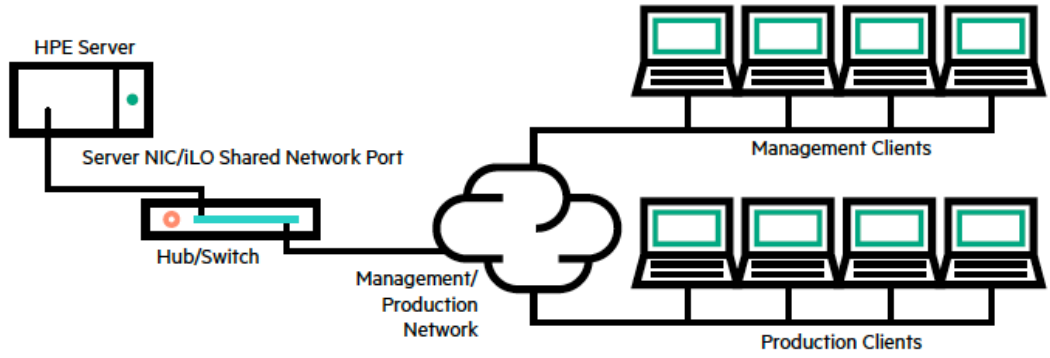
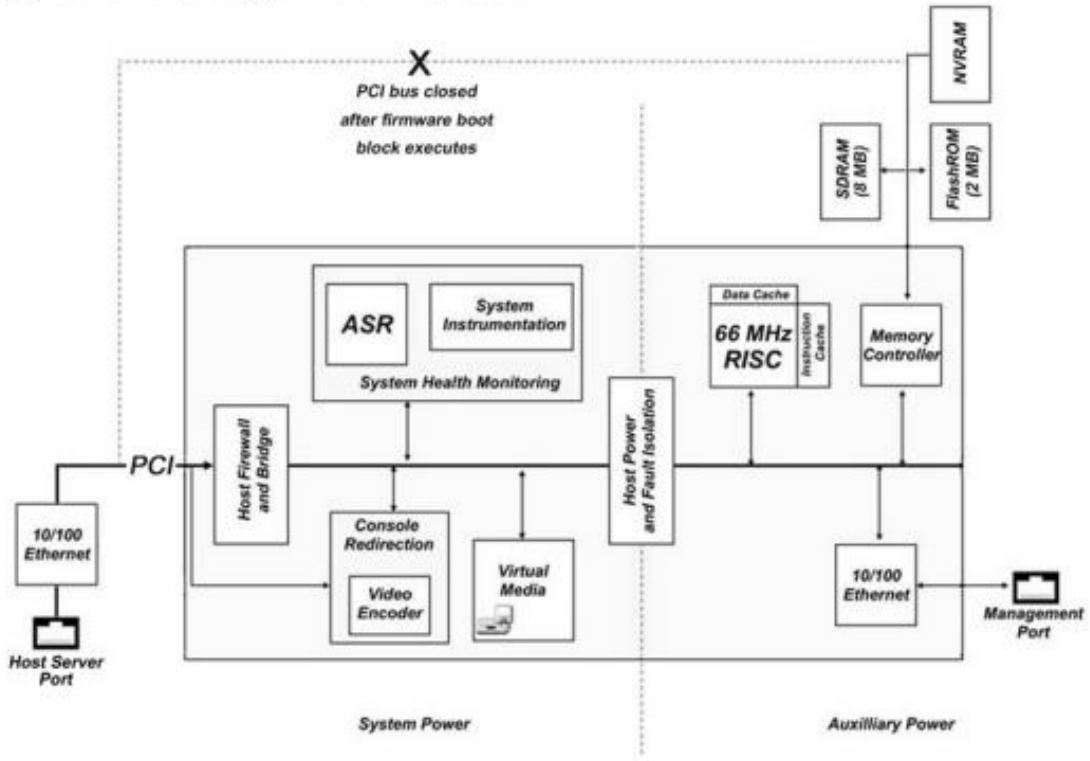


Figure 1. Schematic diagram of the iLO processor



iLO management for HPE ProLiant

HPE Agentless management 2.0:The base hardware monitoring and alerting capability is built into the system (Running on the HPE iLO chipset) and starts working the moment that a power cord and an Ethernet cable is connected to the server. This means that:

- All core management is out-of-band for increased security and stability: no OS software required, no open SNMP port on the OS and zero downtime updates
- Monitor and alerting on key internal server components: CPUs, memory, temperatures, fans, Smart Array controllers, hard drives (Including cache modules) and power supplies
- HPE SIM can see the system and will give users preview of the system health summary and sub-system details
- iLO integrates with HPE OneView

HPE Active Health System

- HPE Active health system is an essential component of the HPE iLO management
- It provides users with: Diagnostics tools/scanners wrapped into one; always on, continuous monitoring for increased stability and shorter downtimes; Rich configuration history; health and service alerts; Easy export and upload to service and support

HPE Active Healthy System Viewer Tool

Enables user to read the active health system log files. It will provide errors messages and advises on a resolution. Use can create a support file, simply by uploading users AHS log file from within this tool

HPE Intelligent Provisioning

- Let's users provision and configure a single server without any separate media
- No more Smart Start CDs or smart update firmware DVDs are needed

HPE Embedded Remote Support

- Hewlett Packard Enterprise offers embedded remote support that allows a user to enable remote support directly from iLO (Also OA and IP) without installing OS agents on the device, greatly reducing the time to activate remote monitoring
- Through insight remote support 7.0.5 and later versions and insight online direct connect capability, users now benefit from 24x7 remote monitoring, auto-generated service events, support cases and anywhere, anytime monitoring with HPE Insight online, a personalized cloud-based IT dashboard

HPE iLO On System Management	
Architecture	PCI Express based health and remote management ASIC
Processor	**iLO 5** Embedded ARM processor core operating at 800MHz **iLO 4** Embedded ARM processor core operating at 400MHz

Interfaces

Serial	**Optional, rear**
Display Port	1 (SFF 1 front, optional via Universal Media Bay, 826708-B21), 8 LFF chassis standard
FlexibleLOM Network Ports	4 x 1 Gb ports shipping standard with optional FlexibleLOM or stand up card

58. Furthermore, the Accused ’016 Products are configured to receive data requests and encrypted management requests via the network interface, wherein the management requests are from a remote administrator. For example, the Accused Products include an iLO processor with an ARM (or similar) core for secure remote administration and which can be configured to share a network connection/port with data requests to/from a production network. The Accused Products decrypt received management requests, as seen below:

iLO 5 is a remote server management processor embedded on the system boards of supported HPE servers and compute modules. iLO enables the monitoring and controlling of servers from remote locations. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely.

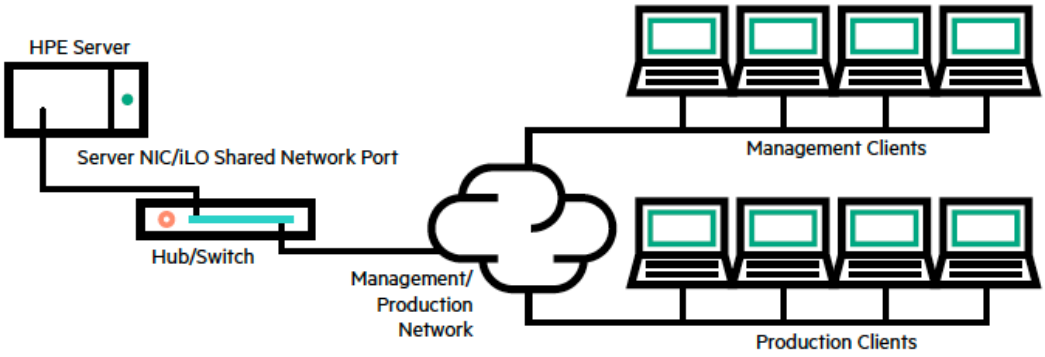
Production network

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network. Using a Shared Network Port configuration reduces the amount of networking hardware and infrastructure required to support iLO.

iLO network port configuration options

The iLO subsystem provides the following options for network connection:

- iLO dedicated network port - Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled iLO) on the back of the server.
- Shared network port LOM - Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.
- Shared network port FlexibleLOM - Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.



iLO encryption settings

HPE iLO Standard, that comes with every Gen10 or later server, gives customers the ability to configure servers in one of three security states. With an iLO Advanced license, customers that need the highest-level encryption capabilities of CNSA have a fourth security state available to them.

As you move up the scale in security, the server enforces stronger encryption rules for web pages, SSH, and network communications. Note that both ends of each network connection must support the encryption rules, or they cannot communicate, and some interfaces are shut down to limit potential security threats.

SSL cipher and MAC support

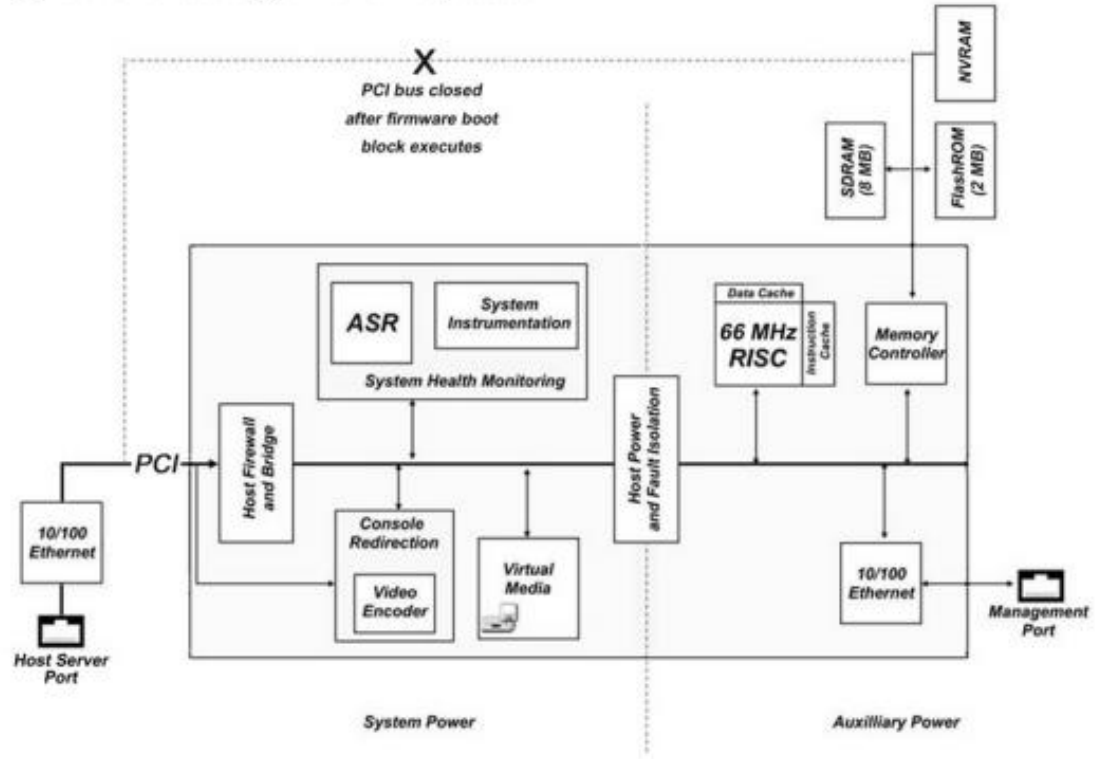
iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. Encryption of HTTP data provided by SSL ensures that the data is secure as it is transmitted across the network.

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the **Encryption** page.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, key manager servers, SSO servers, Insight Remote Support servers, https:// URLs used in virtual media, the iLO RESTful API, CLI commands, and iLO Federation group firmware updates.

59. The Accused ’016 Products further comprise a first bus and a bus controller coupled to the processor via the first bus, wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus. For example, the iLO processor is embedded in the Accused Products themselves and includes an ARM (or similar) core. The iLO processor also includes a bus controller that is coupled to the ARM core via the first bus, and coupled to a second bus distinct from the first bus, as illustrated below:

Figure 1. Schematic diagram of the iLO processor



Network and management ports

Because of the host firewall and bridge logic within iLO, there is no connection between the iLO management port and the host server Ethernet port (Figure 1). Even when using the shared network port (SNP), it is impossible for the iLO processor to bridge traffic between the two network interface controllers (NICs) so that data flows from the management NIC to the host server NIC. An iLO device will not be able to route packets between its 10/100 Ethernet port and an Ethernet port (possibly embedded) on the host server.

Firewall logic

The iLO management processor includes a host firewall and bridge logic (Figure 1) that enables iLO to control the flow of information between the host server and the management console. The firewall logic protects against unauthorized access through the host system PCI bus and therefore shields sensitive keys and data that are stored in memory and firmware.

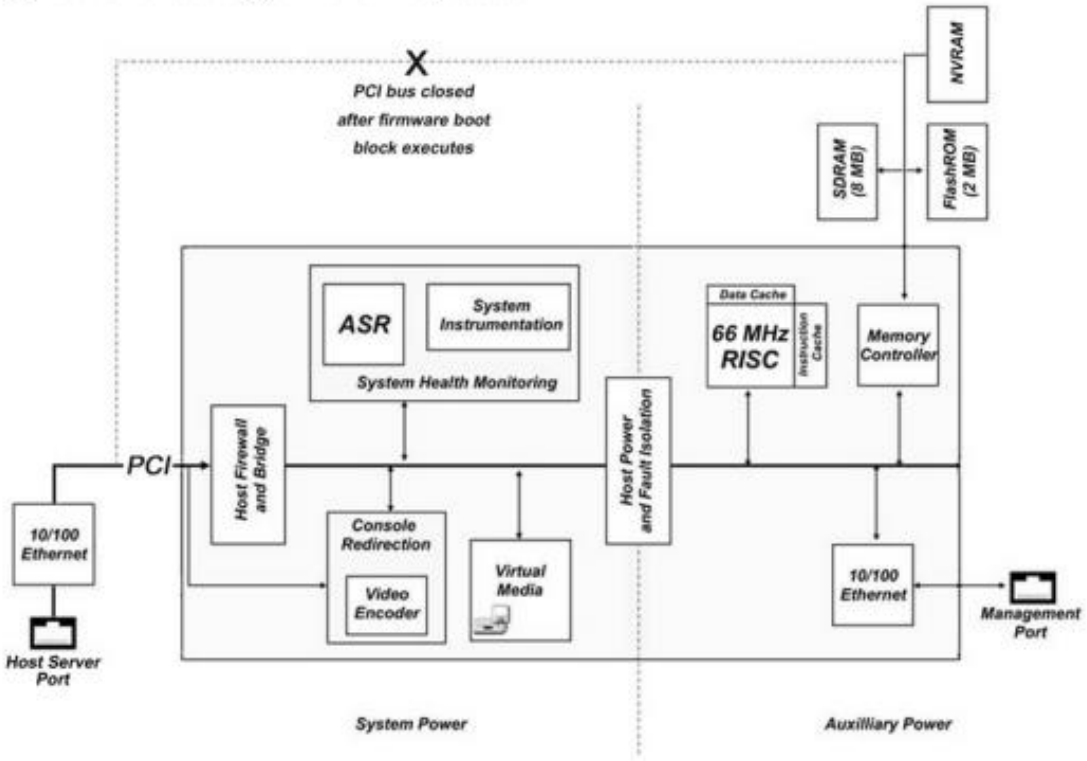
HPE iLO On System Management	
Architecture	PCI Express based health and remote management ASIC
Processor	**iLO 5** Embedded ARM processor core operating at 800MHz **iLO 4** Embedded ARM processor core operating at 400MHz

Interfaces

Serial	**Optional, rear**
Display Port	1 (SFF 1 front, optional via Universal Media Bay, 826708-B21), 8 LFF chassis standard
FlexibleLOM Network Ports	4 x 1 Gb ports shipping standard with optional FlexibleLOM or stand up card

60. In addition, the bus controller in the Accused ’016 Products is configured to receive the encrypted form of the management requests from the second bus, and to convey the encrypted form of the management requests to the processor via the first bus. For example, the Accused Products can use the shared network port to receive encrypted management requests, which are passed from the shared port over a PCI bus to bus logic in the ILO processor, from which they are then conveyed to the embedded ARM (or similar) core in the iLO processor over another bus, as illustrated below:

Figure 1. Schematic diagram of the iLO processor



Network and management ports

Because of the host firewall and bridge logic within iLO, there is no connection between the iLO management port and the host server Ethernet port (Figure 1). Even when using the shared network port (SNP), it is impossible for the iLO processor to bridge traffic between the two network interface controllers (NICs) so that data flows from the management NIC to the host server NIC. An iLO device will not be able to route packets between its 10/100 Ethernet port and an Ethernet port (possibly embedded) on the host server.

Firewall logic

The iLO management processor includes a host firewall and bridge logic (Figure 1) that enables iLO to control the flow of information between the host server and the management console. The firewall logic protects against unauthorized access through the host system PCI bus and therefore shields sensitive keys and data that are stored in memory and firmware.

HPE iLO On System Management	
Architecture	PCI Express based health and remote management ASIC
Processor	**iLO 5** Embedded ARM processor core operating at 800MHz **iLO 4** Embedded ARM processor core operating at 400MHz

Interfaces

Serial	**Optional, rear**
Display Port	1 (SFF 1 front, optional via Universal Media Bay, 826708-B21), 8 LFF chassis standard
FlexibleLOM Network Ports	4 x 1 Gb ports shipping standard with optional FlexibleLOM or stand up card

Security keys

Manages confidentiality of sensitive data and transactions. iLO protects privacy through TLS encryption of web pages and the AES encryption of remote console and virtual serial port data. iLO can be configured to allow only the highest cryptographic methods (like AES) to be used. iLO uses layers of security and industry-standard methods to secure access to the server. When high encryption modes are not used, iLO might negotiate weaker keys or algorithms.

SSL cipher and MAC support

iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. Encryption of HTTP data provided by SSL ensures that the data is secure as it is transmitted across the network.

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the **Encryption** page.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, key manager servers, SSO servers, Insight Remote Support servers, https:// URLs used in virtual media, the iLO RESTful API, CLI commands, and iLO Federation group firmware updates.

iLO encryption settings

HPE iLO Standard, that comes with every Gen10 or later server, gives customers the ability to configure servers in one of three security states. With an iLO Advanced license, customers that need the highest-level encryption capabilities of CNSA have a fourth security state available to them.

As you move up the scale in security, the server enforces stronger encryption rules for web pages, SSH, and network communications. Note that both ends of each network connection must support the encryption rules, or they cannot communicate, and some interfaces are shut down to limit potential security threats.

High Security

When iLO is set to this security state:

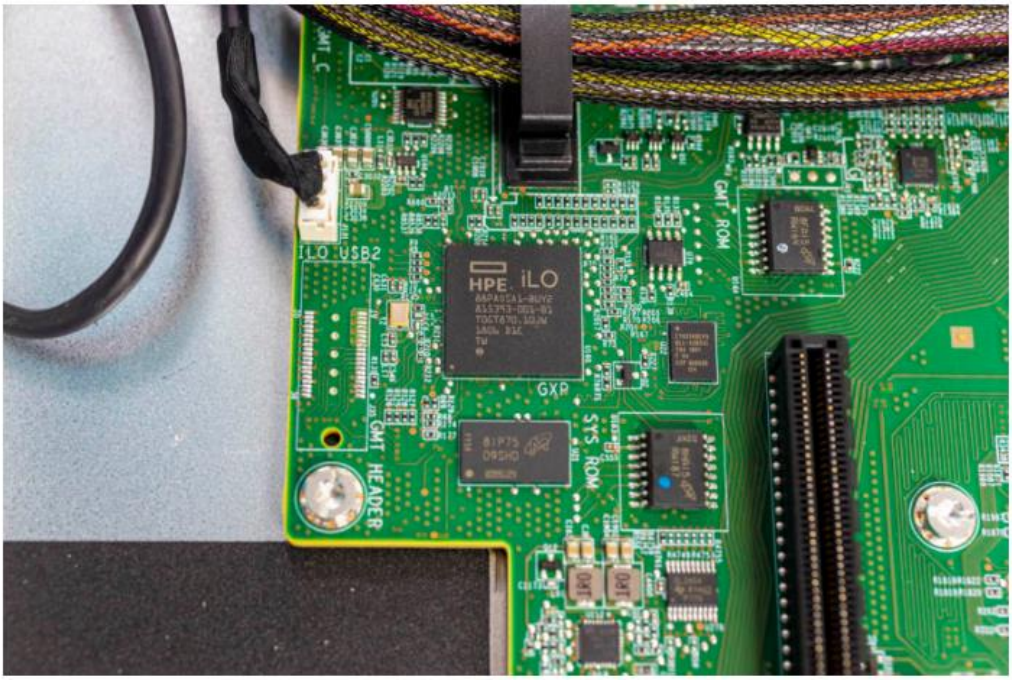
- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.

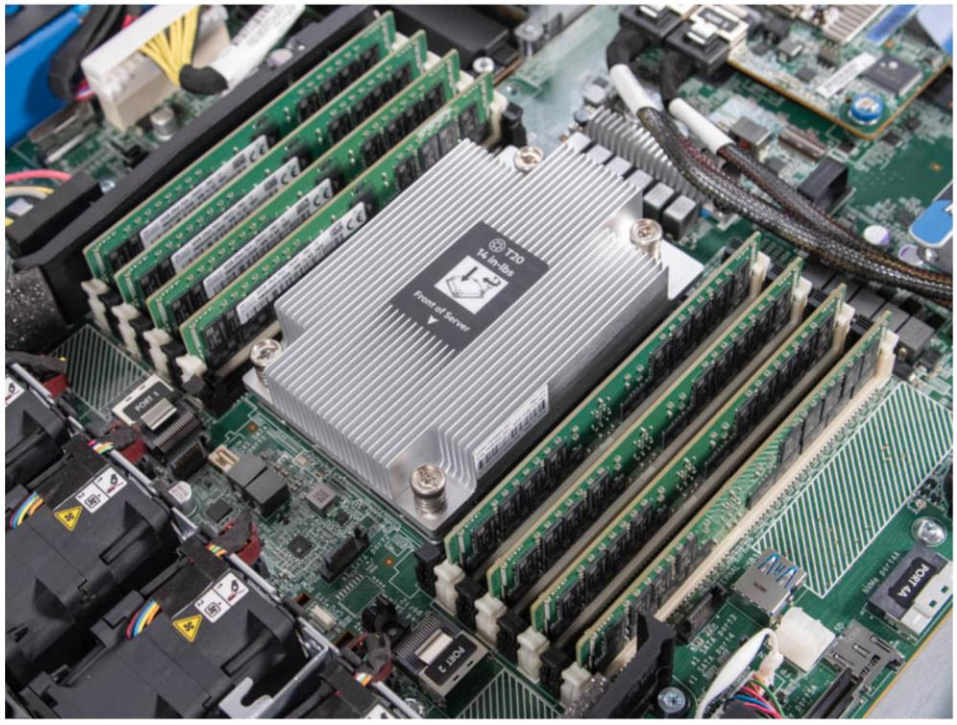
61. Furthermore, a secure management processor in the Accused ’016 Products is configured to decrypt the encrypted form of the management requests. The Accused Products also include a separate processor configured to facilitate the operation of the network device (i.e., each Accused Product), wherein the separate processor is distinct from the secure management processor configured to decrypt the encrypted form of the management requests. For example, the

Accused Products include an iLO secure processor with an embedded ARM (or similar) core for secure remote management that decrypts received encrypted management messages, where the iLO processor is distinct from each of the Accused Product's main processor that processes data requests received by the Accused Products. This is illustrated below:

HPE ProLiant DL325 Gen10 ILO 5 Chip

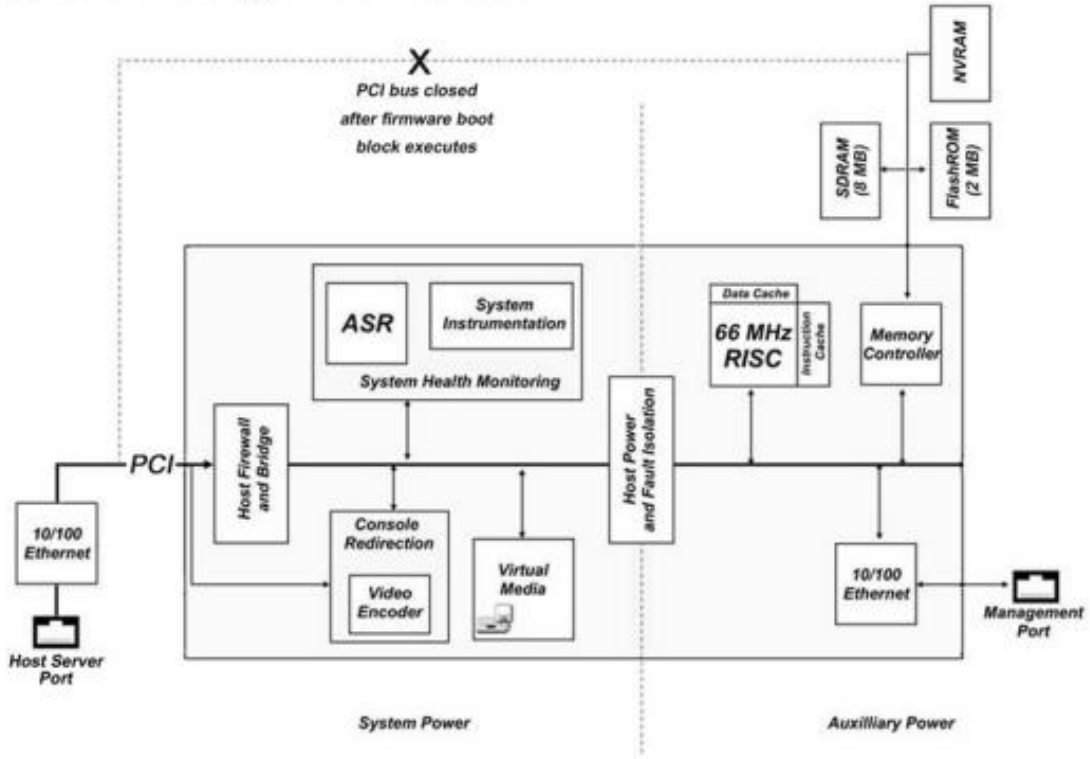


HPE ProLiant DL325 Gen10 ILO 5 Chip



HPE ProLiant DL325 Gen10 CPU And Memory

Figure 1. Schematic diagram of the iLO processor



SSL cipher and MAC support

iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. Encryption of HTTP data provided by SSL ensures that the data is secure as it is transmitted across the network.

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the **Encryption** page.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, key manager servers, SSO servers, Insight Remote Support servers, https:// URLs used in virtual media, the iLO RESTful API, CLI commands, and iLO Federation group firmware updates.

High Security

When iLO is set to this security state:

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

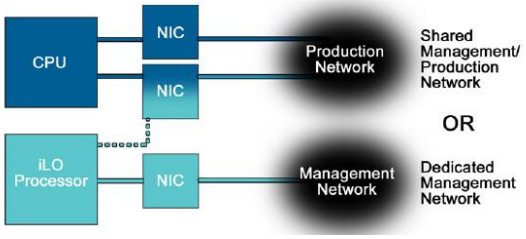
  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.

Authentication determines who is at the other end of the network connection. iLO authenticates users with 128-bit Secure Socket Layer (SSL) encryption.

Data integrity verifies that no one has altered incoming commands or data. iLO uses digital signatures and trusted Java™ and ActiveX applets (used by the Integrated Remote Console) to verify data integrity.

Privacy refers to confidentiality of sensitive data and transactions. iLO protects privacy through the 128-bit SSL encryption of web pages and the RC4 encryption of remote console and virtual serial port data.

Figure 2. Shared network port is available for most ProLiant servers with the iLO processor.



Processors – Up to 2 of the following depending on model.

Intel Xeon Models
Platinum 8280M Processor
Platinum 8280L Processor
Platinum 8280 Processor
Platinum 8276M Processor
Platinum 8276L Processor
Platinum 8276 Processor
Platinum 8270 Processor

62. Additionally, HPE has been, and currently is, an active inducer of infringement of the ’016 patent under 35 U.S.C. § 271(b) and a contributory infringer of the ’016 patent under 35 U.S.C. § 271(c).

63. HPE has actively induced, and continues to actively induce, infringement of the ’016 patent by intending that others use, offer for sale, or sell in the United States, products and/or services covered by one or more claims of the ’016 patent, including but not limited to, all products and services that use an iLO 5 embedded processor, which upon information and belief, include but are not limited to, the HPE ProLiant Gen 10 series servers, the HPE ProLiant Gen 10 Plus series servers, the HPE ProLiant e900 series server blades, the HPE Edgeline Converged Edge System, the HPE Apollo 2000, 4000 and 6000 Series Systems, the HPE Apollo Gen 10 series servers, the HPE Apollo Gen 10 Plus series servers, the HPE Edgeline e900 series server blades, HPE SimpliVity Gen 10 series nodes, HPE SimpliVity 2600 series nodes, HPE Synergy Gen 10 series compute modules, the HPE Gen 10 series servers for HPE Ezmeral Container Platform (including when provided as a GreenLake service), the HPE Apollo series and ProLiant series modules for Qumulo, and any hosted or on-demand services offered by HPE using the aforementioned hardware/software, as well as any other HPE products and/or services, either alone or in combination, that operate in substantially the same manner. HPE provides these products and/or services to others, such as customers, resellers, partners and end-user customers, who, in turn, in accordance with HPE’s design, intent and directions, use, provision for use, offer for sale, or sell in the United States the foregoing products and/or services that directly infringe one or more claims of the ’016 patent as described above. HPE’s inducement includes the directions and instructions found at one or more of the following links, the provision of which is on-going as of the filing of this Complaint and the content of which is specifically illustrated above

- https://support.hpe.com/hpesc/public/docDisplay?docId=a00105236en_us
- https://www.hpe.com/psnow/doc/c04154343.html?jumpid=in_lit-psnow-red
- https://www.informatica.us.es/docs/operativa/HP/HP-iLO-Seguridad.pdf
- https://support.hpe.com/hpesc/public/docDisplay?docId=c04530504

- https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-a00026111en_us
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00039732en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00045457en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00026106en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00045462en_us&docLocale=en_US
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00018323en_us

64. HPE has contributed to, and continues to contribute to, the infringement of the ’016 patent by others by knowingly providing one or more components, for example the iLO 5 processor, a portion thereof, and/or the software modules responsible for the accused functionality described herein, that, when installed, configured, and used result in systems that, as intended by HPE described above, directly infringe one or more claims of the ’016 patent.

65. HPE knew of the ’016 patent, or should have known of the ’016 patent, but was willfully blind to its existence. Upon information and belief, HPE has had actual knowledge of the ’016 patent since at least as early as the receipt of IV’s June 29, 2022, notice letter, which attached a copy of the’016 patent, and service upon HPE of the Complaint in this case. Additionally, upon information and belief, HPE knew or should have known of the ‘016 patent or the applications that became the ’016 patent because the inventor Jeffrey Carley was employed at Hewlett Packard Enterprise Services while simultaneously consulting for his former employer Engedi Technologies, Inc., regarding the prosecution of patent applications that were filed when he was CTO at Engedi. More specifically, Mr. Carley co-founded and operated as the CTO of Engedi Technologies from 2002 through 2005, during which time he was named inventor on several patent applications that were assigned to Engedi. From 2005 through 2011 Mr. Carley

consulted for Engedi and/or Engedi's successor in interest specifically regarding the prosecution of the patent families that he was involved with while at Engedi. From 2009 through 2014 Mr. Carley was employed by Hewlett Packard Enterprise Services (which would eventually become HPE) as a Senior Network Engineer. Thus, at the time Mr. Carley was hired by Hewlett Packard Enterprise Services and for well over two years thereafter he was aiding in the prosecution of his previously filed patent applications, including the application that became the '016 patent. Upon information and belief HPE requires approval for continued work outside of HPE employment relating to similar areas of business, and particularly involving intellectual property, and therefore would have (or should have) known of application 11/946,976 (which issued as the '016 patent) at least as early as April 2009 when Mr. Carley was hired, and no later than the patent's issue date of June 25, 2013.

66. By the time of trial, HPE will or should have known and intended (since receiving such notice) that its continued actions would infringe and actively induce and contribute to the infringement of one or more claims of the '016 patent.

67. HPE has committed, and continues to commit, contributory infringement by, *inter alia*, knowingly selling products and/or services that when used cause the direct infringement of one or more claims of the '016 patent by a third party, and which have no substantial non-infringing uses, or include one or more separate and distinct components such as hardware/software especially made or adapted for use in infringement of the '016 patent that are not staple articles or commodities of commerce suitable for substantial non-infringing use, such as the iLO 5 processor, a portion thereof, and/or software modules responsible for the accused functionality described herein.

68. As a result of HPE's acts of infringement, IV has suffered and will continue to suffer damages in an amount to be paid at trial.

PRAYER FOR RELIEF

IV requests that the Court enter judgment as follows:

(A) that HPE has infringed one or more claims of the asserted patents, directly and/or indirectly, literally and/or under the doctrine of equivalents;

(B) awarding damages sufficient to compensate IV for HPE's infringement under 35 U.S.C. § 284;

(C) finding this case exceptional under 35 U.S.C. § 285 and awarding IV its reasonable attorneys' fees;

(D) awarding IV its costs and expenses incurred in this action;

(E) awarding IV prejudgment and post-judgment interest; and

(F) granting IV such further relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

IV demands trial by jury of all claims so triable under Federal Rule of Civil Procedure 38.

Dated: June30, 2022.

Respectfully submitted,

/s/ Karl Rupp

Karl Rupp
State Bar No. 24035243
SOREY & HOOVER, LLP
100 N. 6TH Street, Ste. 502
Waco, Texas 76701
Tel: (903) 230-5600
Fax: (903) 230-5656
krupp@soreylaw.com

Paul J. Hayes
phayes@princelobel.com
Matthew D. Vella
mvella@princelobel.com
Robert R. Gilman
rgilman@princelobel.com
Jonathan DeBlois
jdeblois@princelobel.com
Brian Seeve
bseeve@princelobel.com
PRINCE LOBEL TYE LLP
One International Place, Suite 3700
Boston, MA 02110
Tel: (617) 456-8000

COUNSEL FOR PLAINTIFFS