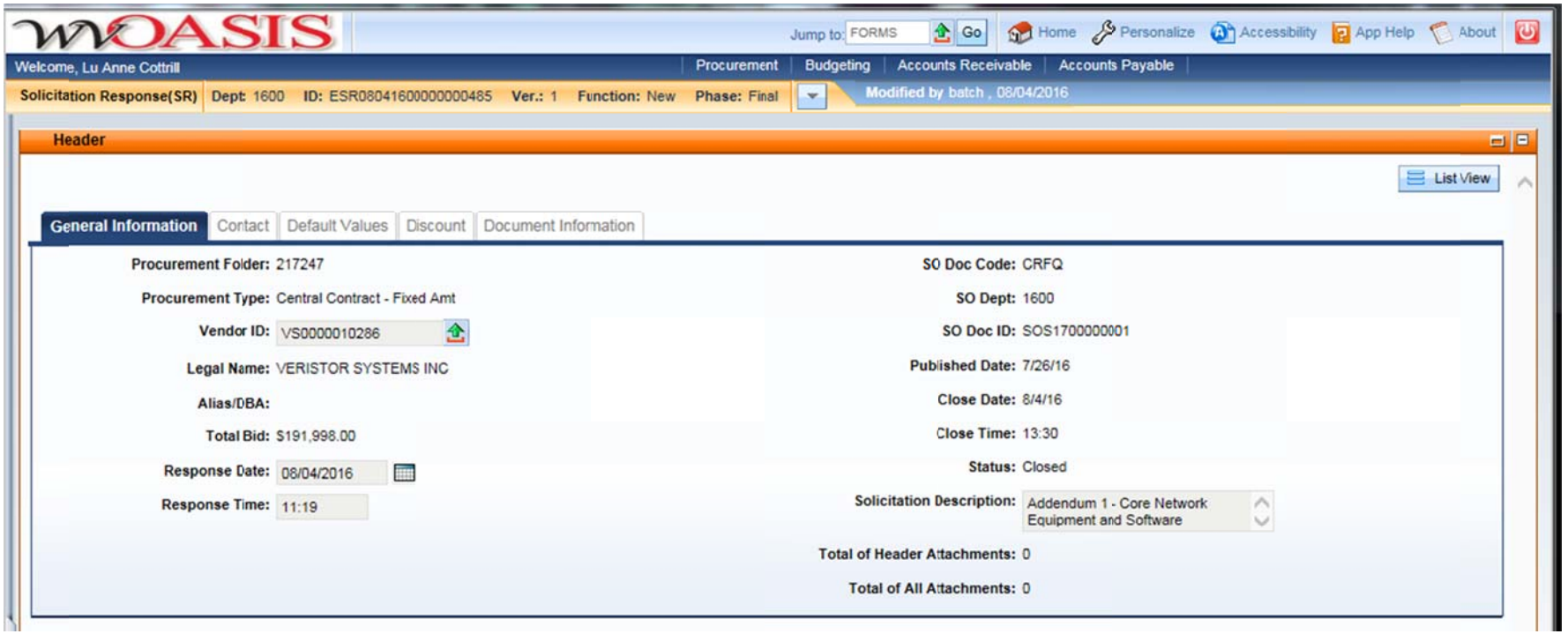
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 1600 ID: ESR08041600000000485 Ver.: 1 Function: New Phase: Final
Modified by batch , 08/04/2016
Header
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 217247
Procurement Type: Central Contract - Fixed Amt
Vendor ID: VS0000010286
Legal Name: VERISTOR SYSTEMS INC
Alias/DBA:
Total Bid: $191,998.00
Response Date: 08/04/2016
Response Time: 11:19
SO Doc Code: CRFQ
SO Dept: 1600
SO Doc ID: SOS1700000001
Published Date: 7/26/16
Close Date: 8/4/16
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum 1 - Core Network Equipment and Software
Total of Header Attachments: 0
Total of All Attachments: 0

Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder : 217247

Solicitation Description : Addendum 1 - Core Network Equipment and Software

Proc Type : Central Contract - Fixed Amt

Date issued	Solicitation Closes	Solicitation Response	Version
	2016-08-04 13:30:00	SR 1600 ESR08041600000000485	1

VENDOR

VS0000010286

VERISTOR SYSTEMS INC

Solicitation Number: CRFQ 1600 SOS1700000001

Total Bid : $191,998.00 **Response Date:** 2016-08-04 **Response Time:** 11:19:27

Comments: At VeriStor we relish the opportunity to help the State of West Virginia Secretary of State's office with their core switching project. We have presented a product set that has an equal and/or better functionality. It is our goal to present alternative. We believe this solution will provide more security, visibility, and control over the network. At the same, providing Secretary or State's office with a more cost effective solution.
If we are awarded the opportunity, we look forward to discussing further details of the solution.
We look forward to your response.

FOR INFORMATION CONTACT THE BUYER

Linda Harper

(304) 558-0468
linda.b.harper@wv.gov

Signature on File **FEIN #** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	4.1.6.1 WS-C4510RE-S8+96V+ "or Equal"	1.00000	EA	$19,802.000000	$19,802.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.1 WS-C4510RE-S8+96V+ "or Equal"

Comments: HPE 7510 w 2x2.4Tbps MPU/Fabric Bundle

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	4.1.6.2 WS-X4748-RJ45V+E "or Equal".	5.00000	EA	$3,606.000000	$18,030.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.2 WS-X4748-RJ45V+E "or Equal".

Comments: HPE 7500 48p 1000BASE-T PoE+ SC Mod

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	4.1.6.3 WS-X45- SUP8-E "or Equal"	1.00000	EA	$8,005.000000	$8,005.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.3 WS-X45- SUP8-E "or Equal"

Comments: . HPE 7500 8-port 10G SFP+ Module

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	4.1.6..3 WS_X45- SUP8-E/2 "or Equal"	1.00000	EA	$8,005.000000	$8,005.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6..3 WS_X45- SUP8-E/2 "or Equal"

Comments: HPE 7500 8-port 10G SFP+ Module

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	4.1.6.4 C4500E-LB-IPB "or Equal"	1.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.4 C4500E-LB-IPB "or Equal"

Comments: Included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	4.1.6.5 CAB-CON-C4K-RJ45 "or Equal"	1.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per Section 4.1.6.5 CAB-CON-C4K-RJ45 "or Equal"

Comments: Included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	4.1.6.6 CAT4500e SUP8e Universal Cryptographic Image	1.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.6 CAT4500e SUP8e Universal Cryptographic Image, "or equal"

Comments: included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	4.1.6.7 C4K-SLOT-CVR-E "or Equal".	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.7 C4K-SLOT-CVR-E "or Equal".

Comments: Cover will be a part of the quote

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	4.1.6.8 PWR-C45-6000ACV "or Equal";	1.00000	EA	$2,573.000000	$2,573.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.8 PWR-C45-6000ACV "or Equal";

Comments: HPE 7500 6000W AC Power Supply

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
10	4.1.6.8 PWR-C45-6000ACV/2 "or Equal"	1.00000	EA	$2,073.000000	$2,073.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.8 PWR-C45-6000ACV/2 "or Equal"

Comments: HPE 7500 6000W AC Power Supply

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
11	4.1.6.9 CAB-L620P-C19-US "or Equal"	4.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.9 CAB-L620P-C19-US "or Equal"

Comments: Cable included

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
12	4.1.6.10 WS-X4712-SFP-E "or Equal",	1.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.10 WS-X4712-SFP-E "or Equal",

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
13	4.1.6.11 SFP-10G-SR-S= "or Equal"	10.00000	EA	$483.000000	$4,830.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.11 SFP-10G-SR-S= "or Equal"

Comments: HPE X130 10G SFP+ LC SR Transceiver

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
14	4.1.6.12 C3KX-NM-10G= "or Equal"	1.00000	EA	$1,772.000000	$1,772.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.6.12 C3KX-NM-10G= "or Equal

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
15	4.1.7.1. ASA5525-FPWR-K9 "or Equal"	2.00000	EA	$28,000.000000	$56,000.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4..7.1. ASA5525-FPWR-K9 "or Equal"

Comments: Palo Alto- PA-3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
16	4.1.7.2 ASA-IC-B-BLANK "or Equal".	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.2 ASA-IC-B-BLANK "or Equal".

Comments: Included in PA 3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
17	4.1.7.3 ASA5500X-SSD120INC "or Equal"	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.3 ASA5500X-SSD120INC "or Equal"

Comments: Included in PA 3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
18	4.1.7.4 ASA5525-MB "or Equal"	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.4 ASA5525-MB "or Equal"

Comments: Included in PA 3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
19	4.1.7.5 ASA5525- CTRL-LIC "or Equal".	2.00000	EA	$11,760.000000	$23,520.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.5 ASA5525- CTRL-LIC "or Equal".

Comments: PAN-PA-3060-GP-HA2 GlobalProtect Gateway subscription for device in an HA pair year 1, PA-3060
PAN-PA-3060-URL4-HA2 PANDB URL Filtering subscription for device in an HA pair year 1, PA-3060
PAN-PA-3060-WF-HA2
WildFire subscription for device in an HA pair year 1, PA-3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
20	4.1.7.6 ASA5500-ENCR-K9 "or Equal"	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.6 ASA5500-ENCR-K9 "or Equal"

Comments: Equal to PA-3060

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
21	4.1.7.7 SF-ASA-X-9.2.2-K8 "or Equal"	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.7 SF-ASA-X-9.2.2-K8 "or Equal"

Comments: equal component in above quotes.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
22	4.1.7.8 SF-ASA-FP5.4-K9 "or Equal".	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.8 SF-ASA-FP5.4-K9 "or Equal".

Comments: equal in above quotes.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
23	4.1.7.9 CAB-AC "or Equal"	2.00000	EA	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.7.9 CAB-AC "or Equal"

Comments: Included in Palo Alto Solution

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
24	4.1.8.7 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 1	12.00000	MO	$2,301.000000	$27,612.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.7 CON-SNT-WS-C451R for SmartNet-8x5xNBD for 1 year, or equal

Comments: This will represent the HPE options: 4 years of maintenance
First, Maintenance/upgrades are included. However, for your requirements of a 15 min response, 2 contacts there is no SKU from HPE for one year of Proactive Care Advanced. A custom agreement can be crafted if awarded the contract. The quote in this response is for 3 year of maintenance.
Secondarily, for even more comprehensive support HPE offers a customizable Data Center Care Support. This can

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
25	4.1.8.8 CON-SNT-A25FPK9 SNTC-8XSXNBD for	12.00000	MO	$412.000000	$4,944.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.8 CON-SNT-A25FPK9 SNTC-8XSXNBD for SmartNet-8x5xNBD for 1 year, or equal

Comments: This is line is our response for maintenance and support for the Palo Alto PA-3060.
Year 1

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
26	4.1.8.8 CON-SNT-A25FPK9 SNTC-8XSXNBD for	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81111706			

Extended Description : Per section 4.1.8.8 CON-SNT-A25FPK9 SNTC-8XSXNBD for SmartNet-8x5xNBD

Comments: See above comments regarding support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
27	Installation Charges	1.00000	LS	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81111706			

Extended Description : Per section 4.1.8.8 CON-SNT-A25FPK9 SNTC-8XSXNBD for SmartNet-8x5xNBD

Comments: See above comments regarding support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
28	4.1.8.9 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 2	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.9 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 2 - OPTIONAL RENEWAL

Comments: Regarding HPE switches see above comment on line 24.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
29	4.1.8.10 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 2	12.00000	MO	$412.000000	$4,944.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.10 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 2 OPTIONAL RENEWAL

Comments: Year 2 Palo Alto estimated support

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
30	4.1.8.10 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 2	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.10 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 2 OPTIONAL RENEWAL

Comments: see above comments

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
31	4.1.8.11 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 3	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.11 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 3 - OPTIONAL RENEWAL

Comments: see above comments in line 24

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
32	4.1.8.12 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 3	12.00000	MO	$412.000000	$4,944.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.12 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 3 OPTIONAL RENEWAL

Comments: Palo Alto
Year 3

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
33	4.1.8.12 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 3	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.12 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 3 OPTIONAL RENEWAL

Comments: See above comments in line 24

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
34	4.1.8.13 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 4	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.12 CON-SNT-WS-C451R for SmartNet-8x5xNBD for Year 4 - OPTIONAL RENEWAL

Comments: Re: HPE switches see comments in line 24

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
35	4.1.8.14 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 4	12.00000	MO	$412.000000	$4,944.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.14 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 4 OPTIONAL RENEWAL

Comments: Palo Alto Estimate Support
Year 4

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
36	4.1.8.14 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 4	12.00000	MO	$0.000000	$0.00

Comm Code	Manufacturer	Specification	Model #
81110000			

Extended Description : Per section 4.1.8.14 CON-SNT-A25FPK9 SNTC-8XSXNBD, "or equal" Year 4 OPTIONAL RENEWAL

Comments: See comments on line 24

Overview

HPE FlexNetwork 7500 Switch Series

Product overview

The HPE FlexNetwork 7500 Switch Series comprises modular, multilayer chassis switches that meet the evolving needs of integrated services networks. The switches can be deployed in multiple network environments, including the enterprise LAN core, aggregation layer, and wiring closet edge.

They offer 40GbE connectivity and cost-effective, wire-speed 10GbE ports to safeguard the throughput and bandwidth needed for your mission-critical data and high-speed communications. A passive backplane, support for load sharing, and redundant management and fabrics help the switch series provide high availability.

Moreover, these switches deliver wire-speed Layer 2 and Layer 3 routing services for the most demanding applications with hardware-based IPv4 and IPv6 support.

Models

HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
HPE FlexNetwork 7510 Switch Chassis	JD238C
HPE FlexNetwork 7506 Switch Chassis	JD239C
HPE FlexNetwork 7503 Switch Chassis	JD240C
HPE FlexNetwork 7502 Switch Chassis	JD242C

Key features

- Versatile, high-performance modular switches
- Enterprise LAN core, aggregation, and edge
- Extensive switching and routing, IPv6, and multiprotocol label switching (MPLS)
- Advanced functionality with service modules

Overview

- Robust network and service virtualization

Features and benefits

Quality of Service (QoS)

- **IEEE 802.1p prioritization**
  delivers data to devices based on the priority and type of traffic
- **Class of Service (CoS)**
  sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Bandwidth shaping**
  - **Port-based rate limiting**
    provides per-port ingress-/egress-enforced increased bandwidth
  - **Classifier-based rate limiting**
    uses an access control list (ACL) to enforce increased bandwidth for ingress traffic on each port
  - **Reduced bandwidth**
    provides per-port, per-queue egress-based reduced bandwidth
- **Weighted random early detection (WRED)/random early detection (RED)**
  delivers congestion avoidance capabilities through the use of queue management algorithms
- **Powerful QoS feature**
  supports the following congestion actions: strict priority (SP) queuing, weighted round robin (WRR), weighted fair queuing (WFQ), and WRED
- **Traffic policing**
  supports Committed Access Rate (CAR) and line rate

Intrusion detection/prevention system (IDS/IPS)

- **Deep packet inspection**
  module supports deep packet inspection and examines the packet payload as well as the frame and packet headers; packets are dropped if attacks or intrusions are detected using signature-based or protocol anomaly-based detection
- **Signature-based detection**
  detects attacks that have known attack patterns; IPS maintains a signature database that contains the pattern definitions for known attacks that can be updated automatically using a subscription service
- **Protocol anomaly-based detection**
  detects attacks that use anomalies in application protocol payloads
- **Severity-based action policies**
  involve action taken against attacks based on their severity; available actions are "allow," "block," and "terminate connection" to provide appropriate mitigation
- **Signature update service**
  provides regular updates to the signature database, helping to ensure that the latest available signatures are installed

Virtual private network (VPN)

- **IPSec**
  provides secure tunneling over an untrusted network such as the Internet or a wireless network; offers data confidentiality, authenticity, and integrity between two network endpoints
- **Generic Routing Encapsulation (GRE)**

Overview

transports Layer 2 connectivity over a Layer 3 path in a secured way; enables the segregation of traffic from site to site

- **Manual or automatic Internet Key Exchange (IKE)**
  provides both manual or automatic key exchange required for the algorithms used in encryption or authentication; auto-IKE allows automated management of the public key exchange, providing the highest levels of encryption
- **Virtual Extensible LAN (VXLAN)**
  delivers network virtualization, enabling IP-based networks to support many VLAN overlays for use as a private collaboration network, or a single, end-to-end VLAN for WiFi. Requires Comware v7 with specific hardware only. Refer to the hardware manuals for details.

Management

- **Management interface control**
  provides management access through a modem port and terminal interface, as well as in-band and out-of-band Ethernet ports; provides access through terminal interface, Telnet, or secure shell (SSH)
- **Industry-standard CLI with a hierarchical structure**
  reduces training time and expenses, and increases productivity in multivendor installations
- **Management security**
  restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide Telnet and SNMP access; local and remote syslog capabilities allow logging of all access
- **SNMPv1, v2, and v3**
  provide complete support of SNMP; provide full support of industry-standard Management Information Base (MIB) plus private extensions; SNMPv3 supports increased security using encryption
- **sFlow (RFC 3176)**
  provides scalable ASIC-based wirespeed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes
- **Remote monitoring (RMON)**
  uses standard SNMP to monitor essential network functions; supports events, alarm, history, and statistics group plus a private alarm extension group
- **FTP, TFTP, and SFTP support**
  offers different mechanisms for configuration updates; FTP allows bidirectional transfers over a TCP/IP network; trivial FTP (TFTP) is a simpler method using User Datagram Protocol (UDP); Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security
- **Debug and sampler utility**
  supports ping and traceroute for both IPv4 and IPv6
- **Network Time Protocol (NTP)**
  synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so that the devices can provide diverse applications based on the consistent time
- **Network Quality Analyzer (NQA)**
  analyzes network performance and service quality by sending test packets, and provides network performance and service quality parameters such as jitter, TCP, or FTP connection delays and file transfer rates; allows a network manager to determine overall network performance and to diagnose and locate network congestion points or failures
- **Information center**
  provides a central repository for system and network information; aggregates all logs, traps, and debugging information generated by the system and maintains them in order of severity; outputs the network information to multiple channels based on user-defined rules
- **IEEE 802.1AB Link Layer Discovery Protocol (LLDP)**
  advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications
- **Dual flash images**

Overview

provides independent primary and secondary operating system files for backup while upgrading

- **Multiple configuration files**
  stores easily to the flash image

Connectivity

- **High-density port connectivity**
  Provides up to 10 interface module slots and up to 40 40GbE ports, 84 10GbE ports, 480 Fiber Gigabit ports, or 480 PoE-enabled ports per HPE 7500 Switch Series system
- **Jumbo frames**
  Allow high-performance remote backup and disaster-recovery systems with up to 9,216 bytes
- **Loopback**
  supports internal loopback testing for maintenance purposes and an increase in availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- **Ethernet operations, administration and maintenance (OAM)**
  detects data link layer problems that occurred in the "last mile" using the IEEE 802.3ah OAM standard; monitors the status of the link between two devices
- **Flexible port selection**
  Includes 100/1000BASE-X auto speed selection, 10/100/1000BASE-T auto speed detection, as well as auto duplex and MDI/MDI-X
- **Monitor link**
  collects statistics on performance and errors on physical links, increasing system availability
- **IEEE 802.3af Power over Ethernet (PoE)**
  provides up to 15.4 W per port to IEEE 802.3af-compliant PoE-powered devices such as IP phones, wireless access points, and security cameras
- **Dual-personality functionality**
  includes four 10/100/1000 ports or SFP slots for optional fiber connectivity such as Gigabit-SX, -LX, and -LH, or 100-FX
- **Packet storm protection**
  protects against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds
- **Flow control**
  provides back pressure using standard IEEE 802.3x, reducing congestion in heavy traffic situations
- **IEEE 802.3at Power over Ethernet (PoE+) support**
  provides up to 30 watts of power at the power sourcing equipment (PSE)

Performance

- **High-speed fully distributed architecture**
  Supports a maximum of 1,152 Gb/s switching capacity with a 2.4 Tb/s backplane, providing enhanced performance and future expansion capability; delivers up to 714 Mp/s throughput with dual fabrics; performs all switching and routing functions in the I/O modules; and meets the current and future demand of an enterprise's bandwidth-intensive applications
- **Scalable system design**
  Provides investment protection to support future technologies and higher-speed connectivity with a backplane designed to accommodate bandwidth increases
- **Flexible chassis selection**
  Enables you to tailor your product selections to your budget with a choice of six chassis, ranging from a 10-slot to a 2-slot chassis

Overview

Resiliency and high availability

- **Redundant/load-sharing fabrics, management, fan assemblies, and power supplies**
  increase total performance and power availability while providing hitless, stateful failover
- **All hot-swappable modules**
  Allows replacement of modules without any impact on other modules
- **Dual internal power supply**
  provides high reliability
- **Separate data and control paths**
  separates control from services and keeps service processing isolated; increases security and performance
- **Passive design system**
  delivers increased system reliability as the backplane has no active components
- **IEEE 802.3ad link-aggregation control protocol (LACP)**
  Supports up to 128 trunks, each with 8 links per trunk; and provides support for static or dynamic groups and a user-selectable hashing algorithm
- **Intelligent Resilient Fabric (IRF)**
  creates virtual resilient switching fabrics, where two or more switches perform as a single L2 switch and L3 router; switches do not have to be co-located and can be part of a disaster-recovery system; servers or switches can be attached using standard LACP for automatic load balancing and high availability; can eliminate the need for complex protocols like Spanning Tree Protocol, Equal-Cost Multipath (ECMP), or VRRP, thereby simplifying network operation
- **IRF capability**
  provides single IP address management for a resilient virtual switching fabric of up to four switches
- **Ring resiliency protection protocol (RRPP)**
  Provides standard sub-100 ms recovery for a ring Ethernet-based topology
- **Virtual Router Redundancy Protocol (VRRP)**
  allows a group of routers to dynamically back each other up to create highly available routed environments
- **Graceful restart**
  supports graceful restart for OSPF, IS-IS, BGP, LDP, and RSVP; the network remains stable during the active-standby switchover; after the switchover, the device quickly learns the network routes by communicating with adjacent routers; forwarding remains uninterrupted during the switchover to achieve nonstop forwarding (NSF)
- **Ultrafast protocol convergence with standards-based failure detection—bidirectional forwarding detection**
  Enables link connectivity monitoring and reduces network convergence time for the routing information protocol (RIP), OSPF, BGP, IS-IS, VRRP, MPLS, and IRF
- **Smart link**
  allows 50 ms failover between links
- **IP/LDP FRR**
  nodes are configured with backup ports, routes, and LSPs; local implementation requires no cooperation of adjacent devices, simplifying the deployment; solves the traditional convergence faults in IP forwarding and MPLS forwarding, protecting the links, nodes, and paths without establishing respective backup LSPs for them; realizes restoration within 50 ms, with the restoration time independent of the number of routes and fast link switchovers, without route convergence
- **In-Service Software Upgrade (ISSU)**
  applies patches and new service features to be installed without restarting the system, increasing network uptime and simplifying maintenance. Requires use of IRF, and R7169P01 or later releases.

Layer 2 switching

- **VLAN**
  Supports up to 4,096 port-based or IEEE 802.1Q-based VLANs; and supports MAC-based VLANs, protocol-based VLANs, and
  IP-subnet-based VLANs for added flexibility

Overview

- **Port isolation**
  increases security by isolating ports within a VLAN while still allowing them to communicate with other VLANs
- **Bridge Protocol Data Unit (BPDU) tunneling**
  transmits Spanning Tree Protocol BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs
- **GARP VLAN Registration Protocol**
  allows automatic learning and dynamic assignment of VLANs
- **Port mirroring**
  Duplicates port traffic (ingress and egress) to a local or remote monitoring port; and supports four mirroring groups, with an unlimited number of ports per group
- **Spanning Tree Protocol (STP)**
  supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- **Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) protocol snooping**
  controls and manages the flooding of multicast packets in a Layer 2 network
- **Device Link Detection Protocol (DLDP)**
  monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks
- **IEEE 802.1ad QinQ and selective QinQ**
  increase the scalability of an Ethernet network by providing a hierarchical structure; connect multiple LANs on a high-speed campus or metro network
- **Super VLAN**
  Saves IP address space, using RFC 3069 standard (also called VLAN aggregation)
- **Per-VLAN Spanning Tree Plus (PVST+)**
  allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs

Layer 3 services

- **Address Resolution Protocol (ARP)**
  determines the MAC address of another IP host in the same subnet; supports static ARPs; gratuitous ARP allows detection of duplicate IP addresses; proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 etwork
- **User Datagram Protocol (UDP) helper**
  redirects UDP broadcasts to specific IP subnets to prevent server spoofing
- **Dynamic Host Configuration Protocol (DHCP)**
  simplifies the management of large IP networks and supports client and server; DHCP Relay enables DHCP operation across subnets
- **Domain Name System (DNS)**
  provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server

Layer 3 routing

- **Static IPv4 routing**
  provides simple manually configured IPv4 routing
- **Routing Information Protocol (RIP)**
  uses a distance vector algorithm with UDP packets for route determination; supports RIPv1 and RIPv2 routing; includes loop protection
- **Open shortest path first (OSPF)**

Overview

delivers faster convergence; uses this link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

- **Intermediate system to intermediate system (IS-IS)**
  uses a path vector Interior Gateway Protocol (IGP), which is defined by the ISO organization for IS-IS routing and extended by IETF RFC 1195 to operate in both TCP/IP and the OSI reference model (Integrated IS-IS)
- **Border Gateway Protocol 4 (BGP-4)**
  delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks
- **Policy-based routing**
  makes routing decisions based on policies set by the network administrator
- **IP performance optimization**
  Provides a set of tools to improve the performance of IPv4 networks; and includes directed broadcasts, customization of TCP parameters, support of ICNP error packets, and extensive display capabilities
- **Unicast Reverse Path Forwarding (uRPF)**
  limits erroneous or malicious traffic in accordance with RFC 3074
- **Static IPv6 routing**
  provides simple manually configured IPv6 routing
- **Dual IP stack**
  maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design
- **Routing Information Protocol next generation (RIPng)**
  extends RIPv2 to support IPv6 addressing
- **OSPFv3**
  provides OSPF support for IPv6
- **IS-IS for IPv6**
  extends IS-IS to support IPv6 addressing
- **BGP+**
  extends BGP-4 to support Multiprotocol BGP (MBGP), including support for IPv6 addressing
- **IPv6 tunneling**
  allows IPv6 packets to traverse IPv4-only networks by encapsulating the IPv6 packet into a standard IPv4 packet; supports manually configured, 6to4, and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels; is an important element for the transition from IPv4 to IPv6
- **Multiprotocol Label Switching (MPLS)**
  uses BGP to advertise routes across Label Switched Paths (LSPs), but uses simple labels to forward packets from any Layer 2 or Layer 3 protocol, which reduces complexity and increases performance; supports graceful restart for reduced failure impact; supports LSP tunneling and multilevel stacks
- **Multiprotocol Label Switching (MPLS) Layer 3 VPN**
  allows Layer 3 VPNs across a provider network; uses MP-BGP to establish private routes for increased security; supports RFC 2547bis multiple autonomous system VPNs for added flexibility
- **Multiprotocol Label Switching (MPLS) Layer 2 VPN**
  establishes simple Layer 2 point-to-point VPNs across a provider network using only MPLS Label Distribution Protocol (LDP); requires no routing and therefore decreases complexity, increases performance, and allows VPNs of non-routable protocols; uses no routing information for increased security; supports Circuit Cross Connect (CCC), Static Virtual Circuits (SVCs), Martini draft, and Kompella-draft technologies
- **Virtual Private LAN Service (VPLS)**
  establishes point-to-multipoint Layer 2 VPNs across a provider network
- **Service loopback**
  allows any module to take advantage of higher-featured modules, including OAA modules, by redirecting traffic; reduces investment and enables higher bandwidth and load sharing; supports IPv6, IPv6

Overview

multicast, tunneling, and MPLS

Security

- **Access control list (ACL)**
  supports powerful ACLs for both IPv4 and IPv6; ACLs are used for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header; rules can be set to operate on specific dates or times
- **Remote Authentication Dial-In User Service (RADIUS)**
  eases switch security access administration by using a password authentication server
- **Terminal Access Controller Access-Control System (TACACS+)**
  delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security
- **Switch management logon security**
  helps secure switch CLI logon by optionally requiring either RADIUS or TACACS+ authentication
- **Secure shell (SSHv2)**
  uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers
- **DHCP snooping**
  enables DHCP clients to receive IP addresses from authorized DHCP servers and maintains a list of DHCP entries for trusted ports; prevents users from receiving fake IP addresses and reduces ARP attacks, improving security
- **IP source guard**
  filters packets on a per-port basis to prevent illegal packets from being forwarded
- **ARP attack protection**
  protects from attacks using a large number of ARP requests with a host-specific, user-selectable threshold
- **Port security**
  allows access only to specified MAC addresses, which can be learned or specified by the administrator
- **IEEE 802.1X support**
  provides port-based user authentication with support for Extensible Authentication Protocol (EAP) MD5, TLS, TTLS, and PEAP with choice of AES, TKIP, and static or dynamic WEP encryption for protecting wireless traffic between authenticated clients and the access point
- **Media access control (MAC) authentication**
  provides simple authentication based on a user's MAC address; supports local or RADIUS-based authentication
- **Multiple user authentication methods**
  - **IEEE 802.1X**
    uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
  - **Web-based authentication**
    provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support the IEEE 802.1X supplicant
  - **MAC-based authentication**
    authenticates the client with the RADIUS server based on the client's MAC address
- **DHCP protection**
  blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- **Endpoint Admission Defense (EAD)**
  provides security policies to users accessing a network
- **Port isolation**
  secures and adds privacy, and prevents malicious attackers from obtaining user information
- **IEEE 802.1AE MACsec**
  provides switch-to-host with IEEE 802.1X or switch-to-switch hardware encryption, and authentication. Requires Comware

Overview

v7 with specific hardware only. Refer to the hardware manuals for details.

Convergence

- **LLDP-MED (Media Endpoint Discovery)**
  defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- **Multicast Source Discovery Protocol (MSDP)**
  allows multiple PIM-SM domains to interoperate; is used for inter-domain multicast applications
- **Internet Group Management Protocol (IGMP)**
  utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3
- **Protocol Independent Multicast (PIM)**
  defines modes of Internet IPv4 and IPv6 multicasting to allow one-to-many and many-to-many transmission of information; supports PIM Dense Mode (DM), Sparse Mode (SM), and Source-Specific Multicast(SSM)
- **Multicast Border Gateway Protocol (MBGP)**
  allows multicast traffic to be forwarded across BGP networks and kept separate from unicast traffic
- **Multicast Listener Discovery (MLD) protocol**
  establishes, maintains, and manages IPv6 multicast groups and networks; supports v1 and v2 and utilizes Any-Source Multicast (ASM) or Source-Specific Multicast (SSM)
- **Multicast VLAN**
  allows multiple VLANs to receive the same IPv4 or IPv6 multicast traffic, lessening network bandwidth demand by reducing or eliminating multiple streams to each VLAN
- **Voice VLAN**
  automatically assigns VLAN and priority for IP phones, simplifying network configuration and maintenance

Integration

- **Open Application Architecture (OAA)**
  provides high-performance application-specific modules fully integrated with the switching architecture; uses the chassis high-speed backplane to access network-related data; increases performance, reduces costs, and simplifies network management
- **VPN 20 Gb/s firewall module**
  Provides enhanced stateful packet inspection and filtering; supports flexible security zones and virtual firewall containment; offers advanced VPN services with 3DES and AES encryption at high performance and low latency; facilitates Web content filtering; and enables application prioritization and optimization

Software-defined networking

- **OpenFlow 1.3**
  enables SDN to provide an end-to-end solution to automate the network, allowing for rapid application deployments (Comware v7 only)

Additional information

- **Green initiative support**
  provides support for RoHS and WEEE regulations
- **Low power-consumption switch**
  Is rated among the switches with the lowest power consumption in the industry by Miercom independent tests
- **Unified Hewlett Packard Enterprise Comware operating system with modular architecture**

Overview

provides an easy-to-enhance-and-extend feature set, which doesn't require whole-scale changes; all switching, routing, and security platforms leverage the Comware OS, a common unified modular operating system

- **OPEX savings**
  simplifies and streamlines deployment, management, and training through the use of a common operating system, thereby cutting costs as well as reducing the risk of human errors associated with having to manage multiple operating systems across different platforms and network layers

Warranty and support

- **1-year warranty**
  See **http://www.hpe.com/networking/warrantysummary** for warranty and support information included with your product purchase.
- **Software releases**
  to find software for your product, refer to **http://www.hpe.com/networking/support**; for details on the software releases available with your product purchase, refer to **http://www.hpe.com/networking/warrantysummary**

Configuration

Build To Order: BTO is a standalone unit with no integration. BTO products ship standalone are not part of a CTO or Rack-Shippable solution.

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle — JH331A

- Must select min 1 Power Supply
- 2 - JH209A included
- min=0 \ max=8 SFP/SFP + Transceivers
- Min=0 \ Max = 2 QSFP Transceiver
- 10U - Height

See Configuration
NOTE:1, 2, 3

HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle — JH332A

- Must select min 1 Power Supply
- 2 - JH209A included
- min=0 \ max=8 SFP/SFP + Transceivers
- Min=0 \ Max = 2 QSFP Transceiver
- 13U - Height

See Configuration
NOTE:1, 2, 3

HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle — JH333A

- Must select min 1 Power Supply
- 2 - JH209A included
- min=0 \ max=8 SFP or SFP + Transceivers
- Min=0 \ Max = 2 QSFP Transceiver
- 16U - Height

See Configuration
NOTE:1, 2, 3

HPE FlexNetwork 7502 Switch Chassis — JD242C

- Must select min 1 Power Supply
- Must select Min 1 Fabric Module
- 4U - Height

HPE FlexNetwork 7503 Switch Chassis — JD240C

- Must select min 1 Power Supply
- Must select Min 1 Fabric Module
- 4U - Height

HPE FlexNetwork 7506 Switch Chassis — JD239C

- Must select min 1 Power Supply
- Must select Min 1 Fabric Module
- 13U - Height

HPE FlexNetwork 7510 Switch Chassis — JD238C

- Must select min 1 Power Supply
- Must select Min 1 Fabric Module
- 16U - Height

Configuration Rules:

Configuration

Note 1	The following Transceivers install into this Module: (Use BTO only when adding to switch)	
	HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
	HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
	HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
	HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
	HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
	HPE X120 1G SFP LC LH100 Transceiver	JD103A
	HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
	HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
	HPE X125 1G SFP LC LH70 Transceiver	JD063B
	HPE X120 1G SFP RJ45 T Transceiver	JD089B
	HPE X120 1G SFP LC SX Transceiver	JD118B
	HPE X120 1G SFP LC LX Transceiver	JD119B
	HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
	HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
	HPE X110 100M SFP LC LH40 Transceiver	JD090A
	HPE X110 100M SFP LC LH80 Transceiver	JD091A
	HPE X115 100M SFP LC FX Transceiver	JD102B
	HPE X110 100M SFP LC LX Transceiver	JD120B
	HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
	HPE X115 100M SFP LC BX 10-D Transceiver	JD101A
Note 2	The following 40G Transceivers install into this Module: (Use BTO only when adding to switch)	
	HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver	JG661A
	HPE X140 40G QSFP+ MPO SR4 Transceiver	JG325B
	HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver	JG709A
	HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver	JL251A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable	JG326A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable	JG327A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable	JG328A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable	JG329A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable	JG330A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable	JG331A
Note 3	The following Transceivers install into this Module: (Use BTO only when adding to switch)	
	HPE X130 10G SFP+ LC SR Transceiver	JD092B
	HPE X130 10G SFP+ LC LRM Transceiver	JD093B
	HPE X130 10G SFP+ LC LR Transceiver	JD094B
	HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	JD095C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable	JD096C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable	JD097C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable	JG081C
	HPE FlexNetwork X240 10G SFP+ SFP+ 7m Direct Attach Copper Cable	JC784C

Configuration

Remarks: BTO Model 1s should never receive an 0D1 and therefore cannot be factory integrated into a rack.

Box Level Integration CTO Models

CTO Solution Sku

HPE 75xx Configure-to-order Switch Solution — JG707A
- SSP trigger sku

CTO Base Sku

HPE FlexNetwork 7502 Switch Chassis — JD242C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**2, 3
- 4U - Height

HPE FlexNetwork 7503 Switch Chassis — JD240C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**1, 3, 4
- 10U - Height

HPE FlexNetwork 7506 Switch Chassis — JD239C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**1, 3, 4
- 13U - Height

HPE FlexNetwork 7510 Switch Chassis — JD238C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**3, 4
- 16U - Height

Configuration Rules:

Note 1 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A

Note 2 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7502 300W AC Power Supply	JD226A
HPE FlexNetwork 7500 650W DC Power Supply	JD209A
HPE FlexNetwork 7500 650W AC Power Supply	JD217A

Note 3 If the Switch Chassis is to be Box Level Factory Integrated (CTO), Then the #0D1 is required on the Switch Chassis and integrated to the JG707A - HPE 75xx Configure-to-order Switch Solution. (Min 1/Max 1 Switch per SSP)

Configuration

Note 4 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A

Rack Level Integration CTO Models

HPE FlexNetwork 7502 Switch Chassis — JD242C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**1, 3
- 4U - Height

HPE FlexNetwork 7503 Switch Chassis — JD240C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**2, 3, 4
- 10U - Height

HPE FlexNetwork 7506 Switch Chassis — JD239C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**2, 3, 4
- 13U - Height

HPE FlexNetwork 7510 Switch Chassis — JD238C
- Must select min 1 Power Supply — See Configuration
- Must select Min 1 Fabric Module — **NOTE:**2, 3, 4
- 16U - Height

Configuration Rules:

Note 1 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7502 300W AC Power Supply	JD226A
HPE FlexNetwork 7500 650W DC Power Supply	JD209A
HPE FlexNetwork 7500 650W AC Power Supply	JD217A

Note 2 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A

Note 3 If HPE CTO Switch Chassis is selected to be Rack Level Integration, Then the CTO Switch Chassis needs to integrate (with #0D1) to the BW966A and BW968A HPE Universal Rack Only. (Default to the BW966A.)

Configuration

Note 4 If this Switch Chassis is selected at least one of these Power Supplies is required: (Use #0D1 if switch is CTO)

HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A

Modules

Fabric Modules

System (std 0 // max 2) User Selection (min 1 // max 2) per enclosure
JH333A JH332A, and JH331A only System (std 2 // max 2) User Selection (min 0 // max 0) per enclosure

HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU — JH209A
- min=0 \ max=8 SFP/SFP + Transceivers — See Configuration
- Min=0 \ Max = 2 QSFP Transceiver — **NOTE:**5, 15, 16, 17, 18

HPE FlexNetwork 7502 Main Processing Unit — JH208A
- No supported Transceivers — See Configuration **NOTE:**14

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit — JH207A
- Min=0 \ Max = 2 QSFP Transceiver — See Configuration **NOTE:**15, 16

HPE FlexNetwork 7500 384Gbps Fabric Module with 2 XFP Ports — JD193B
- min=0 \ max=2 XFP Transceivers — See Configuration **NOTE:**1, 4

HPE FlexNetwork 7500 384Gbps Fabric Module — JD194B
- No supported Transceivers — See Configuration **NOTE:**1

HPE FlexNetwork 7500 384Gbps Fabric Module with 12 SFP Ports — JD224A
- min=0 \ max=12 SFP Transceivers — See Configuration **NOTE:**1, 5

HPE FlexNetwork 7500 384Gbps Advanced Fabric Module — JD195A
- No supported Transceivers — See Configuration **NOTE:**1

HPE FlexNetwork 7500 768Gbps Fabric Module — JD220A
- No supported Transceivers — See Configuration **NOTE:**11

Configuration

Configuration Rules:

Note 1	These Modules install to the following switches: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7506 Switch Chassis	JD239C
	HPE FlexNetwork 7503 Switch Chassis	JD240C
Note 4	The following Transceivers install into this Module: (Use #0D1 if switch is CTO)	
	HPE X135 10G XFP LC ER Transceiver	JD121A
	HPE X130 10G XFP LC LR Single Mode 10km 1310nm Transceiver	JD108B
	HPE X130 10G XFP LC SR Transceiver	JD117B
	HPE X130 10G XFP LC ZR Single Mode 80km 1550nm Transceiver	JD107A
	HPE X180 10G XFP LC LH 80km 1538.98nm DWDM Transceiver	JG226A
	HPE X180 10G XFP LC LH 80km 1539.77nm DWDM Transceiver	JG227A
	HP X180 10G XFP LC LH 80km 1540.56nm DWDM Transceiver	JG228A
	HP X180 10G XFP LC LH 80km 1542.14nm DWDM Transceiver	JG229A
	HPE X180 10G XFP LC LH 80km 1542.94nm DWDM Transceiver	JG230A
	HP X180 10G XFP LC LH 80km 1558.98nm DWDM Transceiver	JG231A
	HP X180 10G XFP LC LH 80km 1559.79nm DWDM Transceiver	JG232A
	HP X180 10G XFP LC LH 80km 1560.61nm DWDM Transceiver	JG233A
Note 5	The following Transceivers install into this Module: (Use #0D1 if switch is CTO)	
	HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
	HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
	HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
	HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
	HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
	HPE X120 1G SFP LC LH100 Transceiver	JD103A
	HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
	HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
	HPE X125 1G SFP LC LH70 Transceiver	JD063B
	HPE X120 1G SFP RJ45 T Transceiver	JD089B
	HPE X120 1G SFP LC SX Transceiver	JD118B
	HPE X120 1G SFP LC LX Transceiver	JD119B
	HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
	HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
	HPE X110 100M SFP LC LH40 Transceiver	JD090A
	HPE X110 100M SFP LC LH80 Transceiver	JD091A
	HPE X115 100M SFP LC FX Transceiver	JD102B
	HPE X110 100M SFP LC LX Transceiver	JD120B
	HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
	HPE X115 100M SFP LC BX 10-D Transceiver	JD101A
Note 11	These Modules install to the following switches only: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7510 Switch Chassis	JD238C

Note 12 If 2 Fabric Modules are selected they must be the same Sku number.

Configuration

Note 13	The following PoE DIMM installs into this Module: (Use #0D1 if switch is CTO)	
Note 14	These Modules install to the following switches: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7502 Switch Chassis	JD242C
Note 15	These Modules install to the following switches only: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7503 Switch Chassis	JD240C
	HPE FlexNetwork 7506 Switch Chassis	JD239C
	HPE FlexNetwork 7510 Switch Chassis	JD238C
Note 16	The following 40G Transceivers install into this Module: (Use #0D1 or #B01 if switch is CTO)	
	HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver	JG661A
	HPE X140 40G QSFP+ MPO SR4 Transceiver	JG325B
	HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver	JG709A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable	JG326A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable	JG327A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable	JG328A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable	JG329A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable	JG330A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable	JG331A
Note 17	The following Transceivers install into this Module: (Use #0D1 or #B01 if switch is CTO)	
	HPE X130 10G SFP+ LC SR Transceiver	JD092B
	HPE X130 10G SFP+ LC LRM Transceiver	JD093B
	HPE X130 10G SFP+ LC LR Transceiver	JD094B
	HPE X130 10G SFP+ LC ER 40km Transceiver	JG234A
	HPE X130 10G SFP+ LC LH 80km Transceiver	JG915A
	HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	JD095C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable	JD096C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable	JD097C
	HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable	JG081C
	HPE FlexNetwork X240 10G SFP+ SFP+ 7m Direct Attach Copper Cable	JC784C
Note 18	The following LC Transceivers install into this Module: (Use #0D1 or #B01 if switch is CTO)	
	HPE X130 10G SFP+ LC LH80 tunable Transceiver	JL250A
	HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver	JL251A

Remark: For Switch A7503,A7506 and A7506-V, these modules can only be inserted into the Slot 0 and Slot 1. And for Switch A7510, this module can only be inserted into the Slot 5 and Slot 6.

For Switch A7503-S, this module can only be inserted into the Slot 0.

Ethernet Modules

Configuration

(Switch JD242C) System (std 0 // max 2) User Selection (min 0 // max 2) per enclosure
(Switch JD240C and JH331A) System (std 0 // max 3) User Selection (min 0 // max 3) per enclosure
(Switch JD239C and JH331A) System (std 0 // max 6) User Selection (min 0 // max 6) per enclosure
(Switch JD238C and JH331A) System (std 0 // max 10) User Selection (min 0 // max 10) per enclosure

HPE FlexNetwork 7500 24-port GbE SFP SC Module • min=0 \ max=24 SFP Transceivers	JD203B See Configuration **NOTE:**1, 18, 19
HPE FlexNetwork 7500 12-port GbE SFP SC Module • min=0 \ max=12 SFP Transceivers	JD207A See Configuration **NOTE:**1, 18, 19
HPE FlexNetwork 7500 48-port GbE SFP Enhanced Module • min=0 \ max=48 SFP Transceivers	JD221A See Configuration **NOTE:**1, 16, 19, 20
HPE FlexNetwork 7500 40-port Gig-T/8-port SFP PoE-upgradable SC Module • min=0 \ max= 8 SFP Transceivers	JD228B See Configuration **NOTE:** 1, 8, 14, 17, 18, 19
HPE FlexNetwork 7500 24-port GbE SFP Enhanced Module • min=0 \ max=24 SFP Transceivers	JD231A See Configuration **NOTE:** 1, 16, 19, 20
HPE FlexNetwork 7500 24-port GbE SFP with 8 Combo SD Module • 16 SFP 100/1000 Mbps ports • 8 dual-personality ports - 1000M Combo ports (SFP or RJ-45) • min=0 \ max=24 SFP Transceivers	JD234A See Configuration **NOTE:** 1, 16, 19, 20
HPE FlexNetwork 7500 48-port GbE SFP SD Module • min=0 \ max=48 SFP Transceivers	JD237A See Configuration **NOTE:** 1, 16, 19, 20
HPE FlexNetwork 7500 48-port GbE SFP SC Module • min=0 \ max=48 SFP Transceivers	JD211B See Configuration **NOTE:** 1, 18, 19
HPE FlexNetwork 7500 20-port Gig-T/4-port GbE Combo PoE-upgradable SC Module • min=0 \ max= 4 SFP Transceivers	JC669A See Configuration **NOTE:** 1, 12, 17, 18, 19
HPE FlexNetwork 7500 8-port 10G SFP+ SC Module • min=0 \ max=8 per SFP+ Transceivers	JF290A See Configuration

Configuration

	NOTE: 3, 16, 19, 20
HPE FlexNetwork 7500 4-port 10GbE XFP Enhanced Module • min=0 \ max=4 XFP	JD232A See Configuration **NOTE:** 4, 16, 19, 20
HPE FlexNetwork 7500 2-port 10GbE XFP Enhanced Module • min=0 \ max=2 XFP	JD233A See Configuration **NOTE:** 4, 16, 19, 20
HP FlexNetwork 7500 8-port 10GbE XFP SD Module • min=0 \ max=8 XFP Transceivers	JD191A See Configuration **NOTE:** 4, 16, 19, 20
HPE FlexNetwork 7500 2-port 10GbE XFP SC Module • min=0 \ max=2 XFP Transceivers	JD201A See Configuration **NOTE:** 4, 18, 19
HPE FlexNetwork 7500 24-port Gig-T/2-port 10GbE XFP SC Module • min=0 \ max=2 XFP Transceivers	JD206A See Configuration **NOTE:** 4, 18, 19
HPE FlexNetwork 7500 4-port 10GbE XFP SD Module • min=0 \ max=4 XFP Transceivers	JD235A See Configuration **NOTE:**4, 16, 19, 20
HPE FlexNetwork 7500 2-port 10GbE XFP SD Module • min=0 \ max=2 XFP Transceivers	JD236A See Configuration **NOTE:** 4, 16, 19, 20
HPE FlexNetwork 7500 24-port GbE SFP/2-port 10GbE XFP Module • min=0 \ max=2 XFP min=0 \ max=24 SFP Transceivers	JD205A See Configuration **NOTE:** 5, 18, 19
HPE FlexNetwork 7500 24-port GbE SFP with 8 Combo and 2-port 10GbE XFP SD Module • 16 SFP 100/1000 Mbps ports • 8 dual-personality ports - 1000M Combo ports (SFP or RJ-45) • 2 XFP 10GbE ports • min=0 \ max=2 XFP min=0 \ max=24 SFP Transceivers	JD230A See Configuration **NOTE:** 4, 5, 16, 19, 20
HPE FlexNetwork 7500 24-port Gig-T SC Module • No supported Transceivers	JD204B See Configuration **NOTE:** 18, 19
HPE FlexNetwork 7500 48-port Gig-T PoE-ready SC Module • No supported Transceivers	JD210A See Configuration **NOTE:** 8, 14, 18, 19

Configuration

HPE FlexNetwork 7500 48-port Gig-T PoE+ SD Module • Includes DIMM	JD229B See Configuration **NOTE:** 16, 17, 19, 20
HPE FlexNetwork 7500 48-port 1000BASE-T PoE+ SC Module • No supported Transceivers	JG663A See Configuration **NOTE:** 16, 17, 19, 20
HPE FlexNetwork 7500 Load Balancing Module • No supported Transceivers	JD252A See Configuration **NOTE:** 18, 19
HP 10500/7500 NetStream Monitoring Module • No supported Transceivers	JD254A See Configuration **NOTE:** 18, 19
HP 7500 48-port Gig-T PoE-ready Module • No supported Transceivers	JD199B See Configuration **NOTE:** 7, 8, 14, 17, 18, 19
HPE 10500/11900/7500 20Gbps VPN Firewall Module • min=0 \ max=2 SFP Transceivers	JG372A See Configuration **NOTE:** 13, 16, 19
HPE FlexNetwork 7500 4-port 40GbE QSFP+ SC Module • min=0 \ max=4 QSFP+ Transceivers	JC792A See Configuration **NOTE:**10, 16, 19
HP 7500 4-port 40GbE CFP SC Module • min=0 \ max=4 CFP Transceivers	JG373A See Configuration **NOTE:** 11, 18, 19
HP 10500/7500 20G Unified Wired-WLAN Module	JG639A See Configuration **NOTE:** 15, 16, 19
HPE FlexNetwork 7500 44-port SFP/4-port SFP+ SE Module • min=0 \ max=48 SFP Transceivers or • min=0 \ max=4 SFP+ Transceivers or • min=0 \ max=48 JD102B	JH210A See Configuration **NOTE:**1, 3, 16, 20
HPE FlexNetwork 7500 24-port SFP/4-port SFP+ SE Module • min=0 \ max=24 SFP Transceivers or • min=0 \ max=4 SFP+ Transceivers or • min=0 \ max=28 JD102B	JH211A See Configuration **NOTE:**1, 3, 16, 20

Configuration

HPE FlexNetwork 7500 48-port 1000BASE-T SE Module • No supported Transceivers	JH212A See Configuration **NOTE:**16, 20
HPE FlexNetwork 7500 48-port 1000BASE-T with PoE+ SE Module • No supported Transceivers	JH213A See Configuration **NOTE:**16, 17, 20
HPE FlexNetwork 7500 16-port 1/10GbE SFP+ SF Module • min=0 \ max=16 SFP Transceivers or • min=0 \ max=16 SFP+ Transceivers or	JH214A See Configuration **NOTE:**1, 3, 16, 20
HPE FlexNetwork 7500 12-port 1/10GbE SFP+ EC Module • min=0 \ max=12 SFP Transceivers or • min=0 \ max=12 SFP+ Transceivers or	JH309A See Configuration **NOTE:**1, 3, 16, 20

Configuration Rules:

Note 1 **The following Transceivers install into this Module: (Use #0D1 if switch is CTO)**

HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
HPE X120 1G SFP LC LH100 Transceiver	JD103A
HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
HPE X125 1G SFP LC LH70 Transceiver	JD063B
HPE X120 1G SFP RJ45 T Transceiver	JD089B
HPE X120 1G SFP LC SX Transceiver	JD118B
HPE X120 1G SFP LC LX Transceiver	JD119B
HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
HPE X110 100M SFP LC LH40 Transceiver	JD090A
HPE X110 100M SFP LC LH80 Transceiver	JD091A
HPE X115 100M SFP LC FX Transceiver	JD102B
HPE X110 100M SFP LC LX Transceiver	JD120B
HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
HPE X115 100M SFP LC BX 10-D Transceiver	JD101A

Note 2 **The following Transceivers install into this Module: (Use #0D1 if switch is CTO)**

HPE X110 100M SFP LC LH40 Transceiver	JD090A
HPE X110 100M SFP LC LH80 Transceiver	JD091A
HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
HPE X115 100M SFP LC BX 10-D Transceiver	JD101A

Configuration

HPE X115 100M SFP LC FX Transceiver	JD102B
HPE X110 100M SFP LC LX Transceiver	JD120B

Note 3 The following Transceivers install into this Module: (Use #0D1 or #B01 if switch is CTO)

HPE X130 10G SFP+ LC SR Transceiver	JD092B
HPE X130 10G SFP+ LC LRM Transceiver	JD093B
HPE X130 10G SFP+ LC LR Transceiver	JD094B
HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	JD095C
HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable	JD096C
HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable	JD097C
HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable	JG081C
HPE FlexNetwork X240 10G SFP+ SFP+ 7m Direct Attach Copper Cable	JC784C

Note 4 The following Transceivers install into this Module: (Use #0D1 if switch is CTO)

HPE X135 10G XFP LC ER Transceiver	JD121A
HPE X130 10G XFP LC LR Single Mode 10km 1310nm Transceiver	JD108B
HPE X130 10G XFP LC SR Transceiver	JD117B
HPE X130 10G XFP LC ZR Single Mode 80km 1550nm Transceiver	JD107A
HPE X180 10G XFP LC LH 80km 1538.98nm DWDM Transceiver	JG226A
HPE X180 10G XFP LC LH 80km 1539.77nm DWDM Transceiver	JG227A
HP X180 10G XFP LC LH 80km 1540.56nm DWDM Transceiver	JG228A
HP X180 10G XFP LC LH 80km 1542.14nm DWDM Transceiver	JG229A
HPE X180 10G XFP LC LH 80km 1542.94nm DWDM Transceiver	JG230A
HP X180 10G XFP LC LH 80km 1558.98nm DWDM Transceiver	JG231A
HP X180 10G XFP LC LH 80km 1559.79nm DWDM Transceiver	JG232A
HP X180 10G XFP LC LH 80km 1560.61nm DWDM Transceiver	JG233A

Note 5 The following Transceivers install into this Module: (Use #0D1 if switch is CTO)

HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
HPE X120 1G SFP LC LH100 Transceiver	JD103A
HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
HPE X125 1G SFP LC LH70 Transceiver	JD063B
HPE X120 1G SFP RJ45 T Transceiver	JD089B
HPE X120 1G SFP LC SX Transceiver	JD118B
HPE X120 1G SFP LC LX Transceiver	JD119B
HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
HPE X110 100M SFP LC LH40 Transceiver	JD090A
HPE X110 100M SFP LC LH80 Transceiver	JD091A
HPE X115 100M SFP LC FX Transceiver	JD102B
HPE X110 100M SFP LC LX Transceiver	JD120B

Configuration

	HPE X135 10G XFP LC ER Transceiver	JD121A
	HPE X130 10G XFP LC LR Single Mode 10km 1310nm Transceiver	JD108B
	HPE X130 10G XFP LC SR Transceiver	JD117B
	HPE X130 10G XFP LC ZR Single Mode 80km 1550nm Transceiver	JD107A
Note 6	The following Transceivers install into this Module: (Use #0D1 if switch is CTO)	
	HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
	HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
	HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
	HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
	HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
	HPE X120 1G SFP LC LH100 Transceiver	JD103A
	HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
	HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
	HPE X125 1G SFP LC LH70 Transceiver	JD063B
	HPE X120 1G SFP RJ45 T Transceiver	JD089B
	HPE X120 1G SFP LC SX Transceiver	JD118B
	HPE X120 1G SFP LC LX Transceiver	JD119B
	HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
	HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
	HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
	HPE X115 100M SFP LC BX 10-D Transceiver	JD101A
Note 7	This Module is not supported on the JD242x at this time.	
Note 8	The following DIMMs install into this Module: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7500 PoE DIMM Memory Module	JD192B
Note 10	The following 40G Transceivers install into this Module: (Use #0D1 or #B01 if switch is CTO)	
	HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver	JG661A
	HPE X140 40G QSFP+ MPO SR4 Transceiver	JG325B
	HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver	JG709A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable	JG326A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable	JG327A
	HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable	JG328A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable	JG329A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable	JG330A
	HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable	JG331A
Note 11	The following CFP Transceivers install into this Module:	
	HPE X140 40G CFP LC LR4 10km SM Transceiver	JC857A
Note 13	The following Transceivers install into this Module: (Use #0D1 if switch is CTO)	
	HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
	HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A

Configuration

	HPE X125 1G SFP LC LH70 Transceiver	JD063B
	HPE X120 1G SFP LC SX Transceiver	JD118B
	HPE X120 1G SFP LC LX Transceiver	JD119B
Note 14	The following PoE DIMM installs into this Module: (Use #0D1 if switch is CTO)	
	HPE FlexNetwork 7500 PoE DIMM Memory Module	JD192B
Note 16	Selecting this module requires one of the following:	
	HPE FlexNetwork 7503 Switch Chassis	JD240C
	HPE FlexNetwork 7506 Switch Chassis	JD239C
	HPE FlexNetwork 7510 Switch Chassis	JD238C
	HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
	HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
	HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
Note 17	If JD242C and JH208a is selected, Then this Module is not allowed.	
Note 18	This Module is not supported with the following MPU's:	
	HPE FlexNetwork 7502 Main Processing Unit	JH208A
	HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
	HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
Note 19	If this module is selected, then the following Comware V5 MPU's are compatible:	
	HPE FlexNetwork 7500 384Gbps Fabric Module with 2 XFP Ports	JD193B
	HPE FlexNetwork 7500 384Gbps TAA-compliant Fabric/MPU with 2 10GbE XFP Ports	JC699A
	HPE FlexNetwork 7500 384Gbps Fabric Module	JD194B
	HPE FlexNetwork 7500 384Gbps Fabric Module with 12 SFP Ports	JD224A
	HPE FlexNetwork 7500 384Gbps Advanced Fabric Module	JD195A
	HPE FlexNetwork 7500 384Gbps TAA-compliant Fabric/Main Processing Unit	JC700A
	HPE FlexNetwork 7500 768Gbps Fabric Module	JD220A
	HPE FlexNetwork 7500 768Gbps TAA-compliant Fabric/Main Processing Unit	JC701A
Note 20	If this module is selected, then the following Comware V7 MPU's are compatible:	
	HPE FlexNetwork 7502 Main Processing Unit	JH208A
	HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
	HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
Remark:	JG639A and JG645A - Additional AP licenses available below in the 'Switch Enclosure Options' category.	

7500 PoE Module

System (std 0 // max 1) User Selection (min 0 // max 1) per Ethernet or Fabric Module

Configuration

HPE FlexNetwork 7500 PoE DIMM Memory Module	JD192B See Configuration **NOTE:**1, 3, 6

Configuration Rules:

Note 1 The JD192B is optional when you have selected the JD199B, JD198B, JD210A, JC709A, JC710A or JD228B modules.

Note 3 If 1 or more of the JD192B (PoE DIMM Module) is ordered than the customer must also order 2 of JD208A, JD218A, JD219A, or JD227A in order to support PoE. (Except for JD242x see rule 6)

Note 6 This Module is supported on the JD242x only when an External DC Power Source is connected to the rear terminals. (See Installation Guide)

Transceivers

SFP+ Transceivers

HPE X130 10G SFP+ LC SR Transceiver	JD092B
HPE X130 10G SFP+ LC LRM Transceiver	JD093B
HPE X130 10G SFP+ LC LR Transceiver	JD094B
HPE X130 10G SFP+ LC ER 40km Transceiver	JG234A
HPE X130 10G SFP+ LC LH 80km Transceiver	JG915A
HPE X130 10G SFP+ LC LH80 tunable Transceiver	JL250A
HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	JD095C
HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable	JD096C
HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable	JD097C
HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable	JG081C
HPE FlexNetwork X240 10G SFP+ SFP+ 7m Direct Attach Copper Cable	JC784C

SFP Transceivers

HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
HPE X170 1G SFP LC LH70 1570 Transceiver	JD110A
HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
HPE X120 1G SFP LC LH100 Transceiver	JD103A
HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
HPE X120 1G SFP RJ45 T Transceiver	JD089B
HPE X120 1G SFP LC SX Transceiver	JD118B
HPE X120 1G SFP LC LX Transceiver	JD119B

Configuration

HPE X125 1G SFP LC LH70 Transceiver	JD063B
HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
HPE X110 100M SFP LC LH40 Transceiver	JD090A
HPE X110 100M SFP LC LH80 Transceiver	JD091A
HPE X115 100M SFP LC FX Transceiver	JD102B
HPE X110 100M SFP LC LX Transceiver	JD120B
HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
HPE X115 100M SFP LC BX 10-D Transceiver	JD101A

XFP Transceivers

HPE X135 10G XFP LC ER Transceiver	JD121A
HPE X130 10G XFP LC ZR Single Mode 80km 1550nm Transceiver	JD107A
HPE X130 10G XFP LC SR Transceiver	JD117B
HPE X130 10G XFP LC LR Single Mode 10km 1310nm Transceiver	JD108B
HPE X180 10G XFP LC LH 80km 1538.98nm DWDM Transceiver	JG226A
HPE X180 10G XFP LC LH 80km 1539.77nm DWDM Transceiver	JG227A
HP X180 10G XFP LC LH 80km 1540.56nm DWDM Transceiver	JG228A
HP X180 10G XFP LC LH 80km 1542.14nm DWDM Transceiver	JG229A
HPE X180 10G XFP LC LH 80km 1542.94nm DWDM Transceiver	JG230A
HP X180 10G XFP LC LH 80km 1558.98nm DWDM Transceiver	JG231A
HP X180 10G XFP LC LH 80km 1559.79nm DWDM Transceiver	JG232A
HP X180 10G XFP LC LH 80km 1560.61nm DWDM Transceiver	JG233A

QSFP+ Transceivers

HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver	JG661A
HPE X140 40G QSFP+ MPO SR4 Transceiver	JG325B
HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver	JG709A
HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver	JL251A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable	JG326A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable	JG327A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable	JG328A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable	JG329A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable	JG330A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable	JG331A

CFP Transceivers

HPE X140 40G CFP LC LR4 10km SM Transceiver	JC857A

Internal Power Supplies

System (std 0 // max 2) User Selection (min 1 // max 2)

Configuration

HPE FlexNetwork 7502 300W AC Power Supply • includes 1 x c13, 300w	JD226A See Configuration **NOTE:**1, 4
PDU Cable NA/MEX/TW/JP • C15 PDU Jumper Cord (NA/MEX/TW/JP)	JD226A#B2B
PDU Cable ROW • C15 PDU Jumper Cord (ROW)	JD226A#B2C
HPE FlexNetwork 7500 650W DC Power Supply	JD209A See Configuration **NOTE:**1
HPE FlexNetwork 7500 650W AC Power Supply • includes 1 x c13, 650w	JD217A See Configuration **NOTE:**1, 4
PDU Cable NA/MEX/TW/JP • C15 PDU Jumper Cord (NA/MEX/TW/JP)	JD217A#B2B
PDU Cable ROW • C15 PDU Jumper Cord (ROW)	JD217A#B2C
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A See Configuration **NOTE:**2
HPE FlexNetwork 7500 1400W AC Power Supply • includes 1 x c19, 1400w	JD218A See Configuration **NOTE:**2, 4
PDU Cable NA/MEX/TW/JP • C19 PDU Jumper Cord (NA/MEX/TW/JP)	JD218A#B2B
PDU Cable ROW • C19 PDU Jumper Cord (ROW)	JD218A#B2C
High Volt Switch to Wall Power Cord • NEMA L6-20P Cord (NA/MEX/JP/TW)	JD218A#B2E
HPE FlexNetwork 7500 2800W AC Power Supply • includes 2 x c19, 2800w	JD219A See Configuration **NOTE:**2, 4
PDU Cable NA/MEX/TW/JP	JD219A#B2B

Configuration

- C19 PDU Jumper Cord (NA/MEX/TW/JP)

PDU Cable ROW JD219A#B2C
- C19 PDU Jumper Cord (ROW)

High Volt Switch to Wall Power Cord JD219A#B2E
- NEMA L6-20P Cord (NA/MEX/JP/TW)

HPE FlexNetwork 7500 6000W AC Power Supply JD227A
- includes 4 x c19, 6000w

See Configuration
NOTE:2, 4

PDU Cable NA/MEX/TW/JP JD227A#B2B
- C19 PDU Jumper Cord (NA/MEX/TW/JP)

PDU Cable ROW JD227A#B2C
- C19 PDU Jumper Cord (ROW)

High Volt Switch to Wall Power Cord JD227A#B2E
- NEMA L6-20P Cord (NA/MEX/JP/TW)

HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit JH215A
- includes 4 x c19, 6000w

See Configuration
NOTE:4, 5

PDU Cable NA/MEX/TW/JP JH215A#B2B
- C19 PDU Jumper Cord (NA/MEX/TW/JP)

PDU Cable ROW JH215A#B2C
- C19 PDU Jumper Cord (ROW)

High Volt Switch to Wall Power Cord JH215A#B2E
- NEMA L6-20P Cord (NA/MEX/JP/TW)

Configuration Rules:

Note 1 **Only supported on the JD242x .**

Note 2 **Only supported on the following:**

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
HPE FlexNetwork 7503 Switch Chassis	JD240C
HPE FlexNetwork 7506 Switch Chassis	JD239C
HPE FlexNetwork 7510 Switch Chassis	JD238C

Configuration

Note 3 If 2 power supplies are selected they must be the same Sku number.

Note 4 Localization (Wall Power Cord) required on orders without #B2B, #B2C (PDU Power Cord) or #B2E. (See Localization Menu)
REMARK: When Switches/Routers are Factory Racked, Then #B2B, #B2C should be the Defaulted Power Cable option on the Switches/Routers.

Note 5 Only supported on the following:

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
HPE FlexNetwork 7503 Switch Chassis	JD240C
HPE FlexNetwork 7506 Switch Chassis	JD239C

Remarks: Drop down under power supply should offer the following options and results:
Switch to PDU Power Cord - #B2B in North America, Mexico, Taiwan, and Japan or #B2C ROW. (Watson Default B2B or B2C for Rack Level CTO)
Switch to Wall Power Cord - Localized Option (Watson Default for BTO and Box Level CTO)
High Volt Power Electrical Module to Wall Power Cord - #B2E Option. (Offered only in North America, Mexico, Taiwan, and Japan)

Switch Enclosure Options

Software Licenses

HP Unified Wired-WLAN 128 AP E-LTU JG649AAE
(min 0 // max 7) See Configuration
REMARK: This license is for use with the Primary Controllers. **NOTE:1**

HP Unified Wired-WLAN 128 AP Redundant E-LTU JG902AAE
(min 0 // max 7) See Configuration
REMARK: This license is for use with the Redundant Controllers. **NOTE:1**

Configuration Rules:

Note 1 Only supported on JG639A and JG645A.

Compact Flash cards

System (std 0 // max 1) User Selection (min 0 // max 1)

HPE X600 1G Compact Flash Card JC684A
See Configuration
NOTE:1

HPE X600 512M Compact Flash Card JC685A
See Configuration

Configuration

NOTE:1

HPE X600 256M Compact Flash Card JC686A

See Configuration

NOTE:1

Configuration Rules:

Note 1 These CF Cards are supported on the following Modules only:

HPE FlexNetwork 7500 384Gbps Fabric Module with 2 XFP Ports	JD193B
HPE FlexNetwork 7500 384Gbps Fabric Module	JD194B
HPE FlexNetwork 7500 768Gbps Fabric Module	JD220A
HPE FlexNetwork 7500 384Gbps Advanced Fabric Module	JD195A
HPE FlexNetwork 7500 384Gbps Fabric Module with 12 SFP Ports	JD224A
HP 7503-S 144Gbps Fabric/MPU with PoE Upgradable 20-port Gig-T/4-port GbE Combo	JC666A
HP 9500 VPN Firewall Module	JD245A

Options for the SSL VPN Service Board Modules (JD253x)

Spare Fan Assembly

HPE FlexNetwork 7502 Spare Fan Assembly JD213A

HPE FlexNetwork 7503 Spare Fan Assembly JD212A

HPE FlexNetwork 7506 Spare Fan Assembly JD214A

HPE FlexNetwork 7510 Spare Fan Assembly JD216A

Remarks: JD213A - This item is only used to replace the fan module of an 7502 . A host is delivered with the fan module.

JD212A - This item is only used to replace the fan module of a 7503. A host is delivered with the fan module.

JD214A - This item is only used to replace the fan module of a 7506. A host is delivered with the fan module.

JD216A - This item is only used to replace the fan module of a 7510. A host is delivered with the fan module.

Opacity Shield Kit

System (std 0 // max 1) User Selection (min 0 // max 1)

HPE FlexNetwork 7510 Opacity Shield Kit JG565A

- Supported on JD238C

See Configuration

NOTE:1, 4

HPE FlexNetwork 7506 Opacity Shield Kit JG566A

Configuration

- Supported on JD239C — See Configuration **NOTE:**1, 3

HPE FlexNetwork 7503 Opacity Shield Kit — JG568A
- Supported on JD240C — See Configuration **NOTE:**1, 2

Configuration Rules:

Note 1 If selected with a CTO Switch Solution, Quantity 1 of JG586A#B01 must also be ordered.

Note 2 Only supported on the following:

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
HPE FlexNetwork 7503 Switch Chassis	JD240C

Note 3 Only supported on the following:

HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
HPE FlexNetwork 7506 Switch Chassis	JD239C

Note 4 Only supported on the following:

HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
HPE FlexNetwork 7510 Switch Chassis	JD238C

Tamper Evidence Labels

HPE 12mm x 60mm Tamper Evidence (100) Labels — JG586A
See Configuration **NOTE:**1, 2

Configuration Rules:

Note 1 If selected with a CTO Switch Solution, Quantity 1 of JG565A#B01, JG566A#B01 or JG568A#B01 must also be ordered.

Note 2 Only supported on the following:

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH331A
HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH332A
HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle	JH333A
HPE FlexNetwork 7503 Switch Chassis	JD240C
HPE FlexNetwork 7506 Switch Chassis	JD239C
HPE FlexNetwork 7510 Switch Chassis	JD238C

Remarks: Each JG565A, JG566A or JG568A would use 1 of JG586A.

Technical Specifications

HPE FlexNetwork 7510 Switch Chassis (JD238C)

Included accessories	1 HP 7510 Spare Fan Assembly (JD216A)	
I/O ports and slots	10 I/O module slots Supports a maximum of 480 Gigabit Ethernet ports or 480 autosensing 10/100/1000 ports or 160 1/10GbE ports or 80 10GbE ports or 40 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD216A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 27.87(h) in (43.6 x 42.0 x 70.8 cm) (16U height)
	Weight	211 lb (95.71 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 53.5 dB, High-speed fan: 56.7 dB
Electrical characteristics	**Frequency**	50/60 Hz
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2

Technical Specifications

	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 460, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: • Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A • Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 1,398 mpps for packet performance and 4,160 Gbps for total switching capacity.	
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office	

HPE FlexNetwork 7506 Switch Chassis (JD239C)

Included accessories	1 HP 7506 Spare Fan Assembly (JD214A)	
I/O ports and slots	6 I/O module slots Supports a maximum of 288 Gigabit Ethernet ports or 288 autosensing 10/100/1000 ports or 96 1/10GbE ports or 48 10GbE ports or 24 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD214A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 22.64(h) in (43.6 x 42.0 x 57.5 cm) (13U height)
	Weight	207 lb (93.9 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM

Technical Specifications

	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 53.6 dB, High-speed fan: 57.7 dB
Electrical characteristics	**Frequency**	50/60 Hz Achieved Miercom Certified Green Award
	Description	The H3C S7506E (HPE 7606) is Certified Green in the 2009 Miercom Green Switches Industry Assessment
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	

Technical Specifications

Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: • Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A JH213A, JH214A, and JH309A • Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 968 mpps for packet performance and 2,880 Gbps for total switching capacity.
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office

HPE FlexNetwork 7503 Switch Chassis (JD240C)

Included accessories	1 HP 7503 Spare Fan Assembly (JD212A)	
I/O ports and slots	3 I/O module slots Supports a maximum of 144 Gigabit Ethernet ports or 144 autosensing 10/100/1000 ports or 48 1/10GbE ports or 24 10GbE ports or 12 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD212A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 17.36(h) in (43.6 x 42.0 x 44.1 cm) (10U height)
	Weight	147 lb (66.68 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 51.6 dB, High-speed fan: 56.1 dB
Electrical characteristics	**Frequency**	50/60 Hz

Technical Specifications

	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: • Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A • Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 645 mpps for packet performance and 1,920 Gbps for total switching capacity.	
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office	

HPE FlexNetwork 7502 Switch Chassis (JD242C)

Technical Specifications

Included accessories	1 HP 7502 Spare Fan Assembly (JD213A)	
I/O ports and slots	2 I/O module slots Supports a maximum of 96 Gigabit Ethernet ports or 96 autosensing 10/100/1000 ports or 32 1/10GbE ports or 16 10GbE ports or 8 40GbE ports, or a combination	
Additional ports and slots	2 MPU (for management modules) slots	
Power supplies	2 power supply slots	
	1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD213A	
	1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 6.89(h) in (43.6 x 42.0 x 17.5 cm) (4U height)
	Weight	59 lb (26.76 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 49.8 dB, High-speed fan: 56.7 dB
Electrical characteristics	**Frequency**	50/60 Hz
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	5/10 A
	Power output	300 W
	Notes	Based on a common power supply of 300 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5

Technical Specifications

	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC – Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). IRF functionality is not supported on the HP 7502 Switch Chassis. Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: • Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A • Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH208A the performance are as follows: up to 213 MPPS for packet performance and 640 Gbps for total switching capacity.	
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office	

HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH333A)

Included accessories	1 HP 7510 Spare Fan Assembly (JD216A) 2 HP 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ Main Processing Unit (JH209A)	
I/O ports and slots	10 I/O module slots Supports a maximum of 480 Gigabit Ethernet ports or 480 autosensing 10/100/1000 ports or 160 1/10GbE ports or 80 10GbE ports or 40 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD216A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 27.87(h) in (43.6 x 42.0 x 70.8 cm) (16U height)
	Weight	211 lb (95.71 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM

Technical Specifications

		MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 53.5 dB, High-speed fan: 56.7 dB
Electrical characteristics	**Frequency**	50/60 Hz
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN	

Technical Specifications

	Firewall Module (JG372A). • Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: • Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A • Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 1,398 mpps for packet performance and 4,160 Gbps for total switching capacity.
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office

HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH332A)

Included accessories	1 HP 7506 Spare Fan Assembly (JD214A) 2 HP 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ Main Processing Unit (JH209A)	
I/O ports and slots	6 I/O module slots Supports a maximum of 288 Gigabit Ethernet ports or 288 autosensing 10/100/1000 ports or 96 1/10GbE ports or 48 10GbE ports or 24 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD214A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 22.64(h) in (43.6 x 42.0 x 57.5 cm) (13U height)
	Weight	207 lb (93.9 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 53.6 dB, High-speed fan: 57.7 dB
Electrical characteristics	**Frequency**	50/60 Hz Achieved Miercom Certified Green Award
	Descriptions	The H3C S7506E (HP 7506) is Certified Green in the 2009 Miercom Green

Technical Specifications

		Switches Industry Assessment.
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2
	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: •Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A •Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 968 mpps for packet performance and 2,880 Gbps for total switching capacity.	
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office	

Technical Specifications

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH331A)

Included accessories	1 HP 7503 Spare Fan Assembly (JD212A) 2 HP 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ Main Processing Unit (JH209A)	
I/O ports and slots	3 I/O module slots Supports a maximum of 144 Gigabit Ethernet ports or 144 autosensing 10/100/1000 ports or 48 1/10GbE ports or 24 10GbE ports or 12 40GbE ports, or a combination	
Additional ports and slots	2 switch fabric slots	
Power supplies	2 power supply slots 1 minimum power supply required (ordered separately)	
Fan tray	includes: 1 x JD212A 1 fan tray slot	
Physical characteristics	**Dimensions**	17.17(w) x 16.54(d) x 17.36(h) in (43.6 x 42.0 x 44.1 cm) (10U height)
	Weight	147 lb (66.68 kg) shipping weight
Memory and processor	**Fabric**	MIPS64 @ 600 MHz, 64 MB flash, 512 MB RAM
	I/O Module	MIPS64 @ 400 MHz, 512 MB RAM MIPS64 @ 1000 MHz, 1 GB RAM
Mounting and enclosure	Mounts in an EIA-standard 19 in. rack or other equipment cabinet (hardware included); Horizontal surface mounting only	
Reliability	**Availability**	99.999%
Environment	**Operating temperature**	32°F to 113°F (0°C to 45°C)
	Operating relative humidity	10% to 95%, noncondensing
	Nonoperating/Storage temperature	-40°F to 158°F (-40°C to 70°C)
	Nonoperating/Storage relative humidity	5% to 95%, noncondensing
	Acoustic	Low-speed fan: 51.6 dB, High-speed fan: 56.1 dB
Electrical characteristics	**Frequency**	50/60 Hz
	Voltage	100 - 120 / 200 - 240 VAC, rated -48 to -60 VDC, rated (depending on power supply chosen)
	Current	16/50 A
	Power output	1400 W
	Notes	Based on a common power supply of 1400 W (AC/DC)
Safety	UL 60950-1; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60950-1/A11	
Emissions	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995 +A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A	
Immunity	**Generic**	ETSI EN 300 386 V1.3.3
	EN	EN 61000-4-2:1995+A1:1998+A2:2001
	ESD	EN 61000-4-2

Technical Specifications

	Radiated	EN 61000-4-3
	EFT/Burst	EN 61000-4-4
	Surge	EN 61000-4-5
	Conducted	EN 61000-4-6
	Power frequency magnetic field	IEC 61000-4-8
	Voltage dips and interruptions	EN 61000-4-11
	Harmonics	EN 61000-3-2, IEC 61000-3-2
	Flicker	EN 61000-3-3, IEC 61000-3-3
Management	IMC - Intelligent Management Center; Command-line interface; Web browser; Out-of-band management (serial RS-232c); SNMP manager; Telnet; Terminal interface (serial RS-232c); Modem interface; IEEE 802.3 Ethernet mib; Ethernet interface mib	
Notes	RFCs supported only in Comware v7: 1541, 1542, 1981, 2080, 2460, 2464, 2473, 2474, 2545, 2711, 2863, 2868, 3315, 3413, 3416, 3484, 3575, 3736, 3810, 3956, 4123, 4271, 4291, 4292, 4293, 4443, 4552, 4607, 4659, 4798, 4861, 4862, 5080, 5095, 5340, 5492, 5905 and 6192 For non-TAA environments, IKE/IPSec functionality is provided by the HPE 7500/10500 20Gbps VPN Firewall Module (JG372A). Comware v7 MPUs (JH207A, JH208A and JH209A) only support these LPUs: •Comware v7 LPUs- JH209A, JH210A, JH211A, JH212A, JH213A, JH214A, and JH309A •Comware v5 LPUs- JG663A, JD229B, JD230A, JD234A, JD237A, JD221A, JD231A, JD232A, JD233A, JD191A, JD235A, JD236A, JF290A, and JC792A Performance depends on the MPU/Fabric installed, and when installed with two (2) JH209A the performance are as follows: up to 645 mpps for packet performance and 1,920 Gbps for total switching capacity.	
Services	Refer to the Hewlett Packard Enterprise website at **http://www.hpe.com/networking/services** for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office	

Standards and protocols (applies to all products in series)	**BGP**	**MIBs**
	RFC 1771 BGPv4 RFC 1772 Application of the BGP RFC 1997 BGP Communities Attribute RFC 1998 PPP Gandalf FZA Compression Protocol RFC 2385 BGP Session Protection via TCP MD5 RFC 2439 BGP Route Flap Damping RFC 2796 BGP Route Reflection RFC 2858 BGP-4 Multi-Protocol Extensions RFC 2918 Route Refresh Capability RFC 3065 Autonomous System Confederations for BGP RFC 3392 Capabilities Advertisement with BGP-4 RFC 4271 A Border Gateway Protocol 4 (BGP-4) RFC 4272 BGP Security Vulnerabilities Analysis RFC 4273 Definitions of Managed Objects for BGP-4 RFC 4274 BGP-4 Protocol Analysis	RFC 1156 (TCP/IP MIB) RFC 1157 A Simple Network Management Protocol (SNMP) RFC 1213 MIB II RFC 1215 A Convention for Defining Traps for use with the SNMP RFC 1229 Interface MIB Extensions RFC 1493 Bridge MIB RFC 1573 SNMP MIB II RFC 1643 Ethernet MIB RFC 1657 BGP-4 MIB RFC 1724 RIPv2 MIB RFC 1757 Remote Network Monitoring MIB RFC 1850 OSPFv2 MIB RFC 1907 SNMPv2 MIB RFC 2011 SNMPv2 MIB for IP RFC 2012 SNMPv2 MIB for TCP

Technical Specifications

RFC 4275 BGP-4 MIB Implementation Survey
RFC 4276 BGP-4 Implementation Report
RFC 4277 Experience with the BGP-4 Protocol
RFC 4360 BGP Extended Communities Attribute
RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC 5291 Outbound Route Filtering Capability for BGP-4
RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4

Denial of service protection
RFC 2267 Network Ingress Filtering
RFC 6192: Protecting the Router Control Plane
Automatic filtering of well-known denial-of-service packets
CPU DoS Protection
Rate Limiting by ACLs

Device management
RFC 1157 SNMPv1/v2c
RFC 1305 NTPv3
RFC 1902 (SNMPv2)
RFC 2579 (SMIv2 Text Conventions)
RFC 2580 (SMIv2 Conformance)
RFC 2819 (RMON groups Alarm, Event, History and Statistics only)
Multiple Configuration Files
Multiple Software Images
SSHv1/SSHv2 Secure Shell
TACACS/TACACS+

General protocols
IEEE 802.1ad Q-in-Q
IEEE 802.1ag Service Layer OAM
IEEE 802.1AX-2008 Link Aggregation
IEEE 802.1p Priority
IEEE 802.1Q VLANs
IEEE 802.1s Multiple Spanning Trees
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
IEEE 802.1X PAE
IEEE 802.3ab 1000BASE-T
IEEE 802.3ac (VLAN Tagging Extension)
IEEE 802.3ad Link Aggregation Control Protocol (LACP)
IEEE 802.3ae 10-Gigabit Ethernet
IEEE 802.3af Power over Ethernet
IEEE 802.3ah Ethernet in First Mile over Point to Point Fiber - EFMF
IEEE 802.3at
RFC 2013 SNMPv2 MIB for UDP
RFC 2096 IP Forwarding Table MIB
RFC 2233 Interfaces MIB
RFC 2452 IPV6-TCP-MIB
RFC 2454 IPV6-UDP-MIB
RFC 2465 IPv6 MIB
RFC 2466 ICMPv6 MIB
RFC 2571 SNMP Framework MIB
RFC 2572 SNMP-MPD MIB
RFC 2573 SNMP-Notification MIB
RFC 2573 SNMP-Target MIB
RFC 2578 Structure of Management Information Version 2 (SMIv2)
RFC 2580 Conformance Statements for SMIv2
RFC 2618 RADIUS Client MIB
RFC 2620 RADIUS Accounting MIB
RFC 2665 Ethernet-Like-MIB
RFC 2668 802.3 MAU MIB
RFC 2674 802.1p and IEEE 802.1Q Bridge MIB
RFC 2787 VRRP MIB
RFC 2819 RMON MIB
RFC 2863 The Interfaces Group MIB
RFC 2925 Ping MIB
RFC 2932 IP (Multicast Routing MIB)
RFC 2933 IGMP MIB
RFC 2934 Protocol Independent Multicast MIB for IPv4
RFC 3414 SNMP-User based-SM MIB
RFC 3415 SNMP-View based-ACM MIB
RFC 3417 Simple Network Management Protocol (SNMP) over IEEE 802 Networks
RFC 3418 MIB for SNMPv3
RFC 3595 Textual Conventions for IPv6 Flow Label
RFC 3621 Power Ethernet MIB
RFC 3813 MPLS LSR MIB
RFC 3814 MPLS FTN MIB
RFC 3815 MPLS LDP MIB
RFC 3826 AES for SNMP's USM MIB
RFC 4133 Entity MIB (Version 3)
RFC 4444 Management Information Base for Intermediate System to Intermediate System (IS-IS)

MPLS
RFC 2205 Resource ReSerVation Protocol
RFC 2209 Resource ReSerVation Protocol (RSVP)
RFC 2702 Requirements for Traffic Engineering Over MPLS
RFC 2858 Multiprotocol Extensions for BGP-4
RFC 2961 RSVP Refresh Overhead Reduction Extensions

Technical Specifications

IEEE 802.3ba 40 and 100 Gigabit Ethernet Architecture
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow Control
IEEE 802.3z 1000BASE-X
RFC 768 UDP
RFC 783 TFTP Protocol (revision 2)
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 TELNET
RFC 894 IP over Ethernet
RFC 903 RARP
RFC 906 TFTP Bootstrap
RFC 925 Multi-LAN Address Resolution
RFC 950 Internet Standard Subnetting Procedure
RFC 951 BOOTP
RFC 959 File Transfer Protocol (FTP)
RFC 1027 Proxy ARP
RFC 1035 Domain Implementation and Specification
RFC 1042 IP Datagrams
RFC 1058 RIPv1
RFC 1142 OSI IS-IS Intra-domain Routing Protocol
RFC 1195 OSI ISIS for IP and Dual Environments
RFC 1213 Management Information Base for Network Management of TCP/IP-based internets
RFC 1256 ICMP Router Discovery Protocol (IRDP)
RFC 1293 Inverse Address Resolution Protocol
RFC 1305 NTPv3
RFC 1350 TFTP Protocol (revision 2)
RFC 1393 Traceroute Using an IP Option
RFC 1519 CIDR
RFC 1531 Dynamic Host Configuration Protocol
RFC 1533 DHCP Options and BOOTP Vendor Extensions
RFC 1541 DHCP
RFC 1542 BOOTP
RFC 1591 DNS (client only)
RFC 1624 Incremental Internet Checksum
RFC 1701 Generic Routing Encapsulation
RFC 1721 RIP-2 Analysis
RFC 1723 RIP v2
RFC 1812 IPv4 Routing
RFC 1981 Path MTU Discovery for IP version 6
RFC 2030 Simple Network Time Protocol (SNTP) v4
RFC 2082 RIP-2 MD5 Authentication
RFC 2091 Trigger RIP
RFC 2131 DHCP
RFC 3031 Multiprotocol Label Switching Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3107 Carrying Label Information in BGP-4
RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3212 Constraint-Based LSP Setup using LDP
RFC 3479 Fault Tolerance for the Label Distribution
Protocol (LDP)
RFC 3487 Graceful Restart Mechanism for LDP
RFC 3564 Requirements for Support of Differentiated Service-aware MPLS Traffic Engineering
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 4447 Pseudowire Setup and Maintenance Using LDP
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4664 Framework for Layer 2 Virtual Private Networks
RFC 4665 Service Requirements for Layer 2 Provider Provisioned Virtual Private Networks
RFC 4761 Virtual Private LAN Service (VPLS) Using
BGP for Auto-Discovery and Signaling
RFC 4762 Virtual Private LAN Service (VPLS) Using
Label Distribution Protocol (LDP) Signaling
RFC 5036 LDP Specification

Network management

IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
RFC 1155 Structure of Management Information
RFC 1157 SNMPv1
RFC 1448 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 2211 Controlled-Load Network
RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
RFC 3176 sFlow
RFC 3411 SNMP Management Frameworks
RFC 3412 SNMPv3 Message Processing
RFC 3414 SNMPv3 User-based Security Model (USM)
RFC 3415 SNMPv3 View-based Access Control Model VACM)

Technical Specifications

RFC 2138 Remote Authentication Dial In User Service (RADIUS)
RFC 2236 IGMP Snooping
RFC 2338 VRRP
RFC 2453 RIPv2
RFC 2460 IPv6
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2644 Directed Broadcast Control
RFC 2711 IPv6 Router Alert Option
RFC 2763 Dynamic Name-to-System ID mapping support
RFC 2784 Generic Routing Encapsulation (GRE)
RFC 2865 Remote Authentication Dial In User Service (RADIUS)
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 3022 Traditional IP Network Address Translator (Traditional NAT)
RFC 3277 IS-IS Transient Blackhole Avoidance
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3416 Protocol Operations for SNMP
RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC 3575 IANA Considerations for RADIUS
RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3736 Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC 3784 ISIS TE support
RFC 3786 Extending the Number of IS-IS LSP Fragments Beyond the 256 Limit
RFC 3787 Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 3847 Restart signaling for IS-IS
RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
RFC 4123: Session Initiation Protocol (SIP)-H.323 Interworking Requirements
ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)

OSPF

RFC 1245 OSPF protocol analysis
RFC 1246 Experience with OSPF
RFC 1765 OSPF Database Overflow
RFC 1850 OSPFv2 Management Information Base (MIB), traps
RFC 2154 OSPF w/ Digital Signatures (Password, MD-5)
RFC 2328 OSPFv2
RFC 2370 OSPF Opaque LSA Option
RFC 3101 OSPF NSSA
RFC 3137 OSPF Stub Router Advertisement
RFC 3623 Graceful OSPF Restart
RFC 3630 Traffic Engineering Extensions to OSPFv2
RFC 4061 Benchmarking Basic OSPF Single Router Control Plane Convergence
RFC 4062 OSPF Benchmarking Terminology and Concepts
RFC 4063 Considerations When Using Basic OSPF Convergence Benchmarks
RFC 4222 Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance
RFC 4577 OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4811 OSPF Out-of-Band LSDB Resynchronization
RFC 4812 OSPF Restart Signaling
RFC 4813 OSPF Link-Local Signaling
RFC 4940 IANA Considerations for OSPF

QoS/CoS

IEEE 802.1p (CoS)
RFC 1349 Type of Service in the Internet Protocol Suite
RFC 2211 Specification of the Controlled-Load Network Element Service
RFC 2212 Guaranteed Quality of Service
RFC 2474 DSCP DiffServ
RFC 2475 DiffServ Architecture
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2598 DiffServ Expedited Forwarding (EF)

Security

IEEE 802.1X Port Based Network Access Control
RFC 1321 The MD5 Message-Digest Algorithm
RFC 1334 PPP Authentication Protocols (PAP)

Technical Specifications

RFC 4251 The Secure Shell (SSH) Protocol Architecture
RFC 4271 A Border Gateway Protocol 4 (BGP-4)
RFC 4291 IP Version 6 Addressing Architecture
RFC 4292 IP Forwarding Table MIB
RFC 4293 Management Information Base for the Internet Protocol (IP)
RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4552 Authentication/Confidentiality for OSPFv3
RFC 4607 Source-Specific Multicast for IP
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
RFC 4861 Neighbor Discovery for IP version 6 (IPv6)
RFC 4862 IPv6 Stateless Address Autoconfiguration
RFC 4884 Extended ICMP to Support Multi-Part Messages
RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
RFC 5130 A Policy Control Mechanism in IS-IS Using Administrative Tags
RFC 5340 OSPF for IPv6
RFC 5492 Capabilities Advertisement with BGP-4
RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

IP multicast

RFC 2236 IGMPv2
RFC 2283 Multiprotocol Extensions for BGP-4
RFC 2362 PIM Sparse Mode
RFC 3376 IGMPv3
RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3973 PIM Dense Mode
RFC 4541 Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener

RFC 1492 TACACS+
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2082 RIP-2 MD5 Authentication
RFC 2104 Keyed-Hashing for Message Authentication
RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 The Internet Key Exchange (IKE)
RFC 2716 PPP EAP TLS Authentication Protocol
RFC 2865 RADIUS Authentication
RFC 2866 RADIUS Accounting
RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
RFC 2868 RADIUS Attributes for Tunnel Protocol Support
RFC 2869 RADIUS Extensions
RFC 5080: Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes
Access Control Lists (ACLs)
Guest VLAN for 802.1X
MAC Authentication
Port Security
SSHv1/SSHv2 Secure Shell

VPN

RFC 2403 - HMAC-MD5-96
RFC 2404 - HMAC-SHA1-96
RFC 2405 - DES-CBC Cipher algorithm
RFC 2407 - Domain of interpretation
RFC 2473 Generic Packet Tunneling in IPv6 Specification
RFC 2547 BGP/MPLS VPNs
RFC 2917 A Core MPLS IP VPN Architecture
RFC 3947 - Negotiation of NAT-Traversal in the IKE
RFC 4302 - IP Authentication Header (AH)
RFC 4303 - IP Encapsulating Security Payload (ESP)

IPsec

RFC 1828 IP Authentication using Keyed MD5
RFC 1829 The ESP DES-CBC Transform
RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention
RFC 2401 IP Security Architecture
RFC 2402 IP Authentication Header
RFC 2406 IP Encapsulating Security Payload
RFC 2410 - The NULL Encryption Algorithm and its

Technical Specifications

Discovery (MLD) Snooping Switches
RFC 4601 Draft 10 PIM Sparse Mode
RFC 4604 Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener
Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC 4605 IGMP/MLD Proxying
RFC 4607 Source-Specific Multicast for IP
RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
RFC 5059 Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

IPv6

RFC 1886 DNS Extension for IPv6
RFC 1887 IPv6 Unicast Address Allocation Architecture
RFC 1981 IPv6 Path MTU Discovery
RFC 2080 RIPng for IPv6
RFC 2081 RIPng Protocol Applicability Statement
RFC 2292 Advanced Sockets API for IPv6
RFC 2373 IPv6 Addressing Architecture
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 IPv6 Specification
RFC 2461 IPv6 Neighbor Discovery
RFC 2462 IPv6 Stateless Address Auto-configuration
RFC 2463 ICMPv6
RFC 2464 Transmission of IPv6 over Ethernet Networks
RFC 2473 Generic Packet Tunneling in IPv6
RFC 2526 Reserved IPv6 Subnet Anycast Addresses
RFC 2529 Transmission of IPv6 Packets over IPv4
RFC 2545 Use of MP-BGP-4 for IPv6
RFC 2553 Basic Socket Interface Extensions for IPv6
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2740 OSPFv3 for IPv6
RFC 2767 Dual stacks IPv46 & IPv6
RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
RFC 3307 IPv6 Multicast Address Allocation
RFC 3315 DHCPv6 (client and relay)
RFC 3484 Default Address Selection for IPv6
RFC 3513 IPv6 Addressing Architecture
RFC 3736 Stateless Dynamic Host Configuration
use with IPsec
RFC 2411 IP Security Document Roadmap

Technical Specifications

Protocol (DHCP) Service for IPv6
RFC 3810 MLDv2 for IPv6
RFC 4214 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
RFC 4861 IPv6 Neighbor Discovery
RFC 4862 IPv6 Stateless Address Auto-configuration

Accessories

HPE FlexNetwork 7500 Switch Series accessories

Modules

HPE FlexNetwork 7500 12-port GbE SFP SC Module	JD207A
HPE FlexNetwork 7500 24-port GbE SFP SC Module	JD203B
HPE FlexNetwork 7500 24-port GbE SFP Enhanced Module	JD231A
HPE FlexNetwork 7500 24-port GbE SFP with 8 Combo SD Module	JD234A
HPE FlexNetwork 7500 24-port GbE SFP/2-port 10GbE XFP Module	JD205A
HPE FlexNetwork 7500 24-port GbE SFP with 8 Combo and 2-port 10GbE XFP SD Module	JD230A
HPE FlexNetwork 7500 48-port GbE SFP SC Module	JD211B
HPE FlexNetwork 7500 48-port GbE SFP Enhanced Module	JD221A
HPE FlexNetwork 7500 48-port GbE SFP SD Module	JD237A
HPE FlexNetwork 7500 20-port Gig-T/4-port GbE Combo PoE-upgradable SC Module	JC669A
HPE FlexNetwork 7500 24-port Gig-T SC Module	JD204B
HPE FlexNetwork 7500 24-port Gig-T/2-port 10GbE XFP SC Module	JD206A
HPE FlexNetwork 7500 40-port Gig-T/8-port SFP PoE-upgradable SC Module	JD228B
HPE FlexNetwork 7500 48-port Gig-T PoE-ready SC Module	JD210A
HPE FlexNetwork 7500 48-port Gig-T PoE+ SD Module	JD229B
HPE FlexNetwork 7500 48-port 1000BASE-T PoE+ SC Module	JG663A
HPE FlexNetwork 7500 2-port 10GbE XFP SC Module	JD201A
HPE FlexNetwork 7500 2-port 10GbE XFP Enhanced Module	JD233A
HPE FlexNetwork 7500 2-port 10GbE XFP SD Module	JD236A
HPE FlexNetwork 7500 4-port 10GbE XFP Enhanced Module	JD232A
HPE FlexNetwork 7500 4-port 10GbE XFP SD Module	JD235A
HP FlexNetwork 7500 8-port 10GbE XFP SD Module	JD191A
HPE FlexNetwork 7500 8-port 10G SFP+ SC Module	JF290A
HPE FlexNetwork 7500 4-port 40GbE QSFP+ SC Module	JC792A
HP 7500 4-port 40GbE CFP SC Module	JG373A
HPE FlexNetwork 7500 44-port SFP/4-port SFP+ SE Module	JH210A
HPE FlexNetwork 7500 24-port SFP/4-port SFP+ SE Module	JH211A
HPE FlexNetwork 7500 48-port 1000BASE-T SE Module	JH212A
HPE FlexNetwork 7500 48-port 1000BASE-T with PoE+ SE Module	JH213A
HPE FlexNetwork 7500 16-port 1/10GbE SFP+ SF Module	JH214A
HPE FlexNetwork 7500 12-port 1/10GbE SFP+ EC Module	JH309A
HP 7500 48-port 100BASE-FX Module	JD197B

Transceivers

HPE X125 1G SFP LC LH40 1310nm Transceiver	JD061A
HPE X120 1G SFP LC LH40 1550nm Transceiver	JD062A
HPE X125 1G SFP LC LH70 Transceiver	JD063B
HPE X120 1G SFP RJ45 T Transceiver	JD089B
HPE X120 1G SFP LC BX 10-U Transceiver	JD098B
HPE X120 1G SFP LC BX 10-D Transceiver	JD099B
HPE X120 1G SFP LC LH100 Transceiver	JD103A

Accessories

HPE X170 1G SFP LC LH70 1550 Transceiver	JD109A
HPE X170 1G SFP LC LH70 1590 Transceiver	JD111A
HPE X170 1G SFP LC LH70 1610 Transceiver	JD112A
HPE X170 1G SFP LC LH70 1510 Transceiver	JD115A
HPE X120 1G SFP LC SX Transceiver	JD118B
HPE X120 1G SFP LC LX Transceiver	JD119B
HPE X115 100M SFP LC BX 10-U Transceiver	JD100A
HPE X115 100M SFP LC BX 10-D Transceiver	JD101A
HPE X115 100M SFP LC FX Transceiver	JD102B
HPE X110 100M SFP LC LX Transceiver	JD120B
HPE X130 10G XFP LC ZR Single Mode 80km 1550nm Transceiver	JD107A
HPE X130 10G XFP LC LR Single Mode 10km 1310nm Transceiver	JD108B
HPE X130 10G XFP LC SR Transceiver	JD117B
HPE X135 10G XFP LC ER Transceiver	JD121A
HPE X130 10G SFP+ LC SR Transceiver	JD092B
HPE X130 10G SFP+ LC LRM Transceiver	JD093B
HPE X130 10G SFP+ LC LR Transceiver	JD094B
HPE X130 10G SFP+ LC LH80 tunable Transceiver	JL250A
HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable	JD095C
HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable	JD096C
HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable	JD097C
HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable	JG081C
HPE X180 10G XFP LC LH 80km 1538.98nm DWDM Transceiver	JG226A
HPE X180 10G XFP LC LH 80km 1539.77nm DWDM Transceiver	JG227A
HPE X180 10G XFP LC LH 80km 1542.94nm DWDM Transceiver	JG230A
HPE X130 10G SFP+ LC ER 40km Transceiver	JG234A
HPE X140 40G QSFP+ MPO SR4 Transceiver	JG325B
HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver	JG661A
HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver	JG709A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable	JG326A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable	JG327A
HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable	JG328A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable	JG329A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable	JG330A
HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable	JG331A
HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver	JL251A

Cables

HPE LC to LC Multi-mode OM3 2-Fiber 50.0m 1-Pack Fiber Optic Cable	AJ839A
HPE LC to LC Multi-mode OM3 2-Fiber 30.0m 1-Pack Fiber Optic Cable	AJ838A
HPE LC to LC Multi-mode OM3 2-Fiber 15.0m 1-Pack Fiber Optic Cable	AJ837A
HPE LC to LC Multi-mode OM3 2-Fiber 5.0m 1-Pack Fiber Optic Cable	AJ836A
HPE LC to LC Multi-mode OM3 2-Fiber 2.0m 1-Pack Fiber Optic Cable	AJ835A
HPE LC to LC Multi-mode OM3 2-Fiber 1.0m 1-Pack Fiber Optic Cable	AJ834A
HPE LC to LC Multi-mode OM3 2-Fiber 0.5m 1-Pack Fiber Optic Cable	AJ833A
HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 1m Cable	QK732A

Accessories

HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 2m Cable	QK733A
HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 5m Cable	QK734A
HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 15m Cable	QK735A
HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 30m Cable	QK736A
HPE Premier Flex LC/LC Multi-mode OM4 2 fiber 50m Cable	QK737A

Mounting Kit

HPE X421 Chassis Universal 4-post Rackmount Kit	JC665A

Appliance

HPE 10500/11900/7500 20Gbps VPN Firewall Module	JG372A

Memory

HPE FlexNetwork 7500 PoE DIMM Memory Module	JD192B
HPE X600 1G Compact Flash Card	JC684A
HPE X600 512M Compact Flash Card	JC685A
HPE X600 256M Compact Flash Card	JC686A

HPE FlexNetwork 7510 Switch Chassis (JD238C)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7510 Spare Fan Assembly	JD216A

HPE FlexNetwork 7506 Switch Chassis (JD239C)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A
HPE FlexNetwork 7506 Spare Fan Assembly	JD214A

HPE FlexNetwork 7503 Switch Chassis (JD240C)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A
HPE FlexNetwork 7503 Spare Fan Assembly	JD212A

Accessories

HPE FlexNetwork 7502 Switch Chassis (JD242C)

HPE FlexNetwork 7502 Main Processing Unit	JH208A
HPE FlexNetwork 7500 650W AC Power Supply	JD217A
HPE FlexNetwork 7500 650W DC Power Supply	JD209A
HPE FlexNetwork 7502 300W AC Power Supply	JD226A
HPE RPS 800 Redundant Power Supply	JD183A
HPE FlexNetwork 7502 Spare Fan Assembly	JD213A

HPE FlexNetwork 7510 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH333A)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7510 Spare Fan Assembly	JD216A

HPE FlexNetwork 7506 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH332A)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A
HPE FlexNetwork 7506 Spare Fan Assembly	JD214A

HPE FlexNetwork 7503 Switch with 2x2.4Tbps Fabric and Main Processing Unit Bundle (JH331A)

HPE FlexNetwork 7500 1.2Tbps Fabric with 2-port 40GbE QSFP+ for IRF-only Main Processing Unit	JH207A
HPE FlexNetwork 7500 2.4Tbps Fabric with 8-port 1/10GbE SFP+ and 2-port 40GbE QSFP+ MPU	JH209A
HPE FlexNetwork 7500 1400W DC Power Supply	JD208A
HPE FlexNetwork 7500 1400W AC Power Supply	JD218A
HPE FlexNetwork 7500 2800W AC Power Supply	JD219A
HPE FlexNetwork 7500 6000W AC Power Supply	JD227A
HPE FlexNetwork 7503/7506/7506 V 650W AC Power Supply Unit	JH215A
HPE FlexNetwork 7503 Spare Fan Assembly	JD212A

Summary of Changes

Date	Version History	Action	Description of Change:
01-Aug-2016	From Version 44 to 45	Added	SKUs added: JL250A
		Changed	Technical Specifications and Accessories updated.
10-Jun-2016	From Version 43 to 44	Changed	Updates on the Configuration section
06-Jun-2016	From Version 42 to 43	Changed	Document name changed to HPE FlexNetwork 7500 Switch Series. Product description updated.
08-Apr-2016	From Version 41 to 42	Changed	SKU descriptions updated on all document.
18-Mar-2016	From Version 40 to 41	Changed	Overview, Features and Benefits, Configuration, Technical Specifications and Accessories updated.
15-Jan-2016	From Version 39 to 40	Changed	Overview and Technical Specifications updated
		Removed	SKUs removed: JD238B, JD239B, JD240B, JD242B
01-Dec-2015	From Version 38 to 39	Changed	Overview and Technical Specifications updated
02-Oct-2015	From Version 37 to 38	Changed	Configuration section updated
28-Sep-2015	From Version 36 to 37	Added	Models added: JD238C, JD239C, JD240C, JD242C, JH331A, JH332A, JH333A Accessories section added
		Changed	Updates made on Overview, Features and Benefits, Configuration and Technical Specifications.
17-Feb-2015	From Version 35 to 36	Changed	SKUs descriptions and Configuration menu updated.
03-Jul-2014	From Version 34 to 35	Changed	Configuration menu updated.
10-Jun-2014	From Version 33 to 34	Changed	Switch Enclosure Options were updated in the Configuration section.
15-Apr-2014	From Version 30 to 33	Changed	Minor edit was made in Product Overview.
31-Mar-2014	From Version 29 to 30	Changed	Configuration Rules was revised throughout Configuration.
19-Mar-2014	From Version 28 to 29	Changed	Transceivers were revised in Configuration.
22-Nov-2013	From Version 27 to 28	Changed	Box Level Integration CTO Models, Rack Level Integration CTO Models, and Internal Power Supplies were revised in Configuration.
14-Oct-2013	From Version 26 to 27	Changed	Configuration was revised, including adding a new Transceiver.
30-Sep-2013	From Version 25 to 26	Changed	Configuration was revised. Features and Benefits was revised. Product overview was revised.
27-Sep-2013	From Version 24 to 25	Changed	Configuration was revised.
11-Sep-2013	From Version 23 to 24	Changed	Minor edit was made in Configuration.
19-Aug-2013	From Version 22 to	Changed	Box Level Integration CTO Models and Rack Level

Summary of Changes

	23		Integration CTO Models were revised in Configuration.
12-Jul-2013	From Version 21 to 22	Changed	Updated the Configuration Information.
19-Jun-2013	From Version 20 to 21	Changed	HP 10500/7500 20G Unified Wired-WLAN Module was added to Accessory Product Details Integration was revised in Features and Benefits
07-Jun-2013	From Version 19 to 20	Changed	Updated the Direct Attach Copper Cables in the Configuration Information section.
22-May-2013	From Version 18 to 19	Changed	Updated the Configuration Information.
12-Apr-2013	From Version 17 to 18	Removed	Completely removed Accessories section. Accessory Product Details: Removed several sections.
		Changed	Configuration: Completely updated Build To Order section.
19-Mar-2013	From Version 16 to 17	Changed	Corrected the new Configuration section.
01-Mar-2013	From Version 15 to 16	Changed	Corrected the formatting in the new Configuration section.
19-Feb-2013	From Version 13 to 15	Added	Added the Configuration section.
		Changed	Changes were made to Features and Benefits. The model specifications had minor updates, as did the Accessories section.
04-Dec-2012	From Version 12 to 13	Changed	Changes were made to Features and Benefits. The model specifications had minor updates, as did the Accessories section.
24-Sep-2012	From Version 11 to 12	Changed	Updated Features and Benefits, Introduction, the specifications, and Accessories.
21-May-2012	From Version 10 to 11	Changed	Updated the Standards and protocols section of Technical specifications.
14-May-2012	From Version 9 to 10	Changed	Features and Benefits, Accessories, and the weight and dimensions for each spec were revised.
02-Apr-2012	From Version 8 to 9	Changed	Part number was revised.
26-Mar-2012	From Version 7 to 8	Changed	Accessories were revised.
16-Nov-2011	From Version 6 to 7	Changed	Specifications were revised.
26-Sep-2011	From Version 5 to 6	Changed	Models, Features and Benefits and Accessories were revised.
07-Sep-2011	From Version 4 to 5	Added	Accessory Product Details was added.
07-Mar-2011	From Version 3 to 4	Changed	Accessories product descriptions and notes and services in Models were revised.
18-Feb-2011	From Version 2 to 3	Changed	Clarified in a couple of locations about the availability of IRF.
08-Oct-2010	From Version 1 to 2	Changed	Corrected the options section.

Summary of Changes

Sign up for updates

To learn more, visit: **http://www.hpe.com/networking**

c04111585 - 13805 - Worldwide - V45 - 1-August-2016

Hewlett Packard Enterprise

PA-3000 Series

Palo Alto Networks® PA-3000 Series of next-generation firewall appliances is comprised of the PA-3060, PA-3050 and PA-3020, all of which are targeted at high-speed Internet gateway deployments. The PA-3000 Series manages network traffic flows using dedicated processing and memory for networking, security, threat prevention and management.

Key Security Features:

Classifies all applications, on all ports, all the time

- Identifies the application, regardless of port, encryption (SSL or SSH), or evasive technique employed.
- Uses the application, not the port, as the basis for all of your safe enablement policy decisions: allow, deny, schedule, inspect and apply traffic-shaping.
- Categorizes unidentified applications for policy control, threat forensics or App-ID™ development.

Enforces security policies for any user, at any location

- Deploys consistent policies to local and remote users running on the Windows®, Mac® OS X®, Linux®, Android®, or Apple® iOS platforms.
- Enables agentless integration with Microsoft® Active Directory® and Terminal Services, LDAP, Novell® eDirectory™ and Citrix®.
- Easily integrates your firewall policies with 802.1X wireless, proxies, NAC solutions, and any other source of user identity information.

Prevent known and unknown threats

- Blocks a range of known threats, including exploits, malware and spyware, across all ports, regardless of common threat-evasion tactics employed.
- Limits the unauthorized transfer of files and sensitive data, and safely enables non-work-related web surfing.
- Identifies unknown malware, analyzes it based on hundreds of malicious behaviors, and then automatically creates and delivers protection.

PA-3060

PA-3050

PA-3020

The controlling element of the PA-3000 Series is PAN-OS®, a security-specific operating system that natively classifies all traffic, inclusive of applications, threats and content, and then ties that traffic to the user, regardless of location or device type. The application, content and user – in other words, the business elements that run your business – are then used as the basis of your security policies, resulting in an improved security posture and a reduction in incident response time.

Performance and Capacities[1]	PA-3050	PA-3060	PA-3020
Firewall throughput (App-ID enabled)	4 Gbps	4 Gbps	2 Gbps
Threat prevention throughput	2 Gbps	2 Gbps	1 Gbps
IPsec VPN throughput	500 Mbps	500 Mbps	500 Mbps
New sessions per second	50,000	50,000	50,000
Max sessions	500,000	500,000	250,000
Virtual systems (base/max[2])	1/6	1/6	1/6

[1] Performance and capacities are measured under ideal testing conditions using PAN-OS 7.1.
[2] Adding virtual systems to the base quantity requires a separately purchased license.

Networking Features

Interface Modes
L2, L3, Tap, Virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
Bidirectional Forwarding Detection (BFD)
IPv6
L2, L3, Tap, Virtual Wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire and SSL decryption
SLAAC
IPSec VPN
Key Exchange: Manual key, IKEv1 and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3DES, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
VLANs
802.1q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation (NAT)
NAT modes (IPv4): Static IP, dynamic IP, dynamic IP and port (port address translation)
NAT64, NPTv6
Additional NAT features: dynamic IP reservation, tunable dynamic IP and port oversubscription
High availability
Modes: Active/Active, Active/Passive
Failure detection: Path monitoring, interface monitoring

Hardware Specifications

I/O
PA-3060 - (8) 10/100/1000, (8) Gigabit SFP, (2) 10 Gigabit SFP+
PA-3050 | PA-3020 - (12) 10/100/1000, (8) SFP Gigabit
Management I/O
(1) 10/100/1000 out-of-band management port, (2) 10/100/1000 high availability, (1) RJ-45 console port
Storage capacity
120GB SSD
Power supply (Avg/max power consumption)
PA-3060 - Redundant 400W AC (160/200)
PA-3050 | PA-3020 - Single 250W AC (150/200)
Max BTU/hr
683
Input voltage (Input frequency)
100-240VAC (50-60Hz)
Max current consumption
2A@100VAC
Rack mountable (Dimensions)
PA-3060 - 1.5U, 19" standard rack (2.6"H x 14"D x 17.5"W)
PA-3050 | PA-3020 -1U, 19" standard rack (1.75"H x 17"D x 17"W)
Weight (Stand alone device/as shipped)
PA-3060 - 18lbs/27.5lbs
PA-3050 | PA-3020 - 15lbs/20lbs
Safety
UL, CUL, CB, cCSAus
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See: https://www.paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32 to 122 F, 0 to 50 C
Non-operating temperature: -4 to 158 F, -20 to 70 C

To view additional information about the features and associated capacities of the PA-3000 Series, please visit www.paloaltonetworks.com/products.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

pan-ds-pa-3000-series-040116

Hewlett Packard Enterprise

HPE Proactive Care Advanced Service

Support Services

HPE Proactive Care Advanced Service expands on HPE Proactive Care Service and is designed to help you maximize the benefits of IT investments, maintain IT infrastructure stability, achieve business and IT project objectives, reduce operational costs, and free your IT staff for other priority tasks. Your assigned HPE Account Support Manager (ASM) provides personalized technical and operational advice, including HPE best practices gleaned from HPE's broad support experience. HPE Proactive Care Advanced can help to save you time with real-time monitoring and analysis of your devices that are connected to HPE, creating personalized proactive reports with recommendations to help prevent problems in your IT infrastructure. Your ASM can also arrange specialist technical advice and assistance to complement your IT skills to assist with specific projects, performance improvements, or other technical needs.

Should an incident occur, reducing business impact requires a swift and comprehensive response. A Hewlett Packard Enterprise Technical Solution Specialist (TSS) delivers an enhanced call experience intended to provide fast incident resolution. For severity 1 incidents, a Critical Event Manager (CEM) is assigned to drive the case and provide you with regular status and progress updates.

HPE Proactive Care Advanced uses Remote Support Technology[1] to monitor devices and collect data, enabling faster delivery of support and services. Running the current version of Remote Support Technology is required to receive full delivery and benefits from this support service.

[1] Remote Support Technology refers to Hewlett Packard Enterprise proprietary service tools used to connect HPE products to HPE for service delivery, including HPE Insight Remote Support, HPE STaTS, and HPE Direct Connect.

Service benefits

HPE Proactive Care Advanced can help you to manage your infrastructure with features designed to provide:

- Increased accountability and personalization through an assigned ASM, who will work with your IT team to share Hewlett Packard Enterprise best practices and specific technical advice relevant to your IT needs and projects
- Faster incident resolution from specially trained, solution-oriented advanced resources who manage the case from start to finish
- A CEM assigned to severity 1 incidents to drive faster resolution and provide regular progress updates to keep you informed
- Recommendations for firmware version and software patching on supported products to help prevent problems[2]
- Identification of risks and issues through regular device-based proactive scans that help ensure that configurations are consistent with Hewlett Packard Enterprise best practices[2]
- Access to technical advice and services from Hewlett Packard Enterprise specialists to augment your team with specific skills and capabilities

HPE Proactive Care Advanced includes credits that you can use to select and fund the specialized service assistance you need, when you need it. You can choose from a range of predefined technical services on the HPE Proactive Select menu, or your ASM can work with you to define the specific advice or assistance you need. More information on Proactive Select can be found at hpe.com/services/proactiveselect.

[2] Requires the Customer to install and operate HPE Remote Support Technology with the data collections function enabled for delivery.

Table 1. Service features overview

HPE support resources (see table 2 for details)	• Account Support Manager (ASM) • Technical Solution Specialist (TSS) • Critical Event Manager (CEM) • Customer Engineer (CE)
Problem prevention and personalized technical expertise (see table 3 for details)	• Firmware and Software Version Report[3] • Proactive Scan Report[3] • Incident Report • Report distribution • Credits for technical advice and services • Support planning and reviews • Remote Support Technology
Incident management (see table 4 for details)	• Enhanced call handling • Enhanced critical incident management • Automatic call logging capability[3] – Basic Software Support and Collaborative Call Management for selected non-HPE software on eligible HPE hardware products • Knowledge database and HPE Support Center access • Replacement parts and materials • Access to firmware updates (for eligible products)
Incident management service levels (see table 4 for details)	• Hardware reactive support choices at three levels: – HPE Next Business Day Proactive Care Advanced Service – HPE 4-hour 24x7 Proactive Care Advanced Service – HPE 6-hour Call-to-Repair Proactive Care Advanced Service • Software reactive support: – 24x7 software support – Software product and documentation updates – License to use software updates if purchased from HPE – HPE recommended software and documentation updates method
Optional additional features for HPE Proactive Care Advanced with defective media retention services (see table 4 for details)	• Defective media retention • Comprehensive defective material retention
Optional additional access to technical expertise (see table 5 for details)	• Proactive Select and Technical Services

[3] Requires the Customer to install and operate Remote Support Technology with the data collections function enabled for delivery.

Table 2. Specifications: HPE support resources

FEATURE	DELIVERY SPECIFICATIONS
Support resources	The Customer has access to the following trained technical specialists.
Account Support Manager (ASM)	The Account Support Manager is an account assigned resource who collaborates with the Customer to understand their specific needs and tailor their support experience accordingly. The ASM can draw on specialist resources as required to help address the Customer's needs. Remote Support Technology is used to provide the Customer with scheduled product-based proactive reports. The ASM will discuss these reports and recommendations with the Customer during local HPE business days and hours excluding HPE holidays. The ASM may deliver services onsite or remotely, at HPE's discretion.
Technical Solution Specialist (TSS)	Technical Solution Specialists provide remote incident support and handle cases from call receipt to call closure. A TSS may engage additional specialist resources, as required, to help achieve resolution. The TSS will remain engaged from case creation through to closure to help ensure a consistent end-to-end support experience for the Customer.
Critical Event Manager (CEM)	Critical Event Managers are assigned to severity 1 cases, as defined in the **General provisions/Other exclusions** section. A CEM is a call center resource who is responsible for managing the incident process, organizing additional resources as required, managing the escalation process, and providing regular updates to the Customer. The assignment of a CEM is intended to accelerate incident resolution and improve Customer communication.
Customer Engineer (CE)	Customer Engineers provide onsite hardware repair when required to resolve an incident. For Next Business Day and 24x7 HPE Proactive Care Advanced service-level customers, the next available CE will respond. 6-hour Call-to-Repair HPE Proactive Care Advanced service-level customers will have an Assigned CE who will respond to incidents, if they are available. If they are not available, the incident will be directed to the next available CE.

Table 3. Specifications: Problem prevention and personalized technical expertise

FEATURE	DELIVERY SPECIFICATIONS
	Hewlett Packard Enterprise will publish a set of reports covering the devices under the HPE Proactive Care Advanced support agreement. These reports will be published to the HPE Support Center for the Customer to access. Remote Support Technology is used to capture the necessary revision and configuration data to enable analysis and report creation. Following the publication of a report, the ASM will review the report with the Customer at an agreed time during HPE local business hours to help ensure that there is a clear understanding of the implications of any detected issues, along with prioritization of recommendations contained within the report.
Firmware and Software Version Report	IT reliability and stability can be impacted by the levels of the Customer's software and firmware revisions. Twice a year, Hewlett Packard Enterprise reviews the products under the HPE Proactive Care Advanced contract to verify that they are at recommended revision levels. HPE provides the Customer with a report containing recommendations for applicable software versions, patches, and firmware revisions for each covered device. The ASM will review these recommendations with the Customer. HPE performs the following core deliverables using Remote Support Technology as part of the firmware and software version recommendation activity.[4] **Firmware version recommendations** The report will indicate the installed and recommended firmware revisions for the devices covered by the HPE Proactive Care Advanced contract. The firmware analysis is limited to those covered devices. Installation is also provided for firmware defined by Hewlett Packard Enterprise as non-customer installable. HPE will install these firmware updates, if requested by the Customer, during the related hardware device support coverage window at no additional charge to the Customer. If HPE determines that the firmware update is designed for remote installation, then additional charges may be applied for onsite installation of the non-customer-installable firmware updates. HPE can provide telephone support for firmware defined as customer installable during the related hardware device support coverage window. The Customer can purchase additional services to install customer-installable firmware. **Software version recommendations** Hewlett Packard Enterprise will provide the Customer with patch analysis and update recommendations for all supported server operating systems, virtualization software, or software required to operate storage devices that are covered under HPE Proactive Care Advanced support.[5] Update recommendations are provided by comparing the Customer's current version information against the latest supported releases. HPE Proactive Care Advanced provides the Customer with HPE's general recommendations, which are intended to address critical gaps with individual devices or products. Hewlett Packard Enterprise can provide telephone assistance, if requested, to help with the installation of software patches for supported software. The Customer can purchase additional services to have HPE install supported software revisions and patches. For select operating systems or virtualization software[5] that is not directly covered by an HPE Proactive Care Advanced agreement but is running on an underlying server covered by HPE Proactive Care Advanced support, HPE will provide an annual report indicating the latest software revisions available. Please consult a Hewlett Packard Enterprise representative or authorized Hewlett Packard Enterprise channel partner for more details.

[4] Requires the Customer to install and operate Remote Support Technology with the data collections function enabled for delivery.

[5] A list of HPE Proactive Care Advanced supported products with selected operating system and virtualization software can be found at hpe.com/services/proactivecareadvanced supportedproducts

Table 3. Specifications: Problem prevention and personalized technical expertise (continued)

FEATURE	DELIVERY SPECIFICATIONS
Proactive Scan Report	Twice a year, Hewlett Packard Enterprise performs a proactive scan of HPE Proactive Care Advanced supported devices in the Customer's computing environment. For HPE servers and certain storage and networking products, this service provides a technical device assessment that is designed to help identify potential system configuration problems before they impact the Customer's business operations. Remote Support Technology is used to collect, transport, and analyze configuration and revision data to identify trends, revisions, or parameters that may impact operation. This analysis uses diagnostic tools and processes to compare the devices to Hewlett Packard Enterprise management best practices or support advisories. HPE then prepares a report that details the findings and highlights potential risks and issues that require resolution or investigation, identifies deviations from HPE best practices, and recommends a possible course of action to address them.[6] The Customer receives a report for supported Hewlett Packard Enterprise servers, storage, and networking products. The ASM will review the possible implications and HPE's suggested recommendations with the Customer. Implementation of the recommendations is the Customer's responsibility; however, additional assistance can be purchased from HPE.
Incident Report	The Customer receives a quarterly report that details the Customer's case history and trends. The ASM will discuss the report content, incident detail, resolution, and longer-term trends with the Customer.
Report distribution	Firmware and Software Version Reports, Proactive Scan Reports, and Incident Reports are provided electronically as part of this service. Through the HPE Support Center (HPESC) portal, reports are distributed using security features designed to maintain confidentiality. Reports are published to the Customer's HPE Support Center account for access by authorized Customer users.
Credits for technical advice and services	HPE Proactive Care Advanced provides access to specialist skills on an as-needed basis. This augments and complements the Customer's own IT team with skills and capacity on a flexible basis. To facilitate this access, 10 credits are included each year of the Customer's support agreement for each configured device. These credits are used to fund technical services, advice, and assistance. A configured device is defined as a chassis device configured with components and software. A list of the categories of configured devices that include credits can be found at hpe.com/services/proactivecareadvancedsupportedproducts. Additional credits can readily be purchased, with or during the life of the support agreement, via HPE Proactive Select by Customers who find they need more than what is included in the standard offer. Credits included in the HPE Proactive Care Advanced agreement are to be used on an annual basis for technical services and assistance on HPE Proactive Care Advanced supported products and systems. The ASM will work with the Customer to determine the Customer's preferred use for their credits. These annual credits expire at the end of each year, on the anniversary date of the Customer's Proactive Services Advanced support agreement. Any unused credits cannot be rolled over to the next year of the support agreement and are not refundable.
Support planning and reviews	The ASM and Customer will work together to develop and document a Support Plan. The ASM will consult with the Customer about upcoming IT priorities and map out how the Hewlett Packard Enterprise deliverables and credit-based services can be used to help provide maximum benefit. Because needs and pressures on the IT department are constantly changing, this process is repeated every six months to help ensure continual alignment and to review what has been achieved. During the semiannual review meetings, the ASM may share HPE best practices and provide IT operational and technical advice to help with the support planning.

[6] Requires the Customer to install and operate Remote Support Technology with the data collections function enabled for delivery.

Table 3. Specifications: Problem prevention and personalized technical expertise (continued)

FEATURE	DELIVERY SPECIFICATIONS
Remote Support Technology	HPE Proactive Care Advanced Service uses Hewlett Packard Enterprise proprietary service tools, which are referred to in this data sheet as Remote Support Technology. Remote Support is the principal method for delivering event monitoring, automated case creation, and a variety of proactive reports. The current version of Remote Support Technology, with the data collections function enabled, is a prerequisite for delivery of HPE Proactive Care Advanced Service. If the Customer does not install and operate the current version of Remote Support Technology, HPE will not provide the Firmware and Software Version Report, Proactive Scan Report, hardware call-to-repair time commitment, remote monitoring, and automated call logging deliverables of Proactive Care Advanced Service. **Remote Support Technology installation assistance** Remote Support Technology is made available to HPE Support customers as a feature of Proactive Care Advanced Service. The Customer is responsible for installing Remote Support Technology. In order to help ensure a successful installation of Remote Support Technology, HPE will provide up to 8 hours of remote technical advice on the installation and configuration of the initial Remote Support Technology installation upon the Customer's request. The ASM will discuss this with the Customer at the commencement of the contract to determine if assistance is required and will then help to organize the assistance if it is needed. As part of this activity, Hewlett Packard Enterprise will explain the features and benefits of Remote Support Technology and recommend the appropriate configuration based on the type and number of devices supported in the Customer's HPE Proactive Care Advanced environment. To maintain ongoing eligibility for this service, the Customer is responsible for enabling data transfer to Hewlett Packard Enterprise, correctly adding devices to the configuration, installing future upgrades, and maintaining the Customer contact details configured in the Remote Support Technology solution. The Customer acknowledges and agrees to install Remote Support Technology during the service startup process.

Table 4. Specifications: Incident management

FEATURE	DELIVERY SPECIFICATIONS
Enhanced call handling	The Customer can contact HPE 24 hours a day, 7 days a week. When the Customer calls with a critical incident, HPE aims to either connect the Customer to a TSS or call the Customer back within 15 minutes. The TSS is trained to address issues in complex computing environments and has access to Hewlett Packard Enterprise's full array of technical knowledge and resources employed with the goal to help rapidly diagnose and resolve issues. In the event that there is a hardware issue requiring onsite service, a CE is dispatched to the Customer's site in accordance with the purchased hardware onsite reactive service level for that affected device. In addition to providing troubleshooting, the TSS employs rigorous case management and escalation procedures and engages additional technical specialists as needed. Hardware support onsite response times and call-to-repair time commitments, as well as software support remote response times, differ depending on incident severity and the purchased onsite coverage level. The Customer determines the incident severity level when logging or confirming a case with Hewlett Packard Enterprise. Incident severity levels are defined in the **General provisions/Other exclusions** section. Once a service request has been placed and Hewlett Packard Enterprise has acknowledged[7] receipt of the case, HPE will work to isolate the hardware or software problem and to troubleshoot, remedy, and attempt to resolve the problem remotely with the Customer. Prior to any onsite assistance, HPE may initiate and perform remote diagnostic tests using innovative automation tools to access covered products, or HPE may use other means available to facilitate remote problem resolution. Incident cases for Hewlett Packard Enterprise connected products using Remote Support Technology can be automatically created 24x7. Customers may also report problems to HPE via a special access phone number or electronically via HPESC. Hewlett Packard Enterprise retains the right to determine the final resolution of all reported problems.
Enhanced critical incident management	Hewlett Packard Enterprise employs integrated case management tools and enhanced escalation procedures to help resolve complex support incidents. For severity 1 incidents, HPE will engage a CEM to internally monitor and coordinate the end-to-end process and provide prompt and effective engagement of additional expertise to help accelerate resolution of an incident. The CEM will provide regular progress updates directly to the Customer. For severity 1 incidents, HPE may provide a post-incident review at its discretion. This activity helps to identify any suggested improvements that could be made by the Customer or HPE, and is intended to help prevent the occurrence of similar incidents, or improve incident handling, in the future. Incident severity levels are defined in the **General provisions/Other exclusions** section.
Automatic call logging capability[8]	For supported devices, automatic call logging capabilities are enabled so that devices will submit service incidents directly to Hewlett Packard Enterprise using Remote Support Technology.[8] Incidents are submitted with "failure data" 24x7 and are responded to within the service level timeframe for the associated device. Where configured, HPE Insight Online can provide a single point of visibility to incidents and resolution.

[7] Please see the "General provisions/Other exclusions" section for more details.

[8] Requires the Customer to install and operate Remote Support Technology with the data collections function enabled for delivery.

Table 4. Specifications: Incident management (continued)

FEATURE	DELIVERY SPECIFICATIONS
Basic Software Support and Collaborative Call Management for selected non-HPE software on eligible HPE hardware products[9]	In cases where the Customer has not purchased HPE Proactive Care Advanced support on selected non-HPE software products that reside on eligible hardware equipment covered by HPE Proactive Care Advanced support, Hewlett Packard Enterprise will provide the Basic Software Support and Collaborative Call Management features as described below, instead of HPE Proactive Care Advanced software support as described in the "Software incident support" section of table 4. Basic Software Support on selected non-HPE software products is limited to the following: Hewlett Packard Enterprise will attempt to resolve problems on these products by applying or asking the Customer to apply fixes that have been made available or known to HPE. In some cases, support may be limited to communication of a known fix available through the installation of a software update or patch, and the Customer will be directed to available sources for the applicable updates or patches because access to the known fix requires additional service contracts with the respective software vendor. If the problem is still not resolved, then Collaborative Call Management can be initiated at the Customer's request. Basic Software Support is available 24 hours per day, 7 days per week. If Hewlett Packard Enterprise determines that a problem is caused by a selected independent software vendor's (ISV) product and the problem is not resolved by the Customer applying known available fixes, HPE will, at the Customer's request, initiate Collaborative Call Management with the ISV. Collaborative Call Management can be provided only in cases where Customers have appropriate active support agreements in place with selected ISVs and the Customer has taken the steps necessary to ensure that Hewlett Packard Enterprise can submit calls on the Customer's behalf for the limited purpose of placing a support call with the vendor. HPE will engage the ISV and provide information about the Customer's issue, as obtained during the Basic Software Support service call. HPE will make the TSS available for a telephone conference with the ISV as the preferred engagement method, but the process is subject to vendor participation and may vary by ISV. Once the call has transitioned to the ISV, it is then the responsibility of the ISV to resolve the Customer issue. Once the call is transitioned to the ISV, the call will be subject to the support levels of the agreement between the Customer and that ISV. Once the ISV is engaged, HPE will close the HPE call, but the Customer or ISV can resume the service issue with HPE if needed by referencing the original call identification number.
Knowledge database and HPE Support Center access	Hewlett Packard Enterprise provides access to HPESC as part of HPE Proactive Care Advanced Service. HPESC is HPE's next-generation support portal that provides a helpful online resource. Key features of this personalized portal include HPE Insight Online (personalized dashboard), support forums, support case submittal, drivers, patch management, product pages, guided troubleshooting, top issues, warranty and contract details, and software updates. Service credits can also be managed through HPESC. HPESC access and functionality are enabled through the linking of the Customer's HPE passport with Service Agreements, and must be done to enable all available features. For more information, visit hpe.com/support/hpesc Through HPESC, the Customer has access to: • Published Proactive Care reports for the Customer. • Subscription to hardware-related proactive service notifications, and participation in support forums for solving problems and sharing best practices with other registered users. • Expanded Web-based searches of entitled technical support documents to facilitate faster problem-solving. • Certain Hewlett Packard Enterprise proprietary service diagnostic tools with password access. • A Web-based tool for submitting questions directly to Hewlett Packard Enterprise. The tool helps to resolve problems quickly with a prequalification process that routes the support or service request to the resource qualified to answer the question. The tool also allows the status of each support or service request submitted to be viewed, including cases submitted by telephone.

[9] For a list of the non-HPE software products eligible for Basic Software Support and Collaborative Call Management, please refer to hpe.com/services/collaborativesupport. In addition to the products covered on this list, any additional ISV products and variations on these deliverables are noted at hpe.com/services/proactivecareadvancedsupportedproducts.

Table 4. Specifications: Incident management (continued)

FEATURE	DELIVERY SPECIFICATIONS
Knowledge database and HPE Support Center access (continued)	• Hewlett Packard Enterprise and available third-party hosted knowledge databases, which can be searched for certain third-party products in order to retrieve product information, get answers to support questions, and participate in support forums. This service may be limited by third-party access restrictions. • Services, which the Customer can browse, select, and schedule using credits, as well as view the current balance of available credits.
Replacement parts and materials	Hewlett Packard Enterprise will provide replacement parts and materials necessary to maintain the covered hardware product in operating condition, including parts and materials for available and recommended engineering improvements. Replacement parts provided by HPE shall be new or functionally equivalent to new in performance. All replaced parts become the property of HPE unless optional Defective Material Retention or Comprehensive Defective Material Retention options have been purchased. Customers who wish to retain, degauss, or otherwise physically destroy replaced parts will be billed and required to pay the list price for the replacement part. Supplies and consumable parts are not supported and will not be provided as part of this service; standard warranty terms and conditions apply to supplies and consumable parts. The repair or replacement of any supplies or consumable parts is the responsibility of the Customer. Some exceptions may apply; contact Hewlett Packard Enterprise for more information. If a consumable part is eligible for coverage, as determined by HPE, call-to-repair time commitments and onsite response times do not apply to repair or replacement of the covered consumable part. **Maximum supported lifetime/maximum usage** Parts and components that have reached their maximum supported lifetime and/or the maximum usage limit as set forth in the manufacturer's operating manual, product QuickSpecs, or the technical product data sheet will not be provided, repaired, or replaced as part of this service.
Firmware updates for eligible products	As Hewlett Packard Enterprise releases entitled firmware updates to HPE hardware products, these updates are only made available to Customers with an active agreement that entitles them to access these updates. HPE Proactive Care Advanced Customers will have the right to download, install, and use firmware updates for hardware products covered by this service, subject to all applicable license restrictions in HPE's current standard sales terms. Hewlett Packard Enterprise will verify entitlement to updates by reasonable means (such as an access code or other identifier), and the Customer is responsible for using any such access tools in accordance with the terms of this data sheet and other applicable agreements with HPE. Hewlett Packard Enterprise may take additional reasonable steps, including audits, to verify the Customer's adherence to terms of their agreements with HPE, including this data sheet. For Customers with licenses to firmware-based software products (features implemented in firmware activated by the purchase of a separate software license product), the Customer must also have, if available, an active HPE Software Support agreement to receive, download, install, and use related firmware updates. HPE will provide, install, or assist the Customer with the installation of firmware updates as previously described in this document only if the Customer has the license to use the related software updates for each system, socket, processor, processor core, or end-user software license as allowed by the original HPE or original manufacturer software license terms.

Table 4. Specifications: Incident management (continued)

FEATURE	DELIVERY SPECIFICATIONS
Incident management service-level choices	
Hardware and software incident support	Each HPE Proactive Care Advanced Service level includes problem prevention and incident management support for hardware and software products. For each HPE Proactive Care Advanced service level, HPE provides all the core problem prevention service features noted in table 2 and table 3, as well as the related core incident management service features noted in table 4. For hardware products, the HPE Proactive Care Advanced portfolio offers three distinct hardware service levels.[10] • HPE Next Business Day Proactive Care Advanced Service • HPE 4-hour 24x7 Proactive Care Advanced Service • HPE 6-hour Call-to-Repair Proactive Care Advanced Service The HPE Proactive Care Advanced portfolio also offers the same three service levels with the inclusion of hardware defective media retention (DMR) and comprehensive defective material retention (CDMR) as additional optional features that the Customer may elect to purchase based upon their requirements. For eligible products, the DMR service feature option, if purchased, allows the Customer to retain a defective hard disk or eligible SSD/Flash drive that the Customer does not want to relinquish due to sensitive data contained within the disk ('Disk or SSD/Flash Drive') covered under this service. All Disk or eligible SSD/Flash Drives on a covered system must participate in the DMR. In addition to DMR, the CDMR service feature option, if purchased, allows the Customer to retain additional components that have been designated by HPE as having data retentive capabilities, such as memory modules. All eligible data retentive components on a covered system must participate in the CDMR. The components that can be retained under this service feature are outlined in the document located at hpe.com/services/cdmr.
	For software products, HPE Proactive Care Advanced Service provides software support 24 hours per day, 7 days per week including HPE holidays. Once a noncritical software service request (severity 3 or 4) is received, HPE will respond to the call within 2 hours after the service request has been logged. HPE provides corrective support to resolve identifiable and customer-reproducible software product problems. HPE also provides support to help the Customer identify problems that are difficult to reproduce. The Customer receives assistance with troubleshooting incidents and resolving configuration parameters. For critical software response (severity 1 or 2) situations, please refer to the 'Enhanced call handling' feature described earlier in this document. The variations in the HPE Proactive Care Advanced reactive hardware service levels are outlined in the section that follows. All coverage windows are subject to local availability. Contact a local Hewlett Packard Enterprise sales office for detailed information on service availability.

[10] All service levels may not be available on all products.

Table 4. Specifications: Incident management (continued)

FEATURE	DELIVERY SPECIFICATIONS
Hardware incident support options	
HPE Next Business Day Proactive Care Advanced Service	Hewlett Packard Enterprise provides the following reactive service levels for the specific devices covered under this option: **Hardware support coverage window:** • Standard business hours, standard business days (9x5): Onsite service is available 9 hours per day between 8:00 a.m. and 5:00 p.m. local time, Monday through Friday, excluding HPE holidays. **Hardware onsite support response time:** • Next Business Day onsite response: A Hewlett Packard Enterprise authorized representative (CE) will arrive at the Customer's site during the onsite coverage window to begin hardware maintenance service on the next coverage day after the call has been received and acknowledged by HPE. Service features are defined in the "Hardware onsite support" area of the **Service limitations** section. Availability of response times is dependent on the proximity of the Customer site to an HPE-designated support hub. See table 6 for more details. Please contact HPE for further information.
HPE 4–hour 24x7 Proactive Care Advanced Service	Hewlett Packard Enterprise provides the following reactive service levels for the specific devices covered under this option: **Hardware support coverage window:** • 24x7: Service is available 24 hours per day, 7 days per week including HPE holidays. **Hardware onsite support response time:** • 4-hour onsite response: A Hewlett Packard Enterprise authorized representative (CE) will arrive at the Customer's site during the onsite coverage window to begin hardware maintenance service within 4 hours after the call has been received and acknowledged by HPE. Service features are defined in the "Hardware onsite support" area of the **Service limitations** section. Availability of response times is dependent on the proximity of the Customer site to an HPE-designated support hub. See table 6 for more details. Please contact HPE for further information.
HPE 6-hour Call-to-Repair Proactive Care Advanced Service	Hewlett Packard Enterprise provides the following reactive service levels for the specific devices covered under this option: **Hardware support coverage window:** • 24x7: Service is available 24 hours per day, 7 days per week including HPE holidays. **Hardware call-to-repair time commitment:** For critical incidents (severity 1 and 2), Hewlett Packard Enterprise will use commercially reasonable efforts to return the covered hardware to operating condition within 6 hours after the call has been received and acknowledged by HPE. Service features are defined in the "Hardware onsite support" and "Hardware call-to-repair commitment" areas of the **Service limitations** section. Availability of response times and call-to-repair times is dependent on the proximity of the Customer site to an HPE-designated support hub. See table 6 for more details. Please contact HPE for further information. For noncritical incidents (severity 3 and 4) or at the Customer's request, Hewlett Packard Enterprise will work with the Customer to schedule an agreed-upon time for the remedial action to begin, and the call-to-repair time commitment will then start at that time. Incident severity levels are defined in the **General provisions/ Other exclusions** section. Call-to-repair time refers to the period of time that begins when the initial call has been received and acknowledged by Hewlett Packard Enterprise or at the start time for work scheduled in agreement with the Customer, as specified in the **General provisions/Other exclusions** section. Call-to-repair time ends with HPE's determination that the hardware is repaired, or when the reported event is closed with the explanation that HPE has determined that it does not currently require onsite intervention.

Table 4. Specifications: Incident management (continued)

FEATURE	DELIVERY SPECIFICATIONS
HPE 6-hour Call-to-Repair Proactive Care Advanced Service (continued)	Repair is considered complete upon Hewlett Packard Enterprise verification that the hardware malfunction has been corrected or that the hardware has been replaced. HPE is not liable for any lost data, and the Customer is responsible for implementing appropriate backup procedures. Verification by HPE may be accomplished by the completion of a power-on self-test, standalone diagnostic, or visual verification of proper operation. At its sole discretion, HPE will determine the level of testing necessary to verify that the hardware is repaired. At its sole discretion, HPE may temporarily or permanently replace the product in order to meet the call-to-repair time commitment. Replacement products are new or functionally equivalent to new in performance. Replaced products become the property of HPE. It will take 30 days from the time this service is purchased to set up and perform necessary audits and processes so that the hardware call-to-repair time commitment can be put into effect. During this initial 30-day period and for up to 5 additional business days after the audit is completed, Hewlett Packard Enterprise will provide a 4-hour onsite response time. Enhanced parts inventory management (call-to-repair time commitment only) To support Hewlett Packard Enterprise call-to-repair time commitments, an inventory of critical replacement parts is maintained for Customers who have selected the call-to-repair option. This inventory is stored at an HPE-designated facility. These parts are managed to allow for increased inventory availability and are accessible to Hewlett Packard Enterprise authorized representatives responding to eligible calls.
Software product and documentation updates	As Hewlett Packard Enterprise releases updates to HPE software, the latest revisions of the software and reference manuals are made available to the Customer. For selected third-party software, HPE will provide software updates as such updates are made available from the third party, or HPE may provide instructions on how the Customer can obtain any software updates directly from the third party. A license key or access code, or instructions for obtaining a license key or access code, will also be provided to the Customer when they are required to download, install, or run the latest software revision.
	For most Hewlett Packard Enterprise software and selected HPE-supported third-party software, updates will be made available through the Software Updates and Licensing portal via the HPESC. The Software Updates and Licensing portal provides the Customer with electronic access to receive and proactively manage software product and documentation updates. For other HPE-supported third-party software, the Customer may be required to download updates directly from the vendor's website.
License to use software updates	The Customer receives the license to use software updates to HPE or HPE-supported third-party software for each system, socket, processor, processor core, or end-user software license covered by this service, as allowed by the Hewlett Packard Enterprise or original manufacturer software license terms. The license terms shall be as described in the HPE software licensing terms corresponding to the Customer's prerequisite underlying software license, or in accordance with the current licensing terms of the third-party software manufacturer, if applicable, including any additional software licensing terms that may accompany such software updates provided under this service.
HPE recommended software and documentation updates method	For HPE or HPE-supported third-party software and documentation updates, the recommended delivery method will be determined by Hewlett Packard Enterprise. The primary delivery method for software updates and documentation updates will be via download from the Software Updates and Licensing portal or a third-party hosted website.

Table 5. Specifications: Optional additional access to technical expertise

FEATURE	DELIVERY SPECIFICATIONS
Proactive Select and Technical Services	The provision of additional technical expertise is an optional feature and is a flexible way to augment and complement the Customer's own IT team skills, providing specialist capacity on an as-needed basis. If the Customer wishes to access technical services from Hewlett Packard Enterprise, such services can be provided through the per-event HPE Technical Services portfolio or by purchasing HPE Proactive Select. HPE Proactive Select can be used by HPE Proactive Care Advanced customers to purchase additional credits. More information on HPE Proactive Select can be found at hpe.com/services/proactiveselect.

Table 6. Specifications: Service travel zones

FEATURE	DELIVERY SPECIFICATIONS		
Geographic locations	Travel zones and charges, if applicable, may vary in some geographic locations.		
Travel zones table for hardware onsite response time	**Distance from HPE-designated support hub**	**4-hour hardware onsite response time**	**Next-day hardware onsite response time**
	0–100 miles (0–160 km)	4 hours	Next coverage day
	101–200 miles (161–320 km)	8 hours	1 additional coverage day
	201–300 miles (321–480 km)	Established at time of order and subject to availability	2 additional coverage days
	More than 300 miles (480+ km)	Established at time of order and subject to availability	Established at time of order and subject to availability
Hardware call-to-repair time commitment	A hardware call-to-repair time commitment is available for sites located within 50 miles (80 km) of an HPE-designated support hub. Travel zones and charges may vary in some geographic locations. The hardware call-to-repair time commitment is not available for sites located more than 100 miles (160 km) from an HPE-designated support hub. For sites that are located from 51 to 100 miles (81 to 160 km) of an HPE-designated support hub, an adjusted hardware call-to-repair time commitment applies, as shown in the table that follows.		
Travel zone table for hardware call-to-repair time commitment	**Distance from HPE-designated support hub**	**6-hour hardware call-to-repair time**	
	0–50 miles (0–80 km)	6 hours	
	51–100 miles (81–160 km)	8 hours	
	More than 100 miles (160+ km)	Not available	

Service limitations

Services provided within the scope of one HPE Proactive Care Advanced support contract are restricted to the IT environment under the direct day-to-day management of one IT manager, in one country. Unless otherwise specified or arranged, proactive and consultative services are performed during standard local HPE business hours and days excluding HPE holidays. Except as otherwise noted in this document, the scope of HPE Proactive Care Advanced Service is limited to the products under the HPE Proactive Care Advanced support contract.

In cases where the Customer purchases additional HPE Proactive Care Advanced support, the proactive service deliverables for the additional devices will be delivered with the existing devices under contract.

The Firmware and Software Version Report and Proactive Scan Report require the installation of the current version of Remote Support Technology with the data collections function enabled. Should Remote Support Technology not currently support any device, the Customer will be requested to manually collect the data required to enable HPE to include that device in the reports listed above. In this event, HPE will provide the Customer with clear instructions on how and when to manually collect and transfer the necessary data. This data needs to be supplied to HPE within the required timelines in order for HPE to include it in the reports listed above; otherwise, HPE will be under no obligation to provide the reports listed above on these devices and there will be no reduction in fee charges for HPE Proactive Care Advanced Service as a result.

The current supported devices list is available as part of the release notes for Insight Remote Support, which can be found at hpe.com/services/getconnected.

Scope of products covered

This service is available for selected servers, software, storage devices, storage arrays, network devices, and storage area networks only, as noted at hpe.com/services/proactivecareadvancedsupportedproducts.

The features of this service may differ, or be limited, based on specific devices or software. Please check with an Hewlett Packard Enterprise sales office or Hewlett Packard Enterprise sales representative for specific limitations and local availability.

General limitations

Hewlett Packard Enterprise delivery staff will provide the required proactive deliverables defined in table 3 during standard local HPE business hours excluding HPE holidays, either remotely or onsite at the discretion of HPE. If these deliverables are required outside of standard business hours, additional charges may apply and are subject to local availability.

Hewlett Packard Enterprise retains the right to determine the final resolution of all service requests.

Activities such as, but not limited to, the following are excluded from this service:

- Services required due to failure of the Customer to incorporate any system fix, repair, patch, or modification provided to the Customer by Hewlett Packard Enterprise
- Services that, in the opinion of Hewlett Packard Enterprise, are required due to unauthorized attempts by non-HPE personnel to install, repair, maintain, or modify hardware, firmware, or software
- Operational testing of applications, or additional tests requested or required by the Customer
- Services that, in HPE's opinion, are required due to improper treatment or use of the products or equipment
- Services required due to failure of the Customer to take avoidance action previously advised by HPE

- Backup and recovery of the operating system, other software, and data
- Implementation of any Hewlett Packard Enterprise recommendations provided as part of this service
- Installation of any customer-installable firmware and/or software updates

Hardware call-to-repair commitment
If an upfront audit is required by Hewlett Packard Enterprise, the hardware call-to-repair time commitment will not take effect until five (5) business days after the audit has been completed. In addition, HPE reserves the right to downgrade service to an onsite response time or cancel the service contract if critical audit suggestions are not followed or the audit is not performed within the specified timeframe.

Hardware call-to-repair time options are specified in the "HPE 6-hour Call-to-Repair Proactive Care Advanced Service" section (see table 4). All call-to-repair times are subject to local availability. Contact a local Hewlett Packard Enterprise sales office for detailed information on availability.

The hardware repair time commitment may vary for specific products.

A call-to-repair time commitment does not apply when the Customer chooses to have Hewlett Packard Enterprise prolong diagnosis rather than execute recommended server recovery procedures.

A call-to-repair time commitment does not apply if the Customer does not install and operate the current version of Remote Support Technology on all devices. A call-to-repair time commitment is also not available for devices that are not supported by Remote Support Technology. The Customer remains responsible for full payment of all fees associated with the provision of HPE Proactive Care Advanced Services.

Call-to-repair time commitments and onsite response times do not apply to the repair or replacement of defective or depleted batteries for selected enterprise storage arrays and enterprise tape products.

If the Customer requests scheduled service, the repair timeframe begins from the agreed-upon scheduled time.

At the discretion of Hewlett Packard Enterprise, service will be provided using a combination of remote diagnosis and support, services delivered onsite, and other service delivery methods. Other service delivery methods may include the delivery via a courier of customer-replaceable parts such as a keyboard, a mouse, certain hard disk drives, and other parts classified by HPE as Customer Self Repair (CSR) parts, or an entire replacement product. HPE will determine the appropriate delivery method required to provide effective and timely Customer support and meet the call-to-repair time commitment, if applicable.

If the Customer agrees to the recommended CSR and a CSR part is provided to return the system to operating condition, the onsite service level shall not apply. In such cases, Hewlett Packard Enterprise practice is to express ship to the Customer location the CSR parts that are critical to the product's operation. For more details on the CSR process and parts, please refer to hpe.com/info/csr.

The following activities or situations will suspend the call-to-repair time calculation (if applicable) until they are completed or resolved:

- Any Customer or third-party action or inaction impacting the repair process
- Any automated recovery processes triggered by the hardware malfunction, such as disk mechanism rebuild or sparing procedures

- Any other activities not specific to the hardware repair but required to verify that the hardware malfunction has been corrected, such as rebooting the operating system

Hewlett Packard Enterprise reserves the right to modify the call-to-repair time commitment as it applies to the Customer's specific product configuration, location, and environment. This is established at the time of the support agreement order and is subject to resource availability.

Hardware onsite support

At the discretion of Hewlett Packard Enterprise, service will be provided using a combination of remote diagnosis and support, services delivered onsite, and other service delivery methods. Other service delivery methods may include the delivery via a courier of customer-replaceable parts such as a keyboard, a mouse, other parts classified as CSR parts, or an entire replacement product. HPE will determine the appropriate delivery method required to provide effective and timely Customer support.

An onsite response time will not apply if the service can be delivered using remote diagnosis, remote support, or other service delivery methods previously described.

Response times are dependent on the location of the Customer's site in relation to a designated Hewlett Packard Enterprise support office. To check service availability, the Customer should contact their local Hewlett Packard Enterprise Services representative.

For technical hardware issues that cannot, in Hewlett Packard Enterprise's judgment, be resolved remotely, an Hewlett Packard Enterprise authorized representative will provide onsite technical support on covered hardware products to return them to operating condition. For certain products, HPE may, at its sole discretion, elect to replace such products in lieu of repairing them. Replacement products are new or functionally equivalent to new in performance. Replaced products become the property of HPE.

Once an Hewlett Packard Enterprise authorized representative arrives at the Customer's site, the representative will continue to deliver the service, either onsite or remotely, at the discretion of HPE, until the products are repaired. Work may be temporarily suspended if parts or additional resources are required, but work will resume when they become available. Work to completion may not apply to onsite support provided for desktop, mobile, and consumer products. Repair is considered complete upon HPE verification that the hardware malfunction has been corrected or that the hardware has been replaced.

Notwithstanding anything to the contrary in this document or Hewlett Packard Enterprise's current standard sales terms, HPE will, for selected enterprise storage arrays and enterprise tape products, cover and replace defective or depleted batteries that are critical to the proper operation of the covered product.

For incidents with covered hardware that cannot be resolved remotely, Hewlett Packard Enterprise will use commercially reasonable efforts to respond onsite in accordance with the purchased hardware onsite reactive coverage level of the affected device.

Onsite response time specifies the period of time that begins when the initial call has been received and acknowledged by Hewlett Packard Enterprise, as described in the **General provisions/Other exclusions** section. The onsite response time ends when the Hewlett Packard Enterprise authorized representative arrives at the Customer's site, or when the reported event is closed with the explanation that HPE has determined it does not currently require onsite intervention.

Response times are measured during the coverage window only and may be carried over to the next day for which there exists a coverage window. Response time options available for eligible products are specified in the Service-level options table. All response times are subject to local availability. Contact a local Hewlett Packard Enterprise sales office for detailed information on service availability.

In the event that a CSR part is provided to return the system to operating condition, the onsite response time, if any, shall not apply. In such cases, Hewlett Packard Enterprise practice is to express ship to the Customer location the CSR parts that are critical to the product's operation. For more details on the CSR process and parts, please refer to: hpe.com/info/csr.

Software
For a Customer with multiple systems at the same location, Hewlett Packard Enterprise may limit the number of physical media sets containing software product and documentation updates provided as part of this service.

Software updates are not available for all software products. When this service feature is not available, it will not be included in this service.

For some products, software updates include only minor improved features. New software versions must be purchased separately.

Limitations to the defective media retention and comprehensive defective material retention service feature options
The defective media retention and comprehensive defective material retention service feature options apply only to eligible data retentive components replaced by Hewlett Packard Enterprise due to malfunction. They do not apply to any exchange of data retentive components that have not failed.

Data retentive components that are specified by Hewlett Packard Enterprise as consumable parts and/or have reached the maximum supported lifetime and/or the maximum usage limit as set forth in the manufacturer's operating manual, the product QuickSpecs, or the technical data sheet are not covered by this service.

Defective media retention service and comprehensive defective material retention service coverage for options designated by Hewlett Packard Enterprise as requiring separate coverage, if available, must be configured and purchased separately.

Failure rates on these components are constantly monitored, and Hewlett Packard Enterprise reserves the right to cancel this service with 30 days' notice if HPE reasonably believes that the Customer is overusing the defective media retention or comprehensive defective material retention service feature option (such as when replacement of defective data retentive components materially exceeds the standard failure rates for the system involved).

Service prerequisites

Hewlett Packard Enterprise, at its sole discretion, may require an audit on the covered products. If such an audit is required, an Hewlett Packard Enterprise authorized representative will contact the Customer, and the Customer will agree to arrange for an audit to be performed within the initial 30-day timeframe. During the audit, key system configuration information is collected and an inventory of the covered products is performed. The information gathered in the audit enables HPE to plan and maintain replacement part inventories at the appropriate level and location, and allows HPE to survey and troubleshoot possible future hardware incidents so that repairs can be completed as quickly and efficiently as possible. At the sole discretion of HPE, the audit may be performed onsite, via remote system access, via remote audit tools, or over the phone.

If an audit is required by Hewlett Packard Enterprise, it will take 30 days from the time this service is purchased to set up and perform the audits and processes that must be completed before the hardware call-to-repair time commitment can be put into effect. The hardware call-to-repair time commitment will not take effect until five (5) business days after the audit has been completed. Until such time, service for the covered hardware will be delivered at a 4-hour onsite response time service level.

In addition, Hewlett Packard Enterprise reserves the right to downgrade service to an onsite response time or cancel the service contract if critical audit suggestions are not followed or the audit is not performed within the specified timeframe, unless the delay is caused by HPE.

For hardware call-to-repair time commitments, Hewlett Packard Enterprise requires that all devices and configurations must be supported by Remote Support Technology and the Customer must install and operate the current version of Remote Support Technology with a secure connection to HPE, in order to enable the delivery of the service.

The installation and use of Remote Support Technology, including the installation and enabling of any agents and data transfer to Hewlett Packard Enterprise, is required to deliver the Firmware and Software Version Report, Proactive Scan Report, hardware call-to-repair time commitment, remote monitoring, and automated call logging deliverables of the HPE Proactive Care Advanced Service. During any such time that the Customer has not deployed Remote Support Technology, or if Customer configurations or devices are not supported by Remote Support Technology and the Customer does not take the steps necessary to provide the data required to HPE, HPE is not obligated to provide any impacted deliverables, and the Customer remains responsible for full payment of all fees associated with the provision of the HPE Proactive Care Advanced Service.

Installation of customer-installable firmware and software is the responsibility of the Customer. There will be additional charges if the Customer requests that Hewlett Packard Enterprise install customer-installable firmware and software updates. Any additional charges to the Customer will be on a time and materials basis, unless otherwise previously agreed to in writing by HPE and the Customer. To be eligible to purchase this service, the Customer must be properly licensed to use the revision of the software product that is current at the beginning of the support agreement period; otherwise, an additional charge may be applied to bring the Customer into service eligibility.

The Customer must have rightfully acquired the license for any underlying firmware that will be covered under these services.

Customer responsibilities

If the Customer does not act upon the specified Customer responsibilities, Hewlett Packard Enterprise or the Hewlett Packard Enterprise authorized service provider will, at HPE's discretion, i) not be obligated to deliver the services as described or ii) perform such service at the Customer's expense at the prevailing time and materials rates.

The Customer must provide accurate and complete information in a timely manner as required for Hewlett Packard Enterprise to perform the services.

For the proactive services provided by HPE Proactive Care Advanced Service, the Customer will provide HPE with the appropriate system manager contact information (name, email, and phone number) for the primary person responsible for the operational viability of the HPE Proactive Care Advanced covered infrastructure. The Customer will identify a focal point and an internal Customer team to work collaboratively with the Hewlett Packard Enterprise assigned ASM.

The call-to-repair time commitment is subject to the Customer providing immediate and unrestricted access to the system, as requested by Hewlett Packard Enterprise. The call-to-repair time commitment does not apply when system access, including physical, remote troubleshooting, and hardware diagnostic assessments, is delayed or denied. If the Customer requests scheduled service, the call-to-repair time period begins at the agreed-upon scheduled time.

Upon Hewlett Packard Enterprise request, the Customer will be required to support HPE's remote problem resolution efforts as well as proactive deliverables. The Customer will:

- Start self-tests and install and run other diagnostic tools and programs
- Install customer-installable firmware updates and patches
- Run data collection 'scripts' on behalf of Hewlett Packard Enterprise when they cannot be initiated from Remote Support Technology
- Provide all information necessary for Hewlett Packard Enterprise to deliver timely and professional remote support and to enable HPE to determine the level of support eligibility
- Perform other reasonable activities to help Hewlett Packard Enterprise identify or resolve problems, as requested by HPE

The Customer is responsible for installing and configuring all supported devices and maintaining the appropriate Remote Support Technology with a secure connection to Hewlett Packard Enterprise. The Customer is responsible for providing all necessary resources in accordance with the Remote Support Technology release notes in order to enable the delivery of the service and options. The Customer must also provide any hardware required to host Remote Support Technology. When an HPE remote support solution is installed, the Customer must also maintain the contact details configured in the version of Remote Support Technology that HPE will use in responding to a device failure. The Customer should contact a local Hewlett Packard Enterprise representative for further details on requirements, specifications, and exclusions. For scheduled calls, the Customer shall promptly make the equipment available to HPE for remedial activities at the agreed-upon time.

In cases where CSR parts or replacement products are shipped to resolve a problem, the Customer is responsible for returning the defective part or product within a time period designated by HPE. In the event that HPE does not receive the defective part or product within the designated time period or if the part or product is degaussed or otherwise physically damaged upon receipt, the Customer will be required to pay the HPE list price for the defective part or product, as determined by HPE.

In order for Hewlett Packard Enterprise to provide Collaborative Call Management, the Customer must have an active support agreement with the software vendor that includes the required service level and features that allow the Customer to place calls and receive support from the vendor. If the vendor requires it, the Customer will take any steps necessary to ensure that HPE can submit calls on the Customer's behalf. In addition, the Customer must provide HPE with the appropriate information needed for HPE to initiate a service call with the software vendor on behalf of the Customer. If the Customer does not meet these requirements, HPE will not be able to transfer calls to the vendor and assumes no responsibility for failure to do so. HPE's obligations are limited to the placement of support calls only. Purchase of Collaborative Call Management does not assign the support agreement between the Customer and vendor to HPE. The Customer remains responsible for the performance of their obligations under such agreements, which include payment of all applicable fees, including any fees that may apply as a result of logging calls with the vendor. HPE is not liable for the performance or non-performance of third-party vendors, their products, or their support services.

The Customer is responsible for installing, in a timely manner, critical customer-installable firmware updates, as well as CSR parts and replacement products delivered to the Customer.

The Customer is responsible for testing any preventative recommendations prior to implementation into production to ensure and to confirm interoperability within their IT environment. Prior to the implementation of any recommendations, the Customer should read and understand any prerequisites, procedures, or requirements as specified in the supporting documentation of the update.

The Customer shall work with Hewlett Packard Enterprise to schedule delivery of the HPE Proactive Care Advanced Service features identified for delivery for a specified number of times on an annual basis. Delivery shall be scheduled for each 12-month period of the annuity support agreement. No deliverables or entitlements shall be carried forward from one 12-month period to the next.

The Customer will:

- Take responsibility for registering to use the Hewlett Packard Enterprise or third-party vendor's electronic facility in order to access knowledge databases and obtain product information; HPE will provide registration information to the Customer as required; additionally, for certain products, the Customer may be required to accept vendor-specific terms for use of the electronic facility
- Retain and provide to Hewlett Packard Enterprise upon request all original software licenses, license agreements, license keys, and subscription service registration information, as applicable for this service
- Take responsibility for acting upon any hardcopy or email notification the Customer may receive in order to download the software update or to request the new software update on media, where this option is available
- Use all software products in accordance with current Hewlett Packard Enterprise software licensing terms corresponding to the Customer's prerequisite underlying software license, or in accordance with the current licensing terms of the third-party software manufacturer, if applicable, including any additional software licensing terms that may accompany such software updates provided under this service

If required by Hewlett Packard Enterprise, the Customer or Hewlett Packard Enterprise authorized representative must activate the hardware product to be supported within 10 days of purchase of this service, using the registration instructions within the Care Pack documentation or the email document provided by HPE, or as otherwise directed by HPE. In the event that a covered product changes location, activation and registration (or proper adjustment to existing HPE registration) is to occur within 10 days of the change.

The Customer is responsible for the security of the Customer's proprietary and confidential information. The Customer is responsible for properly sanitizing or removing data from products that may be replaced and returned to Hewlett Packard Enterprise as part of the repair process to ensure the safeguarding of the Customer's data. More information on Customer responsibilities, including those outlined in the HPE Media Sanitization Policy and Media Handling Policy for Healthcare Customers, can be found at hpe.com/mediahandling.

If the Customer chooses to retain repair parts covered under the defective media retention and/or comprehensive defective material retention service feature options, it is the Customer's responsibility to:

Retain covered data retentive components that are replaced during support delivery by Hewlett Packard Enterprise

Ensure that any Customer sensitive data on the retained covered data retentive component is destroyed or remains secure

- Have an authorized representative present to retain the defective data retentive component, accept the replacement component, provide Hewlett Packard Enterprise with identification information such as the serial number for each data retentive component retained hereunder, and, upon HPE request, execute a document provided by HPE acknowledging the retention of the data retentive component

- Destroy the retained data retentive component and/or ensure that is not put into use again
- Dispose of all retained data retentive components in compliance with applicable environmental laws and regulations

For data retentive components supplied by Hewlett Packard Enterprise to the Customer as loaner, rental, or lease products, the Customer will promptly return the replacement components at the expiration or termination of support with HPE. The Customer will be solely responsible for removing all sensitive data before returning any such loaned, rented, or leased components or products to HPE, and HPE shall not be responsible for maintaining the confidentiality or privacy of any sensitive data that remains on such components.

General provisions/Other exclusions

Hewlett Packard Enterprise will acknowledge a call by logging a case, communicating the case ID to the Customer, and confirming the Customer's incident severity and time requirements for the start of remedial action. Note: For events received via HPE electronic remote support solutions, HPE is required to contact the Customer, determine the incident severity with the Customer, and arrange access to the system before the hardware call-to-repair time or hardware onsite response time period can start.

Onsite hardware support response times and call-to-repair time commitments, as well as software support remote response times, may differ depending on incident severity. The Customer determines the incident severity level.

Incident severity levels are defined as follows:

Table 7. Incident severity levels

Severity 1	Critical Down	For example, the production environment is down; a production system or production application is down or at severe risk; data corruption, loss, or risk has occurred; business is severely affected; there are safety issues.
Severity 2	Critically Degraded	For example, the production environment is severely impaired; a production system or production application has been interrupted or compromised; there is risk of reoccurrence; there is significant impact on the business.
Severity 3	Normal	For example, a non-production system (e.g., test system) is down or degraded; a production system or production application has been degraded with a workaround in place; noncritical functionality has been lost; there is limited impact on the business.
Severity 4	Low	There is no business or user impact.

Ordering information

All units and options with individually sold support services must be ordered with the same service level as the product or enclosure that they are installed in, if that service level is available on those units.

HPE Proactive Care Advanced is not designed to be purchased on software-only configurations due to the integrated nature of the service deliverables. Thus, the software and hardware should be purchased with the same HPE Proactive Care Advanced service level.

Local availability: The Customer may order support from Hewlett Packard Enterprise's current support offerings. Some offerings, features, and coverage (and related products) may not be available in all countries or areas.

To order the service with the comprehensive defective material retention service feature, the defective media retention service feature must also be ordered.

To obtain further information or to order HPE Proactive Care Advanced Service, contact a local Hewlett Packard Enterprise sales representative or authorized Hewlett Packard Enterprise reseller and reference the following product numbers (x denotes the service length in years; options are 3, 4, or 5 years).

Table 8. HPE Proactive Care Advanced configurable/flexible support services

H8B33Ax	HPE Proactive Care ADV NBD SVC
H8B34Ax	HPE Proactive Care ADV NBD wDMR SVC
H8B35Ax	HPE Proactive Care ADV 24x7 SVC
H8B36Ax	HPE Proactive Care ADV 24x7 wDMR SVC
H8B37Ax	HPE Proactive Care ADV CTR SVC
H8B38Ax	HPE Proactive Care ADV CTR wDMR SVC

Table 9. HPE Proactive Care Advanced Contractual services

H8B33AC	HPE Proactive Care ADV NBD SVC
H8B34AC	HPE Proactive Care ADV NBD wDMR SVC
H8B35AC	HPE Proactive Care ADV 24x7 SVC
H8B36AC	HPE Proactive Care ADV 24x7 wDMR SVC
H8B37AC	HPE Proactive Care ADV CTR SVC
H8B38AC	HPE Proactive Care ADV CTR wDMR SVC

For the complete list of HPE Proactive Care Advanced non-configurable/fixed support services, please contact your local Hewlett Packard Enterprise sales representative or Hewlett Packard Enterprise reseller.

Resources

Insight Remote Support release notes:
hpe.com/services/getconnected

HPE Proactive Care Advanced supported products list:
hpe.com/services/proactivecareadvancedsupportedproducts

Software Product List Collaborative Support provided by HPE:
hpe.com/services/collaborativesupport

HPE Proactive Select Services:
hpe.com/services/proactiveselect

HPE Support Center:
hpe.com/support/hpesc

HPE Media Sanitization Policy and Media Handling Policy:
hpe.com/mediahandling

HPE Comprehensive Defective Material Retention:
hpe.com/services/cdmr

Customer Self-Repair information:
hpe.com/info/csr

For more information

For more information on HPE Proactive Care Advanced Service or other support services, contact any of our worldwide sales offices.

Learn more at
hpe.com/services/support

Hewlett Packard Enterprise

4AA5-3259ENW, December 2015, Rev. 1

HP Datacenter Care Service

HP Technology Services Contractual Services

HP Datacenter Care Service is HP's most comprehensive support solution tailored to meet your specific data center support requirements. It offers a wide choice of proactive and reactive service levels to cover requirements ranging from the most basic to the most business-critical environments. HP Datacenter Care Service is designed to scale to any size and type of data center environment while providing a single point of contact for all your support needs for HP as well as selected multivendor products. The service is delivered under the governance of an assigned HP support team that is familiar with your IT environment and understands how it enables your company's business. A mutually agreed upon and executed Statement of Work (SOW) will detail the precise combination of reactive and proactive support features that will be provided under HP Datacenter Care Service based upon your requirements.

You can use HP Datacenter Care Service to complement your organization's own skills and capabilities by mixing and matching any of HP's support offerings with different elements of your IT solution or data center based on the role and importance of the particular products. IT environments are becoming increasingly diverse, combining low-cost virtualized and bladed technology deployed alongside more traditional high-end products—each of which can have very different reactive support needs. (Note that IT environment, as defined by HP, is the IT infrastructure supported by HP Datacenter Care Service, under the direct day-to-day management of one IT organization, in one country, and as detailed in the SOW.) HP Datacenter Care Service is designed to meet a wide range of support requirements.

Regardless of the level of routine reactive support you chose for specific products in your IT infrastructure, the end-to-end IT services they support can be crucial to your overall business. When the unexpected happens, you may still need rapid escalation and incident resolution. In the event of a service incident, HP Datacenter Care Service provides access to HP technical solution specialists who can help you to resolve critical issues as quickly as possible. HP employs accelerated escalation procedures to resolve complex incidents. In addition, your support team of HP specialists is equipped with remote technologies and tools designed to reduce downtime and increase productivity.

A set of optional proactive services, ranging from technology-specific activities such as firmware and OS patch analysis/recommendations and change management support, to a systematic approach to continual improvement based on IT service management (ITSM) and HP best practices, including IT Infrastructure Library (ITIL) and ISO/IEC 20000, have been designed to augment the skills of your own IT staff and complement reactive support options. These proactive services are designed to provide flexible choices and are customized to support different components of a solution or different areas within your data center.

HP Datacenter Care Service is designed to augment your own capabilities; help you reduce risks across people, processes, and technology; increase IT service quality and productivity; and reduce costs.

The service includes an assigned account team led by a trained HP Account Support Manager (ASM). The team's goal is to form a close working relationship with designated members of your IT staff and gain a clear understanding of your business objectives, key service-level agreements (SLAs), and the key performance indicators (KPIs) you need to meet. Delivery of the various support options you have chosen will be overseen by the ASM and directed at meeting your goals.

The flexibility and customization available with HP Datacenter Care Service provides you with a cost-effective support solution tailored to your unique needs.

Datacenter Care also provides the following optional extensions:

- HP Flexible Capacity
- HP Datacenter Care Operational Support Services
- HP Datacenter Care for Multivendor
- HP Datacenter Care for Cloud
- HP Datacenter Care—Infrastructure Automation
- HP Datacenter Care for SAP

HP Flexible Capacity

HP Flexible Capacity (FC) is an infrastructure utility service based on the converged infrastructure of HP server, storage, and networking equipment installed at your site that is billed based on usage and allows you to procure and pay for your capacity needs on a variable monthly usage basis, subject to minimum usage requirements. For detailed information on this extension, refer to the HP Datacenter Care Flexible Capacity Service data sheet addendum.

HP Datacenter Care Operational Support Services

Operational Support Services (OSS) provides HP best practices for operating on-premise infrastructure by delivering 24x7 remote infrastructure monitoring and operational services. The service addresses the service operations stage of the infrastructure, servers, storage, networking, operating system, hypervisor, and backup and restore, and security throughout the IT service lifecycle. For detailed

information, refer to the HP Datacenter Care Operational Support Services (OSS) data sheet addendum.

HP Datacenter Care for Multivendor

HP Datacenter Care for Multivendor extends HP caliber single-source capabilities across the heterogeneous IT environment. Datacenter Care for Multivendor gives you a single point of accountability across hardware and operating environments from multiple eligible vendors. This simplifies service management and problem resolution across your entire data center. For detailed information on this extension, refer to the HP Datacenter Care for Multivendor data sheet addendum.

HP Datacenter Care for Cloud

HP Datacenter Care for Cloud is a version of HP Datacenter Care developed to address the needs of complex private and hybrid cloud environments that is built on the HP CloudSystem infrastructure and HP cloud management software. A primary feature of Datacenter Care for Cloud is its linkage to, and collaboration with, your HP Software Premier Support plan. Optional features and services can be added to accommodate public cloud service providers, pay-per-use pricing, multivendor management, and more. For detailed information on this extension, refer to the HP Datacenter Care for Cloud data sheet addendum.

HP Datacenter Care–Infrastructure Automation

HP Datacenter Care—Infrastructure Automation is an extension of HP Datacenter Care that lets you configure and operate your data center in a new way to help realize the potential of the software-defined data center. With Datacenter Care—Infrastructure Automation, the data center is treated as software that can be designed, documented, version controlled, tested, and deployed using the same tools and processes software developers use. Datacenter Care—Infrastructure Automation is designed to provide the technical advice, process, and tools needed to automate the data center, including eligible multivendor products. For detailed information on this extension, refer to the HP Datacenter Care—Infrastructure Automation data sheet addendum.

HP Datacenter Care for SAP

Systems running SAP products are critical to business outcomes and play an integral part in meeting strategic objectives. To assist you in helping to realize a sustained benefit from your SAP investment, HP provides a Datacenter Care enhancement for SAP. This service enhancement can help you achieve your operational and technical goals as efficiently as possible. For detailed information on this extension, refer to the HP Datacenter Care for SAP data sheet addendum.

Service benefits

HP Datacenter Care Service is designed to help you consistently meet your service-level targets and other business objectives by providing:

- A cost-effective support solution tailored to your exact requirements and addressing the various technologies deployed across your IT solutions and data center
- Proactive issue identification and advice on mitigation of risks
- Access to HP specialists that can augment your own capabilities, with the overall goal to help you reduce risk, increase productivity, and address peak workloads and emerging projects
- Flexible reactive support options that enable you to choose from any of HP's reactive levels, ranging from next business day through to call-to-repair and higher, and allocate them to products according to their role in your solutions
- Consistent and reliable remote support with active end-to-end case management and reporting to help avoid the unnecessary escalation of routine issues
- Fast connection to HP technical specialists who can help you rapidly address any critical issues and achieve quicker resolution
- Flexible proactive support options, delivered by HP specialists, who complement your own capabilities and can help you focus on innovation
- Advanced remote technologies and tools designed to reduce downtime and increase productivity
- An assigned account team focused on your IT environment and business objectives that provides a single point of contact within HP, helps to ensure that your relationship with HP meets your expectations, and verifies delivery of all service options as agreed upon
- Access to HP IT Service Management (ITSM) experts and knowledge built on ITSM best practices, like IT Infrastructure Library (ITIL) v3, ISO/IEC 20000, and so on, which can help provide the ability to improve your IT operation through a formal continual improvement process

Service feature highlights

Table 1. Core features

Core features include the following:

- Relationship management, which includes:
  - Assigned account team
  - Account support plan
  - Site survey
  - Support planning and review
  - Support activity review
  - HP support center
  - HP educational planning and assistance
- Enhanced call handling, which includes:
  - Rapid response to critical hardware and software incidents (24x7)
  - Accelerated escalation management
  - Remote hardware and software incident diagnosis and support
  - HP Electronic Remote Support Solution
  - Assistance on non-HP software products
  - Access to electronic support information and services

Table 2. Optional proactive features

Optional features include the following:

- Environment services, which includes:
  - HP Proactive Select Service credits
  - HP education credits
  - Operational and technical advice
  - Assistance with the implementation of changes and improvements
  - HP Technical Account Manager (TAM) enhancement
  - Assigned business critical consultant (BCC)
  - Customer vision and goal setting
  - Business planning and review
  - Risk identification and benchmarking
  - Service improvement planning
  - Improvement scorecard
  - Service failure analysis
  - ISO/IEC 20000 certification assistance
- Server services, which includes:
  - Operating system patch analysis and management
  - Server firmware and software analysis and management
  - System health check
  - Proactive Scan Assessment
  - Firmware and Software Version Report and recommendations
  - Enhancement for SAP
- Storage services, which includes:
  - Storage firmware and software analysis and management
  - Storage high-availability technical assessment
  - Storage array preventive maintenance
- SAN services, which includes:
  - SAN firmware and software analysis and management
  - SAN supportability assessment
- Network services:
  - Network firmware and software analysis and management
  - Network critical incident notification
  - Network asset report
  - Open network environment support

Service feature highlights *continued*

Table 3. Optional reactive features

Optional features include the following:

- Default service coverage window (24x7)
- Default hardware reactive support features, which includes:
  - Onsite hardware support
  - 4-hour onsite response
  - Replacement parts and materials
  - Work to completion
- Default software reactive support features, which includes:
  - Non-critical software response
  - Software product and documentation updates
  - License to use software updates
  - HP recommended software and documentation updates method
- Optional hardware reactive support features, which includes:
  - Collaborative call management on non-HP products
  - 6-hour call-to-repair time commitment
  - Upfront audit
  - Enhanced parts inventory management
  - Dedicated parts inventory
  - Defective media retention
  - Comprehensive defective material retention

Table 4. Service-level options

Coverage window includes the following:

- Default service coverage window, which includes:
  - 24 hours, seven days a week (24x7)
- Coverage window options, which include:
  - Standard business hours, standard business days (9x5)
  - 13 hours, standard business days (13x5)
  - 16 hours, standard business days (16x5)
  - 24 hours, standard business days (24x5)
  - Coverage extension for additional hours
  - Coverage extension for additional days
  - Coverage window under separate HP contract or HP warranty

Hardware reactive support options

- Onsite response time for hardware support
- Onsite response time options, which include:
  - 2-hour onsite response
  - 4-hour onsite response
  - Next-day onsite response
  - Contracted service that may be under separate HP contract or HP warranty
- Hardware call-to-repair time commitment (in lieu of hardware onsite response time options)
- Hardware call-to-repair time commitment options, which include:
  - 4-hour call-to-repair time
  - 6-hour call-to-repair time
  - 8-hour call-to-repair time
  - 24-hour call-to-repair time
  - Contracted service that may be under separate HP contract or HP warranty

Service feature highlights *continued*

Table 5. Call-to-restoration upgrade enhancement option

Proactive features include the following:	Reactive features include the following:
• Call-to-restoration upgrade enhancement • ITSM assessment • Upfront audit • Daily screen for critical patches • Monthly support reviews • Semi-monthly operating system patch analysis and management • Delivery process reviews • Configuration checkup • HP Proactive Select Service credits	– 4-hour call-to-restoration commitment – Problem resolution verification – Dedicated parts inventory – Customized escalation process

Specification

Table 1. Core features

Feature or service	Delivery specifications
Core features	**The core features of this offering may include the following:**
Relationship management, which includes:	HP Datacenter Care Service relationship management includes an assigned HP account team that understands the Customer's business and IT objectives and works to ensure that these needs are met. The features of relationship management are described in the text that follows.
Assigned account team	HP assigns an account team to the Customer's organization. Members of the HP assigned account team are: • Account Support Manager (ASM) • Technical Account Manager (TAM) • Datacenter Hardware Specialist (DHS) The HP account team is the Customer's advocate and technical focal point for the ongoing support of the IT environment covered by HP Datacenter Care Service. To help meet the Customer's objectives, the team works with the Customer to develop—and routinely review—a mutually agreed-upon account support plan. Additional activities may include: • Conduction of support planning and review meetings, and support activity reviews • Coordination of optional proactive activities and additional HP resources when specific skills are needed (such as storage/SAN or network specialists) • Monitoring of issues, patches, and advisories that could impact the Customer's environment • Service activity reporting and incident trending • Review of HP hardware advisory notifications
Account support plan	The ASM develops an account support plan in conjunction with the Customer's IT staff and documents the necessary combination of reactive and proactive support, devices, geographic coverage, and any other support aspects provided by HP Datacenter Care Service. The account support plan also details roles and responsibilities along with contact information and escalation procedures, and will be formally confirmed with the Customer as part of the startup phase of this service.
Site survey	At the beginning of the HP Datacenter Care Service support period, HP performs a survey to obtain a detailed inventory of the Customer's hardware and software and to record hardware and OS configuration information. This information furthers HP's troubleshooting processes, supports the Customer's daily operations, and assists with planning efforts. HP documents technical configuration information in the account support plan and makes it available on the HP document repository, **www.hp.com/go/esmg**, for reference by both HP and the Customer.

Specification

Table 1. Core features *continued*

Feature or service	Delivery specifications
Core features	**The core features of this offering may include the following:**
Support planning and review	The ASM conducts quarterly (or the timeframe agreed in the SOW) onsite support planning and review sessions during which the Customer and the ASM review the support provided by HP over the previous period, including key topics arising from the support activity report and the outcome of HP Datacenter Care Service activities. These reviews also provide an opportunity to discuss trends, any current or planned changes to the Customer's IT environment and business, and the impact of these changes on the Customer's support requirements. Any additional support requirements can also be identified and discussed. These review sessions provide an open communication forum not only to help the Customer share the Customer organization's business and IT goals, but also to help keep the service aligned with the Customer's needs on an ongoing basis. During these review sessions, the HP account team can share HP best practices and provide IT operational and technical advice related to the Customer's current and future operational needs and projects. Members of the HP account team may participate in these meetings, as determined by the ASM.
Support activity review	HP provides the Customer with a quarterly (or the timeframe agreed in the SOW) support activity review report that documents reactive support call information during that specific period. The report highlights potential risk factors and includes appropriate recommendations.
HP support center	HP provides a comprehensive online resource for instant customized knowledge, tools, and services. This one-stop IT site offers self-solve tools; personalized, reliable assistance; online help and forums; and instant access to comprehensive multivendor and multiplatform IT content.
HP educational planning and assistance	If requested, the ASM can conduct a high-level review of the Customer's training and development needs. The ASM can also provide assistance in contacting HP Customer Education. The Customer may access training curricula and detailed course descriptions on the HP Education Services website at **www.hp.com/learn**. As a separate optional activity, the HP Education Services team can help develop customized courses or end-to-end learning solutions that are tailored to the Customer's specific training requirements.
Enhanced Call Handling, which includes:	Enhanced Call Handling is a set of integrated and accelerated reactive processes designed to address hardware and software incidents. These processes, which are custom tailored to the needs of the Customer, engage appropriate HP technical specialists to help address critical covered support incidents for quicker resolution. The features of Enhanced Call Handling are described below.
Rapid response to critical hardware and software incidents (24x7)	The Customer can contact HP 24 hours a day, 7 days a week. When the Customer calls with a critical incident, HP aims to either connect the Customer to a technical solution specialist (TSS) or call the Customer back within 15 minutes. The TSS is trained to address issues in complex computing environments and has access to HP's full array of technical knowledge and resources to assist in diagnosing and resolving issues as quickly as possible. In the event of a hardware issue requiring an onsite presence, a hardware specialist is dispatched to the Customer's site in accordance with the purchased hardware onsite reactive service coverage level for that affected device. In addition to providing initial troubleshooting, the TSS performs failure data collection and incident definition, employing rigorous case management and escalation procedures, and engaging additional technical specialists as needed. For critical incidents, HP may provide a post-incident review at its discretion. This activity helps to identify any improvements that could be made by the Customer or HP in order to avoid the occurrence of similar incidents in the future, or to improve subsequent incident handling. Incident severity levels are defined in 'General provisions.'
Accelerated escalation management	HP employs integrated, accelerated escalation procedures to address complex covered support incidents for quicker resolution. For critical incidents, a critical event manager (CEM) is assigned. If the situation requires additional resources or skills, the CEM coordinates incident escalation and rapidly enlists key incident solving specialists throughout HP. Incident severity levels are defined in 'General provisions.'
Remote hardware and software incident diagnosis and support	Once the Customer has placed a service request call and HP has acknowledged (for more details, see the 'General provisions' section) receipt of the call, HP will work during the hardware or software coverage window to isolate the hardware or software problem and to remotely troubleshoot, remedy, and resolve the problem with the Customer. Prior to any onsite assistance, HP may initiate and perform remote diagnostic tests using HP Insight Remote Support to access covered products, or use other means available to facilitate remote problem resolution. Incidents with covered hardware or software can be reported to HP via telephone or Web portal, as locally available, or via HP Insight Remote Support as an automated equipment reporting event 24 hours per day, Monday through Sunday. HP will acknowledge the receipt of the service request by logging the call, assigning a case ID, and communicating that case ID to the Customer. HP retains the right to determine the final resolution of all reported problems.
HP electronic remote support solution	For eligible products, the HP electronic remote support solution provides robust troubleshooting and repair capabilities. It can include remote system access solutions and may offer a convenient central point of administration and an enterprise view of open incidents and history. An HP support specialist will only use the remote system access with the Customer's authorization. The remote system access may enable the HP support specialist to provide more efficient troubleshooting and faster problem resolution.

Specification

Table 1. Core features *continued*

Feature or service	Delivery specifications
Core features	**The core features of this offering may include the following:**
Assistance on non-HP software products	If, during the course of problem resolution on supported products the problem is found to exist due to another vendor's product, HP will (where possible) assist the Customer in forwarding the problem to that vendor, provided that the Customer has a valid support agreement with the other vendor. If requested by the Customer, HP may provide collaborative problem call management for selected vendor products. These products are critical to providing solution support and HP support for them is unavailable. The following vendor products are covered: • SAP (all products)—The Customer must have purchased an SAP support agreement from SAP. • Oracle (Oracle Database products and Solaris OS only)—The Customer must have purchased an Oracle Support Agreement from Oracle. The level of HP collaboration with the vendor is dependent on the Customer's service level with that vendor.
Access to electronic support information and services	As part of this service, HP provides the Customer with access to certain commercially available electronic and Web-based tools. The Customer has access to: • Certain capabilities made available to registered users with linked entitlements, such as downloading selected HP software patches and firmware updates, subscribing to hardware-related proactive service notifications, and participating in support forums for solving problems and sharing best practices with other registered users • Expanded Web-based searches of technical support documents to facilitate faster problem-solving • Certain HP proprietary service diagnostic tools with password access • A Web-based tool for submitting questions directly to HP; the tool helps to resolve problems quickly with a pre-qualification process that routes the support or service request to the resource qualified to answer the question; the tool also allows the status of each support or service request submitted to be viewed, including cases submitted by telephone • HP and third-party hosted knowledge databases for certain third-party products, where Customers can search for and retrieve product information, find answers to support questions, participate in support forums, and download software updates; this service may be limited by third-party access restrictions • The Software Updates and Licensing portal, which provides the Customer with electronic access to receive, proactively manage, and plan for software product updates; access to the portal is through the HP Support Center

Specifications

Table 2. Optional proactive features

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected. Supplementary agreed-upon services are provided during normal HP business hours unless after-hours assistance has been purchased. Please contact a local HP representative for further details.**
General description of optional proactive features	HP Datacenter Care Service contains a comprehensive set of optional proactive services to support the Customer and their business objectives. These can be chosen to augment the Customer's own capabilities and will be documented and confirmed in the account support plan.
Environment services, which includes:	The Customer may choose any of the following environment services options to meet the Customer's service-level targets and other business objectives.
HP Proactive Select Service credits	This option provides 10 Proactive Select Service credits. The Customer has the flexibility to choose an activity from the predefined Proactive Select services menu, or to work with the ASM to define a custom activity based on the Customer's needs. See table 13 for more detailed information.
HP Education Services credits	The Customer may purchase credits for HP Education Services to allow staff members to expand and strengthen their technical and process knowledge. Please contact a local HP representative for further details.
Operational and technical advice	The HP account team takes an active role in providing advice and guidance regarding the routine delivery of the Customer's critical IT services and the running of service management processes and technology. As requested by the Customer, the HP account team can provide help in performing activities such as technical change reviews and reviewing event thresholds in monitoring tools.

Specifications

Table 2. Optional proactive features *continued*

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected. Supplementary agreed-upon services are provided during normal HP business hours unless after-hours assistance has been purchased. Please contact a local HP representative for further details.**
Assistance with the implementation of changes and improvements	The HP account team works with the Customer to help design and implement changes and improvements to address any shortcomings during the ongoing service and review meetings.
HP Technical Account Manager (TAM) enhancement	The assigned Technical Account Manager (TAM), who is part of the assigned account team, may address in greater depth the IT operations that add value to the Customer's business. The assigned TAM can also provide additional environmental system health checks, activity and trend reporting, detailed technical assistance, and best practice recommendations. The TAM is available Monday through Friday during standard HP business hours, excluding HP holidays.
Assigned business-critical consultant (BCC)	An ITIL-certified business-critical consultant (BCC) is a specialist in availability, who can be assigned to the Customer's IT staff to identify and reduce risks from technology, people, and processes, and to help the Customer meet their business objectives.
Customer vision and goal setting	The HP account team conducts a vision and goal-setting workshop with the Customer to identify business objectives and IT infrastructure goals as well as the key SLAs and KPIs. During this workshop, HP will document the scope of HP Datacenter Care Service as it relates to the Customer's IT services, people, processes, and technology.
Business planning and review	The ASM holds semiannual (or the timeframe agreed in the SOW) business planning and review meetings to help align the activities of the HP account team with any changing business requirements and any new technology or IT services. The ASM documents changes to the Customer's vision and long-term goals, and discusses any impact on the scope of HP Datacenter Care Service and the account support plan. This activity helps the HP account team and other HP resources maintain an understanding of the Customer's needs during the delivery of this service.
Risk identification and benchmarking	The HP account team designs a customized ITSM assessment based on the scope of the HP Datacenter Care Service and important objectives identified during the service's Customer vision and goal-setting workshop or similar discussion with the Customer. The HP account team performs this customized assessment to identify gaps in capability and opportunities for improvement, and then reviews the assessment findings with the Customer and creates an agreed-upon benchmark of the Customer's current level of risk, maturity, efficiency, and effectiveness. This benchmark compares the Customer's capabilities with industry best practices and the demands of the Customer's SLAs and business objectives.
Service improvement planning	The HP account team creates a service improvement plan (SIP). As part of the risk identification and benchmarking activity, the HP account team performs a customized ITSM assessment. The HP account team discusses the output of this gap analysis with the Customer to identify any weaknesses or opportunities for improvement and helps the Customer create an SIP that reflects the Customer's priorities and recommended activities to address the identified risks through a combination of proactive activities from HP and the Customer's IT staff. Once the SIP has been developed, the HP account team helps the Customer to manage this plan on a quarterly basis by providing advice and guidance in the implementation of improvements. The HP account team also assists the Customer in reviewing and prioritizing new improvements for inclusion in the SIP. Note that the service improvement planning option requires the risk identification and benchmarking option as a prerequisite.
Improvement scorecard	The HP account team works with the Customer to identify and/or design improvement metrics, reporting mechanisms, and an improvement scorecard that will allow the Customer to formally track the improvements made to the Customer's IT services, people, process, and technology. The HP account team then provides quarterly input to help the Customer update the improvement scorecard using improvement data identified during HP Datacenter Care Service activity and SIP review meetings. Note that the improvement scorecard option requires the service improvement planning option as a prerequisite.
Service failure analysis	The HP account team works with the Customer and provides recommendations on how to reduce the business impact of IT service failures in the Customer's environment. The analysis identifies the underlying causes of the Customer's IT service interruptions and details how each contributed to the business impact. The service failure analysis also identifies opportunities to improve the Customer's processes and tools. The HP account team then documents the issues and related learning in the Customer's SIP. The analysis can also be used to investigate removing the need for or reducing the length or impact of Customer planned downtime. Note that the service failure analysis option requires the service improvement planning option as a prerequisite.

Specifications

Table 2. Optional proactive features *continued*

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected. Supplementary agreed-upon services are provided during normal HP business hours unless after-hours assistance has been purchased. Please contact a local HP representative for further details.**
ISO/IEC 20000 certification assistance	The proactive activities of HP Datacenter Care Service can be tailored to help the Customer implement the best practices defined in ISO/IEC 20000, the international standard for IT service management. HP may offer the Customer advice and guidance to help the Customer achieve formal ISO/IEC 20000 certification, if that is one of the Customer's goals. The ITSM assessment included with the risk identification and benchmarking activity is scoped to identify gaps in ISO/IEC 20000 compliance, and appropriate improvements are included for prioritization within the SIP. Progress in the plan is discussed during the SIP review meetings. Note that the ISO/IEC 20000 certification assistance option requires the SIP option as a prerequisite.
Server services, which includes:	The Customer may choose any of the following server services options to meet service-level targets and other business objectives:
Operating system patch analysis and management	For HP-UX, MPE, Tru64 UNIX®, NonStop Kernel, and OpenVMS, HP monitors patch notifications for known critical defects in the OS or previously released patches, evaluates whether the defect may impact the covered environment, and, if warranted, notifies the Customer to discuss possible actions. The number of OSs, hypervisors, and servers to be supported will be documented and confirmed in the account support plan. Quarterly (or the timeframe agreed in the SOW), the Customer and the HP account team discuss the recommended patches. The HP account team makes recommendations to assist with the change management considerations: • For HP-UX and NonStop proprietary OSs, HP provides a customized bundle and report of the recommended patches for Customer installation. • For Tru64 UNIX and OpenVMS OSs, HP provides a customized report of the recommended patches for Customer installation. • For MPE proprietary OSs, HP will provide the latest Power Patch bundle of the recommended patches for Customer installation. • For Microsoft® OSs, HP delivers a written Microsoft service pack briefing, which addresses the features of the latest Microsoft OS and server application service packs. HP also provides monthly (or the timeframe agreed in the SOW) notification on Microsoft security releases and quarterly (or the timeframe agreed in the SOW) notification on HP-Microsoft supported products, applicable to servers outlined in the Customer's account support plan. • For the Linux OS, HP reviews Linux patch notifications from Linux suppliers and provides recommendations of patches that are applicable to the Customer's environment based on Red Hat and SUSE Linux versions for Customer installation. • For VMware and Microsoft Hyper-V hypervisors, HP reviews patch notifications from the suppliers and provides recommendations of patches that are applicable to the Customer's environment.
Server firmware and software analysis and management	Periodically, HP releases firmware updates for servers. These updates may address potential incidents, provide added functionality, or improve performance. In addition to providing proper planning to reduce disruption to the Customer's operations, HP can also provide appropriate updates. Quarterly (or the timeframe agreed in the SOW), the Customer and HP discuss recommended updates. The number of servers to be supported will be documented and confirmed in the account support plan. Onsite installation is also provided for firmware defined by HP as non-customer-installable. HP installs these firmware updates, if requested by the Customer, either during the HP standard business hours or during HP non-standard business hours at no additional charge to the Customer. HP provides telephone assistance for the installation of customer-installable firmware, if requested by the Customer, during the service coverage window.
System health check	HP uses diagnostic tools to assess the computing environment for a single operating system on a single physical server or partition. HP performs a series of diagnostic tests to compare the Customer's computing environment to accepted system management practices and provides a report that details the findings, highlighting the conditions that require resolution or investigation and recommending a suitable course of action. The number and frequency of system health checks to be deployed and the number of servers to be supported will be documented and confirmed in the account support plan.
Proactive Scan Assessment	Twice yearly or quarterly as agreed to in the SOW, HP performs a proactive scan of Datacenter Care supported devices in the Customer's computing environment. Products to be reviewed should be listed in the Datacenter Care SOW. For HP servers and certain storage and networking products, this service provides a technical device assessment that is designed to help identify potential system configuration problems before they impact the Customer's business operations. HP Remote Support Technology tools are used to collect, transport, and analyze configuration and revision data to identify trends, revisions, or parameters that may impact operation. This analysis uses diagnostic tools and processes to compare the devices to HP management best practices or support advisories. HP then prepares a report that details the findings and highlights the potential risks and issues, identifying deviations from HP best practices, based upon output from the tools, along with HP's recommendations for further action by the Customer intended to help address or further investigate them. The Datacenter Care account team is available on request during standard HP business hours to discuss the implications and HP's recommendations with the Customer. Implementation of the recommendations is the Customer's responsibility; however, additional assistance can be purchased from HP to implement the recommendations. Note: Devices that are capable of remote data collection and/or monitoring, need to actively connect to HP in order to receive Proactive Scan reports. If an HP device does not support remote data collection and/or monitoring, HP will provide an alternative reporting solution, where possible.

Specifications

Table 2. Optional proactive features *continued*

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected. Supplementary agreed-upon services are provided during normal HP business hours unless after-hours assistance has been purchased. Please contact a local HP representative for further details.**
Firmware and Software Version Report and recommendations	IT reliability and stability can be impacted by the levels of the Customer's software and firmware revisions. Twice yearly or quarterly as agreed to in the SOW, HP reviews products under the Datacenter Care contract to verify that they are at recommended revision levels. Products to be reviewed should be listed in the Datacenter Care SOW. HP provides the Customer with a report containing its recommendations for applicable software versions, patches, and firmware revisions for each covered device. The Datacenter Care account team is available on request during standard HP business hours to discuss the implications and HP's recommendations with the Customer. Implementation of the recommendations is the Customer's responsibility; however, additional assistance can be purchased from HP to implement the recommendations. As part of the firmware and software version recommendation activity, HP performs the following core deliverables using the HP Remote Support Technology tool suite. **Firmware Version Recommendations** For HP BladeSystem environments and HP ProLiant servers, the firmware analysis includes the enclosure and all the components within the enclosure covered by Datacenter Care, including server and storage blades, power and cooling components, networking, interconnects, and HP Virtual Connect technology. For storage and network devices, the firmware analysis includes any HP supported devices covered by the Datacenter Care contract. If requested by the Customer, HP will provide onsite installation during standard business hours for firmware that is defined by HP as non-customer installable and which cannot be installed remotely. HP can provide telephone support for firmware defined as customer installable during the related hardware device support coverage window. The Customer can purchase additional services to install customer-installable firmware. **Software Version Recommendations** HP will provide the Customer with patch analysis and update recommendations for all supported server operating systems, virtualization software, or software required to operate a storage device that are covered under Datacenter Care support. Update recommendations are provided by comparing the Customer's current version information against the latest supported releases, and indicating whether the current installed version is the latest release. This provides the Customer with HP's general recommendations, which are intended to address critical gaps with individual devices or products. HP can provide telephone assistance, if requested, to help with the installation of software patches for supported software. The Customer can purchase additional services to install supported software revisions and patches. For operating systems, virtualization software, or software required to operate a storage device that is not directly covered by a Datacenter Care agreement but is running on an underlying server or storage device covered by Datacenter Care support, HP will provide only one annual software update notification. For operating systems and virtualization software, please consult an HP representative for details on supported products.
Enhancement for SAP	Systems running SAP products are critical to business outcomes and play an integral part in meeting strategic objectives. This service enhancement is designed to help customers achieve their operational and technical goals as efficiently as possible. For detailed information on this extension, refer to the HP Datacenter Care for SAP data sheet addendum.
Storage services, which includes:	The Customer may choose any of the following storage services options to meet service-level targets and other business objectives:
Storage firmware and software analysis and management	On a quarterly basis (or the timeframe agreed in the SOW), HP analyzes for potential storage-related software and firmware updates. The HP account team provides a recommendation as to applicable software and firmware updates as well as upgrade-planning assistance for the recommendations. Onsite installation is also provided for firmware and embedded storage device-resident software updates defined by HP as non-customer installable. HP will install these updates, if requested by the Customer, either during standard HP business hours or outside standard HP business hours at no additional charge to the Customer. HP will provide telephone assistance for the installation of customer-installable firmware and software, if requested by the Customer, during the service coverage window. The number of storage products to be supported will be documented and confirmed in the account support plan.
Storage high-availability technical assessment	HP performs a high-availability assessment on one storage array. The assessment includes an analysis of the physical environment, the array's configuration, and its firmware and software versions. The connectivity of the array to the SAN is examined for interoperability and availability. HP interviews the Customer's IT staff to assess usage of ITIL best practices for storage management. Upon completion of the assessment, HP provides the Customer with a report and a briefing on the findings and recommendations. The number and frequency of storage assessments are documented and agreed to in the account support plan.
Storage array preventive maintenance	For the HP XP and P9000 disk array product family, HP proactively provides an annual (or the timeframe agreed in the SOW) onsite visit at a mutually agreed-upon time. During these visits, a hardware specialist performs preventive maintenance of electronic system components in accordance with the operational specifications of the storage array.

Specifications

Table 2. Optional proactive features *continued*

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected. Supplementary agreed-upon services are provided during normal HP business hours unless after-hours assistance has been purchased. Please contact a local HP representative for further details.**
SAN services, which includes:	The Customer may choose any of the following SAN services options to meet their service-level targets and other business objectives:
SAN firmware and software analysis and management	On a quarterly basis (or the timeframe agreed in the SOW), HP analyzes for potential SAN-related software and firmware updates. The HP account team provides a recommendation as to applicable software and firmware updates as well as upgrade planning assistance for the recommendations. Onsite installation is also provided for firmware and embedded SAN device-resident software updates defined by HP as non-customer installable. HP will install these updates, if requested by the Customer, either during standard HP business hours or outside standard HP business hours at no additional charge to the Customer. HP will provide telephone assistance for the installation of customer-installable firmware and software, if requested by the Customer, during the service coverage window. The number of SAN products to be supported will be documented and agreed in the account support plan.
SAN supportability assessment	HP assesses the supportability of the Customer's SAN. Issues with the potential to impact stability or supportability are identified and change recommendations are made. An initial SAN supportability assessment is included the first time SAN support is selected. The assessment is updated in each subsequent year for which SAN support is continued.
Network services, which includes:	The Customer may choose any of the following Network services options to meet their service-level targets and other business objectives:
Network firmware and software analysis and management	New releases of network firmware and software updates from HP and from organizations for which HP is an authorized service provider may address potential incidents, provide added functionality, and help improve performance. If the updates are applicable to the Customer's HP Datacenter Care Service environment, the HP account team will review them with the Customer during the support planning and reviews. The number of network devices to be supported will be documented and confirmed in the account support plan.
Network critical incident notification	When necessary, HP will notify the Customer about critical software incidents that may impact network operation. The notification is specific to HP network device software and network device software from organizations for which HP is an authorized service provider for devices within the scope of the HP Datacenter Care Service environment. The number of network devices to be supported will be documented and confirmed in the account support plan.
Network asset report	Annually (or the timeframe agreed in the SOW), the HP account team can complete a network equipment audit to map the Customer's network topology. In addition, the Customer will receive a report describing the network hierarchy, network software versions, hardware products, and changes made since the previous audit. The number of network products to be supported will be documented and confirmed in the account support plan.
Open network environment support	HP can also offer a single point of contact for reactive and proactive support for many open (multivendor) networks. HP troubleshoots and performs fault isolation for the Customer's multivendor network and manages problem resolution. In addition, HP incorporates the multivendor devices in the Customer's account support plan, support planning and reviews, and support activity reviews.

Specifications

Table 3. Optional reactive features

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected.**
General description of optional reactive features	All IT infrastructure and products supported by HP Datacenter Care Service must have valid reactive support provided by HP. This support can either be explicitly entitled by including the products on the Datacenter Care Service agreement, or the service agreement can be layered on top of existing HP support agreements or HP warranty coverage. The IT infrastructure and products supported by this service will be documented in a Customer proposal, SOW, or equivalent document, and will be confirmed with the Customer by the ASM during service startup.
Default service coverage window (24x7)	The coverage window specifies the time during which reactive services are delivered onsite or remotely. The default coverage window for HP Datacenter Care Service is 24 hours a day, Monday through Sunday, including HP holidays. A response to any critical incident is available 24 hours a day, Monday through Sunday, including HP holidays, and is described as part of Enhanced Call Handling within the core features described above.

Specifications

Table 3. Optional reactive features *continued*

Feature or service	Delivery specifications
Optional features include the following:	**Optional features listed below may also be added to this customized offering, and will be priced accordingly based upon the services and features selected.**
Default hardware reactive support features, which includes:	If hardware products are explicitly included in the HP Datacenter Care Service agreement, the default hardware support for this service is a 4-hour onsite response with a 24x7 coverage window. The supported hardware product under the HP Datacenter Care Service agreement could also have a coverage window and service level per separate HP contract or HP warranty.
Onsite hardware support	For hardware incidents that cannot, in HP's judgment, be resolved remotely, an HP authorized representative will provide onsite technical support on covered hardware products to return them to operating condition. For certain products, HP may, at its sole discretion, elect to replace such products in lieu of repairing them. Replacement products are new or functionally equivalent to new in performance. Replaced products become the property of HP. Once an HP authorized representative arrives at the Customer's site, the representative will continue to deliver the service, either onsite or remotely, at the discretion of HP, until the products are repaired. Work may be temporarily suspended if parts or additional resources are required, but work will resume when they become available. Work to completion may not apply to onsite support provided for desktop, mobile, and consumer products. Repair is considered complete upon HP verification that the hardware malfunction has been corrected or that the hardware has been replaced. 'Fix-on-Failure': In addition, at the time of onsite technical support delivery, HP may: • Install available engineering improvements for covered hardware products to help the Customer ensure proper operation of the hardware products and maintain compatibility with HP-supplied hardware replacement parts • Install available firmware updates defined by HP as non-customer installable for covered hardware products, that, in the opinion of HP, are required to return the covered product to operating condition or to maintain supportability by HP 'Fix-on-Request': In addition, at the Customer's request, HP will install during coverage hours critical firmware updates defined by HP as non-customer installable for covered hardware products. Critical firmware updates are firmware updates recommended by the HP product division for immediate installation. Notwithstanding anything to the contrary in this document or HP's current standard sales terms, HP will, for select enterprise storage arrays and enterprise tape products, cover and replace defective or depleted batteries that are critical to the proper operation of the covered product.
4-hour onsite response	An HP authorized representative will arrive at the Customer's site during the coverage window to begin hardware maintenance service within 4 hours after the service request has been received and acknowledged by HP.
Replacement parts and materials	HP will provide HP-supported replacement parts and materials necessary to maintain the covered hardware product in operating condition, including parts and materials for available and recommended engineering improvements. Replacement parts provided by HP shall be new or functionally equivalent to new in performance. Replaced parts become the property of HP. Customers who wish to retain, degauss, or otherwise physically destroy replaced parts will be billed and required to pay the list price for the replacement part. Supplies and consumable parts are not supported and will not be provided as part of this service; standard warranty terms and conditions apply to supplies and consumable parts. The repair or replacement of any supplies or consumables is the responsibility of the Customer. Some exceptions may apply; contact HP for more information. If a consumable part is eligible for coverage, as determined by HP, call to repair time commitments and onsite response times do not apply to repair or replacement of the covered consumable parts. **Maximum supported lifetime/maximum usage:** Parts and components that have reached their maximum supported lifetime and/or the maximum usage limit as set forth in the manufacturer's operating manual, product QuickSpecs, or the technical product data sheet will not be provided, repaired, or replaced as part of this service.
Work to completion	Once an HP authorized representative arrives at the Customer's site, the representative will continue to deliver the service, either onsite or remotely at the discretion of HP, until the products are repaired. Work may be temporarily suspended if additional parts or resources are required, but work will resume when they become available. Work to completion applies to onsite response time hardware service levels only and may not apply to onsite support provided for desktop, mobile, and consumer products. Repair is considered complete upon HP verification that the hardware malfunction has been corrected or that the hardware has been replaced.

Specifications

Table 3. Optional reactive features *continued*

Feature or service	Delivery specifications
Default software reactive support features, which includes:	
Non-critical software response	Once a non-critical software incident is logged, HP will respond to the call within 2 hours after the service request has been logged, if this time falls within the contracted coverage window. HP provides corrective support to resolve identifiable and customer-reproducible software product problems. HP also provides support to help the Customer identify problems that are difficult to reproduce. The Customer receives assistance in troubleshooting incidents and resolving configuration parameters. For critical software response, please refer to the feature definition for Enhanced Call Handling response to critical hardware and software incidents. Incident severity levels are defined in 'General provisions.'
Software product and documentation updates	As HP releases updates to HP software, the latest revisions of the software and reference manuals are made available to the Customer. For selected third-party software, HP will provide software updates as such updates are made available from the third party, or HP may provide instructions on how to obtain any software updates directly from the third party. A license key or access code, or instructions for obtaining a license key or access code, will also be provided to the Customer when required to download, install, or run the latest software revision. For most HP software and selected HP-supported third-party software, updates will be made available through the Software Updates and Licensing portal via the HP Support Center. The Software Updates and Licensing portal provides the Customer with electronic access to receive and proactively manage software product and documentation updates. For other HP-supported third-party software, the Customer may be required to download updates directly from the vendor's website.
License to use software updates	The Customer receives the license to use software updates to HP or HP-supported third-party software for each system, socket, processor, processor core, or end-user software license covered by this service, as allowed by the original HP or original manufacturer software license terms. The license terms shall be as described in the HP software licensing terms corresponding to the Customer's prerequisite underlying software license, or in accordance with the current licensing terms of the third-party software manufacturer, if applicable, including any additional software licensing terms that may accompany such software updates provided under this service.
HP recommended software and documentation updates method	For HP or HP-supported third-party software and documentation updates, the recommended delivery method will be determined by HP. The primary delivery method for software updates and documentation updates will be via download from the Software Updates and Licensing portal or third-party hosted website.
Additional optional features include the following:	The additional optional features described here are available for eligible products only.
Optional hardware reactive support features, which includes:	
Collaborative call management on non-HP software products	HP accepts calls on selected non-HP software products installed on HP servers that are covered under an HP Collaborative Support Service agreement and attempts to resolve the problem by applying known remedies available to HP. If HP determines that a problem is caused by selected third-party software and the problem is not resolved by the Customer applying known, available fixes as defined in the Basic Software Support deliverables in the HP Collaborative Support Service data sheet, HP will, at the Customer's request, initiate a service call with the third-party software vendor, provided appropriate support agreements exist between the Customer and the vendor and provided the Customer has in place the necessary agreements with that vendor to allow HP to forward the problem to them on behalf of the Customer. Once the software vendor is engaged, HP will close the HP call, but the Customer can resume the service issue with HP if necessary by referencing the original call identification number. Please refer to the HP Collaborative Support Service data sheet for additional details. For more information on which non-HP software products are supported, refer to the website located at **www.hp.com/go/collaborativesupport**.

Specifications

Table 3. Optional reactive features *continued*

Feature or service	Delivery specifications
Optional hardware reactive support features, which includes:	
6-hour call-to-repair time commitment	For critical problems with covered hardware that cannot be quickly resolved remotely, HP will use commercially reasonable efforts to return the covered hardware to operating condition within 6 hours of the initial service request to the HP Global Solution Center. Call-to-repair time refers to the period of time that begins when the initial service request is logged at the HP Global Solution Center and ends with HP's determination that the hardware is repaired. Repair is considered complete upon HP verification that the hardware malfunction has been corrected or that the hardware has been replaced or, for eligible storage products, that access to the Customer's data has been restored. Verification by HP may be accomplished by the completion of a power-on self-test, standalone diagnostic, or visual verification of proper operation. At its sole discretion, HP will determine the level of testing necessary to verify that the hardware is repaired. At its sole discretion, HP may temporarily or permanently replace the affected hardware product in order to meet the repair time commitment. Replacement products are new or equivalent to new in performance. Replaced products become the property of HP. It will take 30 days from the time this service is purchased to set up and perform any audits deemed necessary by HP, together with any associated processes, before the hardware call-to-repair time commitment is in effect. During this initial 30-day period and for up to 5 additional business days after the audit is completed, HP will provide a 4-hour onsite response time as defined herein.
Upfront audit	HP, at its sole discretion, may require an audit on the covered products. If such an audit is required, an HP authorized representative will contact the Customer, and the Customer will agree to arrange for an audit to be performed within the initial 30-day timeframe. During the audit, key system configuration information is collected and an inventory of the covered products is performed. The information gathered in the audit enables HP to plan and maintain replacement part inventories at the appropriate level and location, and allows an HP resolution engineer to survey and troubleshoot possible future hardware incidents and complete the repair as quickly and efficiently as possible. At the sole discretion of HP, the audit may be performed onsite, via remote system access, via remote audit tools, or over the phone. If an audit is required by HP, the hardware call-to-repair time commitment will not take effect until five (5) business days after the audit has been completed. In addition, HP reserves the right to downgrade service to an onsite response time or cancel the service contract if critical audit suggestions are not followed or the audit is not performed within the specified timeframe unless the delay is caused by HP.
Enhanced parts inventory management	To support HP call-to-repair time commitments, an inventory of critical replacement parts is maintained for call-to-repair Customers. This inventory is stored at an HP designated facility. These parts are managed to allow for increased inventory availability and are accessible to HP authorized representatives responding to eligible support requests. Enhanced parts inventory management is included with select, optional call-to-repair time commitments.
Dedicated parts inventory	The Customer may choose to have a dedicated kit of critical hardware replacement parts stored at the Customer site or at an HP facility. This inventory, owned by HP, is dedicated to the Customer’s organization and is actively managed by HP. This option is available with the hardware call-to-repair time commitment only.
Defective media retention	For eligible products, this service feature option allows the Customer to retain defective hard disk or eligible SSD/Flash drive components that the Customer does not want to relinquish due to sensitive data contained within the disk ('Disk or SSD/Flash Drive') covered under this service. All Disk or eligible SSD/Flash Drives on a covered system must participate in the defective media retention.
Comprehensive defective material retention	In addition to defective media retention, this service feature option allows the Customer to retain additional components that have been designated by HP as having data retentive capabilities, such as memory modules. All eligible data retentive components on a covered system must participate in the comprehensive defective material retention. The components that can be retained under this service feature are outlined in the document located at **www.hp.com/services/cdmr**.

Specifications

Table 4. Service-level options

Service-level option	Delivery specifications
Service-level options availability	Not all service-level options are available on all products. The service-level options the Customer has chosen will be specified in the Customer's contract documentation.
Coverage window includes the following:	The coverage window specifies the time during which the described services are delivered onsite or remotely. Calls received outside this coverage window will be logged at the time the call is placed to HP, but will not be acknowledged as described in 'General provisions' until the next day for which the Customer has a coverage window. Coverage window options available for eligible products are specified in the Service-level options table. All coverage windows are subject to local availability. Contact a local HP sales office for detailed information on service availability.

Specifications

Table 4. Service-level options *continued*

Service-level option	Delivery specifications
Default service coverage window, which includes:	
24 hours, seven days a week (24x7)	Default coverage window for HP Datacenter Care Service is 24 hours per day, Monday through Sunday, including HP holidays.
Coverage window options, which include:	Service is available during the specified coverage hours and days:
Standard business hours, standard business days (9x5)	9 hours per day between 8:00 a.m. and 5:00 p.m. local time, Monday through Friday excluding HP holidays
13 hours, standard business days (13x5)	13 hours per day between 8:00 a.m. and 9:00 p.m. local time, Monday through Friday excluding HP holidays
16 hours, standard business days (16x5)	16 hours per day between 8:00 a.m. and 12:00 a.m. local time, Monday through Friday excluding HP holidays
24 hours, standard business days	24 hours per day, Monday through Friday excluding HP holidays
Coverage extension for additional hours	The coverage window is extended to define custom coverage hours that include additional individual hours before or after the selected coverage window.
Coverage extensions for additional days	The coverage window is extended by applying the selected coverage hours to additional days of the week, including the following: • Saturdays, excluding HP holidays • Sundays (requires Saturday and holiday coverage) • HP holidays, should these fall on a weekday that would otherwise be included in the selected coverage window
Coverage window under separate HP contract or HP warranty	Service is available per the coverage window outlined in separate HP contract or HP warranty. Please contact a local HP representative for more information.
Hardware reactive support options include the following:	
Onsite response time for hardware support	For incidents with covered hardware that cannot be resolved remotely, HP will use commercially reasonable efforts to respond onsite within the specified onsite response time. Onsite response time specifies the period of time that begins when the initial call has been received and acknowledged by HP, as described in 'General provisions.' The onsite response time ends when the HP authorized representative arrives at the Customer's site, or when the reported event is closed with explanation that HP has determined it does not currently require an onsite intervention. Response times are measured during the coverage window only and may be carried over to the next day for which there exists a coverage window. Response time options available for eligible products are specified in the Service-level options table. All response times are subject to local availability. Contact a local HP sales office for detailed information on service availability.
Onsite response time options, which include:	
2-hour onsite response	An HP authorized representative will arrive at the Customer's site during the coverage window to begin hardware maintenance service within 2 hours after the service request has been received and acknowledged by HP.
4-hour onsite response	An HP authorized representative will arrive at the Customer's site during the coverage window to begin hardware maintenance service within 4 hours after the service request has been received and acknowledged by HP.
Next-day onsite response	An HP authorized representative will arrive at the Customer's site during the coverage window to begin hardware maintenance service the next coverage day after the service request has been received and acknowledged by HP.

Specifications

Table 4. Service-level options *continued*

Service-level option	Delivery specifications
Onsite response time options, which include:	
Service level under separate HP contract or HP warranty	Hardware reactive support onsite response time is outlined in a separate HP contract or HP warranty. Please contact a local HP representative for more information.
Hardware call-to-repair time commitment (in lieu of hardware onsite response time options)	For incidents with covered hardware that cannot be resolved remotely, an HP authorized representative will arrive at the Customer's site to begin hardware maintenance service after the service request has been acknowledged by HP, as specified in 'Service prerequisites.'
Hardware call-to-repair time commitment options, which include:	
4-hour call-to-repair time	HP will use commercially reasonable efforts to return the covered hardware to operating condition within 4 hours after the incident has been received and acknowledged by HP, if this time falls within the coverage window.
6-hour call-to-repair time	HP will use commercially reasonable efforts to return the covered hardware to operating condition within 6 hours after the incident has been received and acknowledged by HP, if this time falls within the coverage window.
8-hour call-to-repair time	HP will use commercially reasonable efforts to return the covered hardware to operating condition within 8 hours after the incident has been received and acknowledged by HP, if this time falls within the coverage window.
24-hour call-to-repair time	HP will use commercially reasonable efforts to return the covered hardware to operating condition within 24 hours after the incident has been received and acknowledged by HP, if this time falls within the coverage window.
Service level under separate HP contract or HP warranty	Hardware reactive support call-to-repair time is outlined in a separate HP contract or HP warranty. Please contact a local HP representative for more information.

Specifications

Table 5. Call-to-restoration upgrade enhancement option

Feature or service	Delivery specifications
Proactive features include the following:	
Call-to-restoration upgrade enhancement	The call-to-restoration upgrade enhancement option is available for servers using the HP-UX operating system, which builds on HP Datacenter Care Service deliverables and adds additional proactive and reactive elements for businesses whose customer relations or revenues are impacted by every moment of downtime. Call-to-restoration provides both faster resolution of complex problems and a closer relationship with HP, which aligns support activities with the Customer's IT strategy and availability goals.
ITSM assessment	Prior to implementing a call-to-restoration enhancement, HP conducts an ITSM assessment. During the assessment, key members of the Customer's IT staff meet with HP specialists to review procedures, processes, configurations, and administration practices. HP analyzes the information gathered and reports the findings via an executive presentation and detailed report. The focus of this assessment is to help the Customer implement appropriate processes to recover the Customer's systems. If the report highlights critical improvements, these improvements must be implemented prior to enacting the 4-hour call-to-restoration enhancement.

Specifications

Table 5. Call-to-restoration upgrade enhancement option*continued*

Feature or service	Delivery specifications
Proactive features include the following:	
Upfront audit	HP may, at its sole discretion, require an audit on the covered products. If such an audit is required, an HP authorized representative will contact the Customer, and the Customer will agree to arrange for an audit to be performed within the initial 30-day timeframe. During the audit, key system configuration information is collected and an inventory of the covered products is performed. The information gathered in the audit enables HP to plan and maintain replacement part inventories at the appropriate level and location, and allows an HP resolution engineer to survey and troubleshoot possible future hardware incidents and complete the repair as quickly and efficiently as possible. At the sole discretion of HP, the audit may be performed onsite, via remote system access, via remote audit tools, or over the phone. If an audit is required by HP, the call-to-restoration time commitment will not take effect until five (5) business days after the audit has been completed. During this initial 30-day period and for up to 5 additional business days after the audit is completed, HP will provide a 4-hour onsite response time. HP reserves the right to downgrade service to an onsite response time or cancel the service contract if critical audit suggestions are not followed or the audit is not performed within the specified timeframe unless the delay is caused by HP.
Daily screen for critical patches	HP conducts a daily screen (Monday through Friday, excluding HP holidays) of newly released critical HP patches, known critical problems that may impact the Customer, and changes in the status of patches already installed on the Customer's system. The daily screen is intended to identify critical patch information that requires immediate attention and assist the Customer in preventing a severe problem from occurring. When critical patch information requires action, the Customer is immediately contacted to discuss the information and agree on the action to be taken. If the Customer has more than one operating system version in their environment, the HP account team reviews patches for one operating system version per day.
Monthly support reviews	These monthly meetings allow HP to focus on a breadth of topics with the depth expected to thoroughly understand the Customer's environment and risks. These meetings typically focus on topics such as system availability, escalations, change management, patching strategies, and status on outstanding support tasks. The Customer can expect that this comprehensive meeting will also address issues concerning backup and recovery plans and processes, performance, security, and data management. Typically, the HP account team will provide progress reports as to how the Customer's issues are being addressed and recommendations as to how to enhance the Customer's environment.
Semi-monthly operating system patch analysis and management	On a Semimonthly basis, the account team monitors the release of new patches, reviews these patches with the Customer's staff, and provides the Customer with a customized bundle of the appropriate and agreed-upon patches.
Delivery process reviews	Twice a year, HP conducts a formal support process review of all delivered support activities. These reviews address changes in the Customer's environment, allowing the Customer and HP to exchange information on business objectives and IT priorities, with a focus on the role of support in achieving these goals. These reviews evaluate technology trends, the status of outstanding service requests, gaps in delivery, training needs, and other areas related to the delivery of services that contribute to the Customer's business priorities. These delivery process reviews are normally conducted as an extension of selected support review meetings and include the Customer's senior IT management.
Configuration checkup	Once a year, the HP account team audits the configuration of selected servers and identifies suboptimal configuration parameters, single points of failure, and areas of exposure to downtime and supportability risk. The team provides recommendations about reconfiguration steps to minimize these risks.
HP Proactive Select Service credits	For Customers who purchase the call-to-restoration upgrade option with HP Datacenter Care Service, HP provides 60 credits per year, from the Proactive Select services menu. The Customer has the flexibility of choosing an activity from the predefined menu addressing areas such as virtualization, storage data management, infrastructure optimization, assessments, performance analysis, and firmware management. Alternatively, the Customer may choose to work with the ASM and use these 60 service credits for a customized activity. More detailed information is provided in table 8.
Reactive features	
4-hour call-to-restoration commitment	The hardware and operating system (OS) incidents will be restored within 4 hours of the Customer's initial call to HP, subject to certain limitations. System connectivity to the network is also established within this timeframe. Call-to-restoration time refers to the period of time that begins when the original call is placed to HP and ends when the server is available for use. The server is considered to be available for use when an operating system prompt is re-established and the operating system is restored to the Customer's last configuration or, alternatively, when the OS is restored to a generic configuration for that OS version. It does not include time needed for recovery of middleware, application software, or data. At its sole discretion, HP may temporarily or permanently replace the product in order to meet the restoration commitment.
Problem resolution verification	HP formally reviews all critical problems with HP hardware and software. This review is intended to analyze each problem and verify that the final resolution addresses the problem. If a temporary fix or workaround was required to restore operation, creation and delivery of a more appropriate solution is a priority for HP support and research and development. The solution may include creating OS patches and server firmware updates.

Specifications

Table 5. Call-to-restoration upgrade enhancement option*continued*

Feature or service	Delivery specifications
Proactive features include the following:	
Dedicated parts inventory	Included with the call-to-restoration service is a dedicated inventory of critical replacement parts. HP maintains this dedicated inventory of critical replacement parts exclusively for the Customer. These parts are managed to allow for continuous availability, enabling a quicker resolution of critical hardware problems. The Customer may choose to have the parts inventory located either at HP or at the Customer's site.
Customized escalation process	HP designs and tests a custom-tailored, accelerated escalation process that considers the Customer's internal problem management, escalation processes, and participants.

Specifications

Table 6. Service travel zones

Service	Travel zone specifications
Geographic coverage	Travel zones and charges, if applicable, may vary in some geographic locations.
Hardware onsite response time	All hardware onsite response times apply only to sites located within 25 miles (40 km) of an HP-designated support hub. Travel to sites located within 200 miles (320 km) of an HP-designated support hub is provided at no additional charge. If the site is located more than 200 miles (320 km) from the HP-designated support hub, there will be an additional travel charge. Travel zones and charges may vary in some geographic locations. Response times to sites located more than 100 miles (160 km) from an HP-designated support hub will be modified for extended travel, as shown in the table that follows.
Travel zones for hardware onsite response time	

Distance from HP-designated support hub	2-hour hardware onsite response time	4-hour hardware onsite response time	Next-day hardware onsite response time
0–25 miles (0–40 km)	2 hours	4 hours	Next coverage day
26–50 miles (41–80 km)	Established at time of order and subject to availability	4 hours	Next coverage day
51–100 miles (81–160 km)	Not available	4 hours	Next coverage day
101–200 miles (161–320 km)	Not available	8 hours	1 additional coverage day
201–300 miles (321–480 km)	Not available	Established at time of order and subject to resource availability	2 additional coverage days
Greater than 300 miles (480+ km)	Not available	Established at time of order and subject to resource availability	Established at time of order and subject to resource availability

Hardware call-to-repair time commitment	A hardware call-to-repair time is available for sites located within 50 miles (80 km) of an HP-designated support hub. Travel zones and charges may vary in some geographic locations. The hardware call-to-repair time is not available for sites located more than 100 miles (160 km) from an HP-designated support hub. For sites that are located from 51 to 100 miles (81 to 160 km) of an HP-designated support hub, an adjusted hardware call-to-repair time applies, as shown in the table that follows.

Specifications

Table 6. Service travel zones *continued*

Service	Travel zone specifications				
Travel zones for hardware call-to-repair time commitment					
	Distance from HP-designated support hub	**4-hour hardware call-to-repair time**	**6-hour hardware call-to-repair time**	**8-hour hardware call-to-repair time**	**24-hour hardware call-to-repair time**
	0–50 miles (0–80 km)	4 hours	6 hours	8 hours	24 hours
	51–100 miles (81–160 km)	6 hours	8 hours	10 hours	24 hours
	Greater than 100 miles (160+ km)	Not available	Not available	Not available	Not available
Call-to-restoration time commitment	The 4-hour call-to-restoration time commitment is available for sites located within 50 miles (80 km) of an HP-designated support hub. For sites that are located between 51 and 100 miles (81 and 160 km) from an HP-designated support hub, an adjusted 6-hour hardware call-to-restoration time commitment is provided. The call-to-restoration time commitment is not available for sites located more than 100 miles (160 km) from an HP-designated support hub. Travel zones and charges may vary in some geographic locations.				
Travel zones for call-to-restoration time commitment					
	Distance from HP-designated support hub	**4-hour call-to-restoration time**			
	0–50 miles (0–80 km)	4 hours			
	51–100 miles (81–160 km)	6 hours			
	Greater than 100 miles (160+ km)	Not available			

Specifications

Table 7. Enabling technologies and tools

Service focus	Description
Enabling technologies and tools	To support HP Datacenter Care Service Customers, HP uses a powerful suite of tools and technologies for managing complex and diverse IT environments. HP remote support technologies integrate management of multiple servers, OSs, and networking and storage devices. This suite of remote support technologies provides a wide range of proactive capabilities, including continuous event monitoring, automatic collection of configuration and topology data, and automated notification of potential problems. These capabilities help the Customer improve system uptime, turn unscheduled events into scheduled maintenance, and experience faster incident resolution when incidents do occur. The electronic remote monitoring and support provided by these remote support technologies also help HP support engineers resolve incidents faster. This is accomplished using remote troubleshooting and diagnostic tools, as well as capabilities that provide specific details of the Customer's configurations, identify configuration changes, and systematically analyze the Customer's configurations against HP standard best practices. Recognizing that any remote support solution must provide security for the Customer's IT environment, these remote support technologies comply with industry-standard security tools and practices. HP's rigorous security architecture helps provide data integrity and transaction security through a multilevel, layered structure utilizing encryption, authentication, industry-standard security protocols, and industry best practices integrated at the physical, network, application, and operational levels. The Customer is responsible for maintaining the contact details configured in the remote support solution that HP will use in responding to a device failure.

Specifications

Table 8. HP Proactive Select services

Service focus	Description
HP Proactive Select services	HP Proactive Select services address the Customer's need to maintain efficiency, cost-effectiveness, and quality within the Customer's IT environment. The Customer has the flexibility to choose from a variety of service activities ranging from virtualization, storage data management, infrastructure optimization, power and cooling, assessments, security, performance analysis, and firmware management. These service activities cover a broad spectrum of IT technology domains, including servers, blades, OSs, storage, SANs, networks, and ISV software. The goal of HP Proactive Select services is to provide the flexibility that the Customer needs by filling resource gaps and providing specialized expertise whenever it is required. The ASM can help determine how these services can be tailored to fit the Customer's needs. Consult an HP representative for a comprehensive list of available services.

Service limitations

Services provided within the scope of one support contract are restricted to the IT environment under the direct day-to-day management of one IT organization, in one country, and as detailed in the SOW. Unless otherwise specified or arranged, proactive and consultative services are performed during standard HP business hours. Delivery of specific features on technologies in the Customer's environment (servers, storage, SAN, and networks) is dependent on prior purchase of the appropriate technology service module(s).

HP Proactive Select services are available for selected HP servers, software, storage devices, storage arrays, networks, and SANs only. Features of these services may differ, or be limited, based on specific devices or software. Please check with an HP sales office for specific limitations or local availability.

The HP account team provides the required proactive deliverables during HP standard business hours on standard business days, either remotely or onsite, at the discretion of HP.

Delivery of proactive support outside HP standard business hours on standard business days can be purchased separately and is subject to local availability.

HP retains the right to determine the final resolution of all reported incidents.

From time to time, HP may provide advice on customer security practices; however, the Customer is fully responsible for the security of its IT environment.

At the discretion of HP, service will be provided using a combination of remote diagnosis and support, services delivered onsite, and other service delivery methods. Other service delivery methods may include the delivery, via a courier, of customer-replaceable parts such as a keyboard, a mouse, or if agreed by the Customer, other parts classified by HP as Customer Self Repair parts, or an entire replacement product. HP will determine the appropriate delivery method required to provide effective and timely Customer support and meet the call-to-repair time commitment, if applicable.

HP is not liable for the performance or non-performance of third-party vendors, their products, or their support services.

The following list includes, but is not limited to, specific activities that are excluded from HP Datacenter Care Service:

- Troubleshooting for interconnectivity or compatibility problems
- Services required due to failure of the Customer to incorporate any system fix, repair, patch, or modification provided to the Customer by HP
- Services required due to failure of the Customer to take avoidance action previously advised by HP
- Services that, in the opinion of HP, are required due to unauthorized attempts by non-HP personnel to install, repair, maintain, or modify hardware, firmware, or software
- Operational testing of applications, or additional tests requested or required by the Customer
- Backup and recovery of the operating system, other software, and data
- Services that, in HP's opinion, are required due to improper treatment or use of the products or equipment

Hardware call-to-repair and call-to-restoration commitment

It will take 30 days from the time this service is purchased to set up and perform the audits and processes that must be completed before hardware call-to-repair, call-to-restoration, and various other contract commitments can be put in effect. During this initial phase of HP Datacenter Care Service, the HP account team will perform necessary hardware and software audits, set up processes, assess the high-availability environment, and implement the customizable elements of this service as appropriate to the Customer's operation. During this initial 30-day period and for up to 5 additional business days after the audit is completed, HP will provide a 4-hour onsite response time.

Hardware call-to-repair time options are specified in the service-level options table. All call-to-repair times and call-to-restoration times are subject to local availability and may not be available on all products. Contact a local HP sales office for detailed information on availability.

The hardware repair time commitment may vary for specific products.

A call-to-repair time commitment does not apply when the Customer chooses to have HP prolong diagnosis rather than execute recommended server recovery procedures.

If the Customer requests scheduled service, the repair timeframe begins from the agreed-upon scheduled time.

In the event that only a customer-replaceable part is required to return the system to operating condition, the call-to-repair time commitment, if any, shall not apply. In those cases HP intends to ship Customer Self Repair parts that are critical to the product operation to the Customer location utilizing the fastest locally available commercial carrier option.

HP reserves the right to modify the call-to-repair time commitment as it applies to the Customer's specific product configuration, location, and environment. This is established at the time of support agreement order and is subject to resource availability.

Call-to-restoration for critical software problems is intended for software products normally used in a production environment. For critical problems with all other HP software, HP will use reasonable commercial efforts to resolve the problem, subject to resource availability.

The call-to-restoration commitment only applies to server hardware, HP-UX operating system software, and connectivity of the Customer's server to the network.

The following are excluded from the call-to-repair and call-to-restoration time commitment (if applicable):

- Time for disk mechanism rebuild or sparing procedures
- Any restoration/recovery of compromised data
- Situations where a logical unit number (LUN) may be blocked to preserve data integrity
- Any period of non-availability not directly caused by the hardware fault

In addition, call-to-restoration excludes repair of network hardware devices or network-related problems, as well as the time needed for recovery of middleware, application software, or data. Restoration of the last operating system configuration requires the Customer to implement and execute specific backup procedures. In the absence of these procedures, a generic configuration will be restored.

Hardware onsite support

An onsite response time will not apply if the service can be delivered using remote diagnosis, remote support, or other service delivery methods described earlier.

Open Network Environment support

The following are excluded from Open Network Environment support:

- Establishment of a contract between the third-party vendor and the end-user Customer
- Establishment of a service-level agreement concerning, or assumption of responsibility for, the performance of a third-party vendor's products or services
- Resolution or repair of third-party product changes to restore solution to original operable state
- Subcontracting of any service to a third-party vendor, including billing that vendor on the Customer's behalf

HP will not be able to contact a third-party vendor on the Customer's behalf unless the Customer has appointed HP as a special agent.

Software

For all the servers that are included in the HP Datacenter Care Service environment, if the Customer has not purchased the OS license and the related reactive support from a third party, then software support must be purchased for each license and/or device that is covered under this service. If software support is not purchased from HP, software support will not be provided.

For the Customer with multiple systems at the same location, HP may limit the number of physical media sets containing software product and documentation updates provided as part of this service.

Software updates are not available for all software products. When this service feature is not available, it will not be included in this service.

For some products, software updates include only minor improved features. New software versions must be purchased separately.

Limitations to the defective media retention and comprehensive defective material retention service feature options

The defective media retention and comprehensive defective material retention service feature options apply only to eligible data retentive components replaced by HP due to malfunction. They do not apply to any exchange of data retentive components that have not failed.

Data retentive components that are specified by HP as consumable parts and/or have reached the maximum supported lifetime and/or the maximum usage limit as set forth in the manufacturer's operating manual, the product QuickSpecs, or the technical data sheet are not covered by this service.

Defective media retention service and comprehensive defective material retention service coverage for options designated by HP as requiring separate coverage, if available, must be configured and purchased separately.

Failure rates on these components are constantly monitored, and HP reserves the right to cancel this service with 30 days' notice if HP reasonably believes that the Customer is overusing the defective media retention or comprehensive defective material retention service feature option (such as when replacement of defective data retentive components materially exceeds the standard failure rates for the system involved).

The defective media retention and comprehensive defective material retention service feature options apply only to eligible data retentive components replaced by HP due to malfunction. They do not apply to any exchange of data retentive components that have not failed.

Data retentive components that are specified by HP as consumable parts and/or have reached the maximum supported lifetime and/or the maximum usage limit as set forth in the manufacturer's operating manual, the product QuickSpecs, or the technical data sheet are not covered by this service.

Defective media retention service and comprehensive defective material retention service coverage for options designated by HP as requiring separate coverage, if available, must be configured and purchased separately.

Failure rates on these components are constantly monitored, and HP reserves the right to cancel this service with 30 days' notice if HP reasonably believes that the Customer is overusing the defective media retention or comprehensive defective material retention service feature option (such as when replacement of defective data retentive components materially exceeds the standard failure rates for the system involved).

HP shall have no obligation whatsoever with respect to the contents of or the destruction of any data retentive component retained by the Customer. Notwithstanding anything in HP's current standard sales terms or the technical data sheet to the contrary, in no event will HP or its affiliates, subcontractors, or suppliers be liable for any incidental, special, or consequential damages or damages for loss of or misuse of data under this defective media retention or comprehensive defective material retention service.

Service prerequisites

For call-to-repair and call-to-restoration time commitments, an upfront audit may be required by HP. It will take 30 days from the time this service is purchased to set up and perform the audits and processes that must be completed before hardware call-to-repair, call-to-restoration, and various other contract commitments can be put in effect. During this initial phase of HP Datacenter Care Service, the HP account team will perform necessary hardware and software audits, set up processes, assess the high-availability environment, and implement the customizable elements of this service as appropriate to the Customer's operation. During this initial 30-day period and for up to 5 additional business days after the audit has been completed, HP will provide a 4-hour onsite response time.

For hardware onsite response time options, HP strongly recommends that the Customer install and operate the appropriate HP remote support solution, with a secure connection to HP, in order to enable the delivery of the service.

For hardware call-to-repair time commitments, HP requires that the Customer install and operate the appropriate HP remote support solution, with a secure connection to HP, in order to enable the delivery of the service.

Also, if HP determines that the best practice for a particular technology is to install firmware and embedded storage and SAN device-resident software updates remotely, then the Customer will be required to install and operate the appropriate HP remote support solution. Please contact a local HP representative for further details on requirements, specifications, and exclusions. If the Customer does not deploy the appropriate HP remote support solution, HP may not be able to provide the service as defined and is not obligated to do so.

Additional charges will be applied for the manual collection of system information for proactive analysis activities. Additional charges will also be applied for onsite installation of non-customer-installable firmware and non-customer-installable embedded storage and SAN device-resident software updates, if the Customer does not deploy the required remote support solution, where recommended and available. Installation of customer-installable firmware and software is the responsibility of the Customer. If the Customer requests that HP install customer-installable firmware and software updates, additional charges will apply. Any additional charges to the Customer will be on a time and materials basis, unless otherwise previously agreed in writing by HP and the Customer.

The 4-hour call-to-restoration time commitment requires that the Customer purchase the call-to-restoration upgrade enhancement option, the Technical Account Manager (TAM) enhancement option, and 4-hour hardware call-to-restoration reactive support for all hardware devices covered under this commitment.

The call-to-restoration time commitment requires that, twice per month, HP perform OS patch analysis and management for each different version of the OS on the HP servers covered by this service feature.

HP will acknowledge a call by logging a case, communicating the case ID to the Customer, and confirming the Customer's incident severity and time requirements for commencement of remedial action. Note: For events received via the HP electronic remote support solutions, HP is required to contact the Customer, determine the case severity with the Customer, and arrange access to the system before the hardware call-to-repair, call-to-restoration, or onsite response time period can start. Incident severity levels are defined in 'General provisions.'

To be eligible to purchase this service, the Customer must be properly licensed to use the revision of the software product that is current at the beginning of the Support Agreement period; otherwise, an additional charge may be applied to bring the Customer into service eligibility.

For the optional enhancement for SAP service, HP requires that the Customer install and operate the appropriate HP remote support solution, with a secure connection to HP, in order to enable the delivery of this option.

For Customers with licenses to firmware-based software products (features implemented in firmware activated by the purchase of a separate software license product) or licensed firmware, the Customer must also have, if available, an active HP Software Support agreement to receive, download, install, and use related firmware updates. HP will provide, install, or assist the Customer with installation of firmware updates as previously described in this document only if the Customer has the license to use the related software updates for each system, socket, processor, processor core, or end-user software license as allowed by the original HP or original manufacturer software license terms.

Customer responsibilities

The Customer will identify a focal point and an internal Customer team to work collaboratively with the HP account team in the development, implementation, and ongoing review of the account support plan.

The call-to-repair and call-to-restoration time commitments are subject to the Customer providing immediate and unrestricted access to the system, as requested by HP. The call-to-repair and call-to-restoration time commitments do not apply when system access, including physical, remote troubleshooting, and hardware diagnostic assessment, is delayed or denied. If the Customer requests scheduled service, the call-to-repair or call-to-restoration time period begins at the agreed-upon scheduled time.

Upon HP request, the Customer will be required to support HP's remote problem resolution efforts. The Customer will:

- Start self-tests and install and run other diagnostic tools and programs
- Install customer-installable firmware updates and patches
- Provide all information necessary for HP to deliver timely and professional remote support and to enable HP to determine the level of support eligibility
- Perform other reasonable activities to help HP identify or resolve problems, as requested by HP

For HP Datacenter Care Service, HP strongly recommends that the Customer install the appropriate HP remote support solution, with a secure connection to HP, and to provide all necessary resources in accordance with the HP remote support solution release notes, in order to enable the delivery of the service and options. When an HP remote support solution is installed, the Customer must also maintain the contact details configured in the remote support solution that HP will use in responding to a device failure. Please contact a local HP representative for further details on requirements, specifications, and exclusions. For scheduled calls, the Customer shall promptly make the equipment available for remedial activities at the agreed-upon time.

In cases where Customer Self Repair parts or replacement products are shipped to resolve a problem, the Customer is responsible for returning the defective part or product within a time period designated by HP. In the event that HP does not receive the defective part or product within the designated time period or if the part or product is degaussed or otherwise physically damaged upon receipt, the Customer will be required to pay the HP list price less any applicable discounts for the defective part or product, as determined by HP.

In order for HP to provide collaborative call management, the Customer must have an active support agreement with the software vendor that includes the required service level and features that allow the Customer to place calls and receive support from the vendor. If the vendor requires it, the Customer will take any steps necessary to ensure that HP can submit calls on the Customer's behalf. In addition, the Customer must provide HP with the appropriate information needed for HP to initiate a service call with the software vendor on behalf of the Customer. HP's obligations are limited to the placement of support calls only.

HP is not liable for the performance or non-performance of third-party vendors, their products, or their support services. Purchase of this service does not assign the support agreement between the Customer and the vendor to HP. The Customer is still responsible for performance of obligations under such agreements, including payment of all applicable fees, as well as any fees that may apply as a result of logging calls with the vendor.

The Customer is responsible for installing, in a timely manner, critical customer-installable firmware updates, as well as Customer Self Repair parts and replacement products delivered to the Customer.

The Customer will:

- Take responsibility for registering to use the HP or third-party vendor's electronic facility in order to access knowledge databases, obtain product information, and download software updates or patches (upon the purchase of this service, HP will provide registration information to the Customer, as required; additionally, for certain products, the Customer may be required to accept vendor-specific terms for use of the electronic facility)
- Retain, and provide to HP upon request, all original software licenses, license agreements, license keys, and subscription service registration information, as applicable for this service
- Take responsibility for acting upon software product updates and obsolescence notifications received from the HP Support Center
- Use all software products in accordance with current HP software licensing terms corresponding to the Customer's prerequisite underlying software license or in accordance with the current licensing terms of the third-party software manufacturer, if applicable, including any additional software licensing terms that may accompany the actual software update provided under this service

The Customer is responsible for the security of the Customer's proprietary and confidential information, as well as properly sanitizing or removing data from products that may be replaced and returned to HP as part of the repair process to ensure the safeguarding of the Customer's data. For more information on Customer responsibilities, including those outlined in HP's Media Sanitization Policy and Media Handling Policy for Healthcare Customers, go to **www.hp.com/go/mediahandling**.

If the Customer chooses to retain repair parts covered under the defective media retention and/or comprehensive defective material retention service feature options, it is the Customer's responsibility to:

- Retain covered data retentive components that are replaced during support delivery by HP
- Ensure that any Customer sensitive data on the retained component is destroyed or remains secure
- Have an authorized representative present to retain the defective data retentive component, accept the replacement component, provide HP with identification information such as the serial number for each component retained hereunder, and, upon HP request, execute a document provided by HP acknowledging the retention of the data retentive component
- Destroy the retained data retentive component and/or ensure that it is not put into use again
- Dispose of all retained data retentive components in compliance with applicable environmental laws and regulations

For data retentive components supplied by HP to the Customer as loaner, rental, or lease products, the Customer will promptly return the replacement components at the expiration or termination of support with HP. The Customer will be solely responsible for removing all sensitive data before returning any such loaned, rented, or leased components or products to HP, and HP shall not be responsible for maintaining the confidentiality or privacy of any sensitive data that remains on such components.

Open Network Environment support

The Customer will appoint HP as special agent and grant HP full power and authority to act for the Customer and in the Customer's name for the limited purposes as set forth below:

- To contact non-affiliate vendor(s) directly to initiate a service call for remote assistance with the Customer's product
- To follow up directly with non-affiliate vendor(s) until the problem is resolved
- To facilitate communication between non-affiliate vendor(s) and other vendor(s) related to the Customer's network or between non-affiliate vendor(s) and HP during the process of fault isolation and problem resolution
- To provide telephone numbers and call logging instructions for each vendor the Customer wants HP to contact on the Customer's behalf
- To provide contract information that describes the level of service the Customer is to receive from the vendor

If the Customer does not comply with these Customer responsibilities, HP or an HP authorized service provider will not be obligated to deliver the services as described.

General provisions/Other exclusions

Hardware support onsite response time and call-to-repair and call-to-restoration time commitments, as well as software support remote response time, may differ depending on incident severity. The Customer determines the incident severity level.

Incident severity is defined as:

- Severity 1—Critical Down: for example, production environment down; production system or product application down/at severe risk; data corruption/loss or risk; business severely affected; safety issues
- Severity 2—Critically Degraded: for example, production environment severely impaired; production system or production application interrupted/compromised; risk of reoccurrence; significant impact on business
- Severity 3—Normal: for example, non-production system (i.e., test system) down or degraded; production system or production application degraded with workaround in place; non-critical functionality lost; limited impact on the business
- Severity 4—Low: for example, no business or user impact

Travel charges may apply; please consult your local HP office.

HP Proactive Select Service credits

HP Proactive Select Service credits:

- Must be utilized and redeemed against specific service activities within the scope of one account support plan and are restricted to the IT environment under the direct day-to-day management of one IT organization, in one country, and as detailed in the SOW
- Are not transferable
- Will terminate at the end of the current contract term and cannot be rolled over at contract renewal time; service credits unused at the end of the current contract term will not be refunded and cannot be added to another contract
- Can be canceled for a pro rata amount based on the unused Proactive Select Service credits, less any applicable early termination fees; conversely, HP will invoice the Customer on a pro rata basis for any credits used but not paid for at the time of contract cancellation

Ordering information

To obtain further information or to order HP Datacenter Care Service, contact a local HP sales representative and reference the following product number:

HP Contractual services: HP Datacenter Care Service (H2T12AC)

The flexibility and customization available in HP Datacenter Care Service provides a cost-effective support solution tailored to meet a Customer's unique needs. The exact combination of reactive and proactive support, the products to be covered, geographic coverage, and details of any other aspects of support will be documented in a SOW, or equivalent. As part of the startup phase of this service, the ASM will confirm all of these support commitments in an account support plan for formal agreement with the Customer.

Optional hardware onsite response support is selected in lieu of hardware call-to-repair or call-to-restoration time commitment support levels. The Customer may not select both onsite response support and call-to-repair, or call-to-restoration, time commitment support for the same device.

Enhanced parts inventory management and upfront audit are included with the call-to-repair time commitment option only; they may not be sold separately.

Dedicated parts inventory management and upfront audit are included with the call-to-restoration upgrade enhancement option.

Dedicated parts inventory management is available as an additional option with the hardware call-to-repair commitment service level only.

For more information

For more information on HP Datacenter Care Service or other HP Support Services, contact any of our worldwide sales offices or visit our website at:

www.hp.com/services/support

4AA4-0459ENW, Created March 2012; Updated February 2015, Rev. 3

WILDFIRE

Protection from Targeted and Unknown Attacks

WildFire™ cloud-based malware-analysis environment is an advanced threat intelligence service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. Once deployed, WildFire automatically disseminates updated protections in near-real time to immediately halt threats from spreading – without manual intervention. This closed-loop, automated process gives organizations the assurance that their networks, endpoints and cloud are armed with the absolute latest threat intelligence at all times.

Benefits

- Our Next-Generation Security Platform provides up-to-date protection throughout your organization to reduce the attack surface across multiple attack vectors.
- WildFire identifies unknown malware and zero-day exploits using advanced static and dynamic analysis techniques against multiple OS and application versions.
- WildFire automatically generates malware, URL and DNS signatures and distributes them within minutes to all global, WildFire-subscribed Palo Alto Networks platforms.
- Information about indicators of compromise (IOCs) from WildFire analysis reports is used by our Next- Generation Security Platform and our technology partners to identify infected hosts and prevent secondary downloads.

Advanced cyberattacks are employing stealthy and persistent methods to evade traditional security measures. Skilled adversaries demand that modern security teams re-evaluate their prevention tactics to better address the volume and sophistication of today's attacks. Purpose-built for high fidelity hardware emulation, WildFire analyzes suspicious samples as they execute. When new threats emerge, Palo Alto Networks® Next-Generation Security Platform automatically routes suspicious files and URLs to WildFire for deep analysis.

WildFire inspects millions of samples per week from its global network of customers and threat intelligence partners looking for new forms of previously unknown malware, exploits, malicious domains and outbound command-and-control activity. The cloud-based service creates new protections that are capable of blocking targeted and unknown malware, exploits, and outbound C2 activity by observing their actual "behavior," rather than relying on pre-existing signatures. The protections are shared globally in minutes.

Next-Generation Security Platform

WildFire is built on our industry-leading Next-Generation Security Platform, benefiting from full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption. Known threats are proactively blocked with our Next-Generation Firewall, Threat Prevention, URL Filtering, Traps and Aperture, providing baseline defenses against known exploits, malware, malicious URLs and command-and-control (C2) activity. Unknown files, and email links are forwarded and analyzed by WildFire in a scalable sandbox environment, where new threats are identified and protections are automatically developed and delivered to the security elements in your organization in the form of signatures and verdict updates. The result is a unique, closed-loop approach to preventing cyberthreats that includes: positive security controls to reduce the attack surface; inspection of all traffic, ports and protocols

to block all known threats; rapid detection of unknown threats by observing the actions of malware in a cloud-based execution environment; and automatic deployment of new protections back to the frontline to ensure threats are known to all and blocked across the attack lifecycle.

Behavior-Based Cyberthreat Discovery

To find unknown malware and exploits, WildFire executes suspicious content in the Windows® XP, Windows 7, Android® and Mac® OS X® operating systems, with full visibility into common file types, including: EXE, DLL, ZIP, PDF, as well as Microsoft® Office documents, Java® files, Android APKs, Adobe® Flash® applets, and webpages, including high-risk, embedded content, such as Java and Adobe Flash files and images.

WildFire identifies hundreds of potentially malicious behaviors to uncover the true nature of malicious files based on their actions, including:

- **Changes made to host:** WildFire observes all processes for modifications to the host, including file and registry activity, code injection, memory heap spray (exploit) detection, addition of auto-run programs, mutexes, Windows services, and other suspicious activities.
- **Suspicious network traffic:** WildFire performs analysis of all network activity produced by the suspicious file, including backdoor creation, downloading of next-stage malware, visiting low-reputation domains, network reconnaissance, and much more.
- **Anti-analysis detection:** WildFire monitors techniques used by advanced malware that is designed to avoid VM-based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features, and more.

Natively integrated with our Next-Generation Security Platform, which is capable of classifying all traffic across hundreds of applications, WildFire uniquely applies this behavioral analysis to web traffic, email protocols (SMTP, IMAP, POP) and FTP, regardless of ports or encryption.

WildFire Architecture

To support static and dynamic malware analysis at scale, across the organization, WildFire is built on a cloud-based architecture that can be leveraged by your existing Palo Alto Networks Next-Generation Security Platform with no additional hardware. Where regulatory or privacy requirements prevent the use of a cloud infrastructure, a local hardware solution can be deployed on premises using the WF-500 appliance. You can leverage both the cloud and local versions of WildFire within the same environment. This hybrid solution enables you to define which files types are sent to the cloud and which are sent to the local appliance, based on data sensitivity. Analysis results in the form of new protections that are shared globally.

Threat Prevention with Global Intelligence Sharing

When an unknown threat is discovered, WildFire automatically generates protections to block it across the cyberattack lifecycle, sharing these updates with all global subscribers in as little as five minutes. These quick updates are able to stop rapidly spreading malware; since these updates are payload based, they can block proliferation of future variants without any additional action or analysis.

In addition to protecting organizations from malicious and exploitive files and links, WildFire looks deeply into malicious outbound communication, disrupting command-and-control activity with anti-C2 signatures and DNS-based callback signatures. The information is also fed into URL Filtering with PAN-DB, where newly discovered malicious URLs are automatically blocked. This correlation of threat data and automated protections are key to identifying and blocking ongoing intrusion attempts and future attacks on your organization.

Integrated Logging, Reporting and Forensics

WildFire users receive integrated logs, analysis and visibility into WildFire events through the management interface, Panorama™, AutoFocus™ or the WildFire portal, enabling teams to quickly investigate and correlate events observed in their networks. This allows security staff to rapidly locate the data needed for timely investigations and incident response. Host-based and network-based indicators of compromise become actionable through log analysis and custom signatures.

To aid security and IR staff in discovering infected hosts, WildFire also provides:

- Detailed analysis of every malicious file sent to WildFire across multiple operating system environments, including both host-based and network-based activity.
- Session data associated with the delivery of the malicious file, including source, destination, application, User-ID™, URL, etc.
- Access to the original malware sample for reverse-engineering and full PCAPs of dynamic analysis sessions.
- An open API for integration with best-in-class SIEM tools, such as the Palo Alto Networks application for Splunk, and leading endpoint agents. This analysis provides a wealth of indicators of compromise (IOCs) that can be applied across the attack lifecycle.
- Native integration with Traps™ advanced endpoint protection and Aperture; advanced SaaS protection.
- Access to the actionable intelligence and global context provided by Palo Alto Networks AutoFocus threat intelligence service.
- Natively integrated with the correlation engine in our next- generation firewalls.

Maintaining the Privacy of Your Files

WildFire leverages a public cloud environment managed directly by Palo Alto Networks. All suspicious files are securely transferred between the Next-Generation Security Platform and the WildFire data center over encrypted connections, signed on both sides by Palo Alto Networks. Any files that are found to be benign are destroyed, while malware files are archived for further analysis.

WildFire Requirements:

- PAN-OS® 4.1+
- DF, Java, Office, and APK analysis require PAN-OS 6.0+
- Adobe Flash and webpage analysis require PAN-OS 6.1+

Licensing Information:

Basic WildFire functionality is available as a standard feature on all platforms running PAN-OS 4.1 or greater:

- Windows XP and Windows 7 image analysis
- EXE and DLL file types, including compressed (zip) and encrypted (SSL) content
- Automatic submission of suspicious files
- Automatic protections are delivered with regular threat prevention content updates (Threat Prevention license is required) every 24-48 hours

The WildFire subscription adds near-real time protection from advanced threats, including these additional features:

- Automatic WildFire signature updates every 15 minutes for all new malware detected anywhere in the world
- Enhanced file-type support, including: PE files (EXE, DLL, and others), all Microsoft Office file types, PDF files, and Java applets (JAR and CLASS)

WF-500

The WF-500 is an optional hardware appliance to support customers who choose to deploy WildFire as a private cloud for additional data privacy. The WF-500 is sized to accommodate most mid-range to large-scale networks, with the option of deploying additional appliances as traffic volumes increase or for networks that require geographic distribution.

The WF-500 can be deployed in a hybrid mode with the global WildFire services.

WF-500 Specifications

Processor	Memory	System Disk
Dual 6-Core Intel® Processor with Hyper -Threading Technology	128 GB RA 1	20GB SSD

Hardware Specifications

I/O Storage	Capacity	Power Supply
4x10/100/1,000 DB9 Console serial port, USB HDD for 2 TB of RAID storage	2TB RAID1: 4 x 1TB RAID Certified	Dual 920W power supplies in hot swap, redundant configuration
Max Power Consumption	**Rack Mountable (Dimensions)**	
390 Watts	2U, 19" standard rack (3.5"H x 21"D x 17.5"W)	
Max Btu/Hr	**Input Voltage (Input Frequency)**	
1300 BTU/hr	100-240VAC (50-60Hz)	
Max Current Consumption	**Safety**	
3.2A@120VAC	UL, CUL, CB	
EMI	**Environment**	
FCC Class A, CE Class A, VCCI Class A	Operating Temperature: 32 to 95 F, 5 to 35 C Non-operating Temperature: -4 to 158 F, -40 to 65 C	

To view additional information about the WF-500 security features and associated capacities, please visit www.paloaltonetworks.com/products.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

URL Filtering

An integrated approach to risk reduction

Fully integrated URL filtering database enables granular control over web browsing activity, complementing safe application enablement policies.

- Safely enable web usage with the same policy control mechanisms that are applied to applications—allow, allow and scan, apply QoS, block, and more.
- Reduce malware incidents by blocking access to known malware and phishing download sites.
- Tailor web filtering control efforts with white lists (allow), black lists (block), custom categories and database customization.
- Facilitate SSL decryption policies such as "don't decrypt traffic to financial services sites" but "decrypt traffic to blog sites".

Tech-savvy users are spending more and more time on their favorite website or using the latest and greatest web application. This unfettered web surfing and application use exposes organizations to security and business risks including propagation of threats, possible data loss, and lack of regulatory or internal policy compliance.

Stand-alone URL filtering solutions are insufficient control mechanisms because they are easily bypassed with external proxies (PHproxy, CGIproxy), translation sites (Google Translate, Bing Translator), search engine caches (Google Search, Internet Archive), circumventors (Tor, UltraSurf, Hamachi) and remote desktop access tools (GoToMyPC, RDP, SSH). Controlling users' application activity requires a integrated approach that implements policies to control web activity and the applications that are commonly used to bypass traditional security mechanisms.

Palo Alto Networks® next-generation firewalls natively classifies all traffic, inclusive of applications, threats and web content, then ties that traffic to the user, regardless of location or device type. The application, content and user, the business elements that run your business, are then used as the basis of all security policies. By addressing the lack of visibility and control from both the application and web content perspective, your organization is safeguarded from a full spectrum of legal, regulatory, productivity, and resource utilization risks.

paloalto NETWORKS®
the network security company™

Flexible, Policy-based Control

As a complement to the application visibility and control enabled by App-ID™, URL categories can be used as a match criteria for policies. Instead of creating policies that are limited to either allowing all or blocking all behavior, the URL category as a match criteria allows for exception-based behavior, resulting in increased flexibility yet more granular policy enforcement. Examples of how using URL categories can be used in policies include:

- Identify and allow exceptions to general security policies for users who may belong to multiple groups within Active Directory (e.g. deny access to malware and hacking sites for all users, yet allow access to users that belong to the security group).
- Allow access to streaming media category, but apply QoS to control bandwidth consumption.
- Prevent file download/upload for URL categories that represent higher risk (e.g. allow access to unknown sites, but prevent upload/download of executable files from unknown sites to limit malware propagation).
- Apply SSL decryption policies that allow encrypted access to finance and shopping categories but decrypt and inspect traffic to all other URL categories.

Tighten controls over common policy evasion tactics

URL filtering policies can be enforced even when common evasion tactics such as cached results and language translation sites are used.

- **Search engine cached results prevention:** a common tactic to evade controls is to access cached results within the popular search engines. URL filtering policies will be applied to cached results when end-users attempt to view the cached results of Google Search and Internet Archive.
- **Translation site filtering:** URL filtering policies are applied to URLs that are entered into translation sites such as Google Translate as a means of bypassing policies.

Safe Search Enforcement

Safe Search Enforcement allows you to prevent inappropriate content from appearing in users' search results. When this feature is enabled, only Google, Yahoo or Bing searches with the strictest Safe Search option set will be allowed; all other searches will be blocked.

Customizable URL Database and Categories

To account for each organization's unique traffic patterns, on-device caches are used to store the most recently accessed URLs. Devices can also automatically query a master cloud-based database for URL category information when an unknown URL is found. Lookup results are automatically inserted into the cache for future activity. Additionally, administrators can create custom URL categories to suit their specific needs.

Customizable End-User Notification

Each organization has different requirements on how best to inform end-users that they are attempting to visit a web page that is blocked according to the corporate policy and associated URL filtering profile. To accomplish this goal, administrators can use a custom block page to notify end users of the policy violation. The custom block page can include references to the username, IP address, the URL they are attempting to access, and the URL category. In order to place some of the web activity ownership back in the user's hands, administrators have two powerful options:

- **URL filtering continue:** when a user accesses a page that potentially violates URL filtering policy, a block page warning with a "Continue" button can be presented to the user, allowing them to proceed if they feel the site is acceptable.
- **URL filtering override:** requires a user to correctly enter a password in order to bypass the block page and continue surfing.

URL Activity Reporting and Logging

A set of pre-defined or fully customized URL filtering reports provides IT departments with visibility into URL filtering and related web activity including:

- **User activity reports:** an individual user activity report shows applications used, URL categories visited, websites visited, and a detailed report of all URLs visited over a specified period of time.
- **URL activity reports:** a variety of top 50 reports that display URL categories visited, URL users, websites visited, blocked categories, blocked users, blocked sites and more.
- **Real-time logging:** logs can be filtered through an easy-to-use query tool that uses log fields and regular expressions to analyze traffic, threat or configuration incidents. Log filters can be saved and exported and for more in-depth analysis and archival, logs can also be sent to a syslog server.

Deployment Flexibility

The unlimited user license behind each URL filtering subscription and the high performance nature of the Palo Alto Networks next-generation firewall means that customers can deploy a single appliance to control web activity for an entire user community without worrying about cost variations associated with user-based licensing.

paloalto NETWORKS®

the network security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

GLOBALPROTECT

Prevent Breaches and Secure the Mobile Workforce

GlobalProtect extends the protection of the Palo Alto Networks Next-Generation Security Platform to the members of your mobile workforce, no matter where they may go.

Key Usage Scenarios

Secures Internet Traffic

- Stops threats from reaching the endpoint
- Protects against phishing and credential theft

Enforces Acceptable Use Policies

- Filters access to malicious domains and adult content
- Prevents the use of avoidance and evasion tools to disguise traffic

Provides Remote Access VPN

- Provides secure access to internal and cloud-based business applications from laptops, tablets and smartphones

Secures Access to SaaS Applications

- Controls access and enforces policies for SaaS applications while blocking unsanctioned applications

Enables BYOD

- Secures business applications while respecting the boundaries for end-user privacy

Strengthens Internal Network Segmentation

- Delivers immediate and accurate user and host information for internal controls between corporate network segments

Key Benefits

- Blocks cybersecurity threats
- Maintains visibility in network traffic
- Consistently enforces security policy
- Reduces complexity
- Improves the user experience

The world that you need to secure continues to expand as both users and applications shift to locations outside of the traditional network perimeter. Security teams face challenges with maintaining visibility into network traffic and enforcing security policies to stop threats. Traditional technologies used to protect mobile endpoints, such as host endpoint antivirus software and remote access VPN, are not capable of stopping the advanced techniques employed by today's more sophisticated attacker.

GlobalProtect™ network security client for endpoints, from Palo Alto Networks®, enables organizations to protect the mobile workforce by extending the Next-Generation Security Platform to all users, regardless of location. It secures traffic by applying the platform's capabilities to understand application use, associate the traffic with users and devices, and enforce security policies with next-generation technologies.

Extending the Platform Externally

GlobalProtect safeguards the mobile workforce by inspecting all traffic using the organization's next-generation firewalls that are deployed as Internet gateways, whether at the perimeter, in the DMZ, or in the cloud. Laptops, smartphones and tablets with the GlobalProtect app automatically establish a secure SSL/IPsec VPN connection to the next-generation firewall with the best performance for a given location, thus providing the organization

with full visibility of all network traffic, for applications, and across all ports and protocols. By eliminating the blind spots in mobile workforce traffic, the organization maintains a consistent view into applications.

Securing the Network Internally

Not all users need access to every corner of the corporate network. Security teams are are adopting network segmentation to partition their network and enforce precise controls for access to internal resources. GlobalProtect provides the fastest, most authoritative User-ID information for the Next-Generation Security Platform, enabling organizations to write precise policies that allow or restrict access based on business need. Furthermore, GlobalProtect provides host information that establishes device criteria associated with security policies. These measures allow organizations to take preventive steps to secure their internal networks, adopt Zero Trust network controls, and reduce the attack surface area.

When GlobalProtect is deployed in this manner, the internal network gateways may be configured for use with or without a VPN tunnel.

Inspection of Traffic and Enforcement of Security Policies

GlobalProtect enables security teams to build policies that are consistently enforced, regardless of whether the user is internal or remote. Security teams can apply all of the platform's capabilities for cyberattack prevention, including:

- **App-ID™** – Identifies application traffic, regardless of port number, and enables organizations to establish policies to manage application usage based on users and devices.
- **User-ID™** – Identifies users and group memberships for visibility as well as the enforcement of role-based network security policies.
- **Decryption** – Inspect and control applications that are encrypted with SSL/TLS/SSH traffic. Stop threats within the encrypted traffic.
- **WildFire™** – WildFire cloud-based malware analysis automates the analysis of content to identify new, previously unknown, and highly targeted malware by its behavior and generates the threat intelligence to stop it in near-real time.
- **Threat Prevention for IPS and antivirus** – Intrusion prevention blocks network-based exploits targeting vulnerable applications and operating systems, DoS attacks and port scans. Antivirus profiles stop malware and spyware from reaching the endpoint using a stream-based engine.
- **URL Filtering with PAN-DB** – PAN-DB categorizes URLs based on their content at the domain, file and page level, and receives updates from WildFire so that when web content changes, so do categorizations.
- **File Blocking** – Stop the transfer of unwanted and dangerous files while further scrutinizing allowed files with WildFire.
- **Data Filtering** - Data filtering enables administrators to implement policies that can be used to stop the unauthorized movement of data, such as the transfer of customer information or other confidential content.

Identifying Users and Devices

User Authentication

GlobalProtect supports all of the existing PAN-OS® authentication methods, including Kerberos, RADIUS, LDAP, client certificates, and a local user database. Once GlobalProtect authenticates the user, it immediately provides the next-generation firewall with a user to IP address mapping that's used for User-ID.

Strong Authentication Options

GlobalProtect supports a range of third-party, multifactor authentication methods, including one-time password tokens, certificates and smart cards through RADIUS integration. These options help organizations strengthen the proof of identity for access to internal data center or SaaS applications.

GlobalProtect has options to make strong authentication even easier to use and deploy:

- **Cookie-based authentication:** After authentication, an organization may choose to use an encrypted cookie for subsequent access to a portal or gateway for the lifetime of that cookie.
- **Simplified certificate enrollment protocol support:** GlobalProtect can automate the interaction with an enterprise PKI for managing, issuing and distributing certificates to GlobalProtect clients.

Host Information Profile

GlobalProtect checks the endpoint to get an inventory of how it's configured and builds a Host Information Profile (HIP) that's shared with the next-generation firewall. The next-generation firewall uses the host information profile to enforce application policies that only permit access when the endpoint is properly configured and secured. These principles help enforce compliance with policies that govern the amount of access a given user should have with a particular device.

Host Information Profile policies can be based on a number of attributes, including:

- Operating system and application patch level
- Host anti-malware version and state
- Host firewall version and state
- Disk encryption configuration
- Data backup product configuration
- Customized host conditions (e.g., registry entries, running software)

Control Access to Applications and Data

Security teams can establish policies based on application, user, content and host information to maintain granular control over access to a given application. These policies may be associated with specific users or groups defined in a directory to ensure that organizations provide the correct levels of access based on business need. Users who have no need to access a particular application do not get access, thus providing prevention through risk reduction.

Architecture Matters

The flexible architecture for GlobalProtect provides many capabilities that help organizations solve an array of security challenges. At the most basic level, organizations can use GlobalProtect as a replacement for the traditional VPN gateway, eliminating the complexity and headaches of administering a stand-alone, third-party VPN gateway. Options for manual connections and gateway selection enable organizations to tailor the configuration to support business requirements as needed.

In a more comprehensive deployment for securing traffic, GlobalProtect can be deployed with an always-on VPN connection with a full tunnel, ensuring that protection is always present and transparent to the user experience.

GlobalProtect Specifications

VPN Connection

- IPsec
- SSL
- Automatic / manual connection
- Automatic / manual gateway selection

Host Information Profile

Host information profile match criteria includes:

- Patch management
- Host antispyware
- Host antivirus
- Host firewall
- Disk encryption
- Disk backup
- Data loss prevention
- Customized host conditions (e.g. registry entries, running software)

Authentication Methods

- LDAP
- Client certificates
- Kerberos
- RADIUS
- Local user database
- Two factor authentication

Management Tools and APIs

- Palo Alto Networks Next-Generation Security Platform, including physical (such as the PA-7000 Series, the PA-3000 Series and the PA-200) and virtual (VM-Series) form factors.
- Autoscaling supported on VM-Series for Amazon® Web Services

Cloud-Based Internet Gateways

Workforces shift from one location to another, creating changes in traffic load. This is especially true when considering how companies evolve, whether on a temporary (such as a natural disaster in a region) or permanent (such as entering new markets) basis.

In order to maintain excellent performance for all users, no matter where they go, GlobalProtect can automatically adapt to changing conditions by dynamically adjusting the number of cloud-based Internet gateway firewalls that are available. GlobalProtect handles these changes automatically, with no disruption to the user experience.

Conclusion

The protections provided by the Palo Alto Networks Next-Generation Security Platform play a critical role in preventing breaches. Use GlobalProtect to extend the protection of the platform to users wherever they go. By using GlobalProtect, organizations can get consistent enforcement of security policy so that, even when users leave the building, their protection from cyberattack remains in place.

GlobalProtect App Specifications

Supported Platforms

- Microsoft® Windows® 10, Surface™ Pro, 8.1, 8, 7, Vista®, XP
- Apple® Mac OS® X® 10.6 and later
- Android™ 4.0.3 and later
- Apple iOS 6.0 and later
- Google® Chrome® OS
- Linux® supported using third-party vpnc and StrongSwan client

Localization

- English
- Spanish
- German
- French
- Japanese
- Chinese

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

VERISTOR

Quote Date: 8/4/16
Exp Date: 9/4/16
Quote No: AR3-93330-02

VeriStor Systems, Inc
4850 River Green Parkway
Duluth, GA 30096
Phone: 678-990-1593
Fax: 678-990-1597

Quote Prepared For:

Company Name	West Virginia Secretary of State
Customer Contact	Linda Harper
Address	2019 Washington Ave East
City, State, Zip	Charleston, WV 25305
Phone #	304-558-6000
Customer Email	linda.b.harper@wv.gov

Core Netwok Equipment and Software Response
CRFQ,1600,SOS1700000001

Item No.	Description	Qty	Price	Extended Price
	HP - 4 Year Support			
JH333A	HPE 7510 w 2x2.4Tbps MPU/Fabric Bundle	1	$19,802.00	$19,802.00
JD227A	HPE 7500 6000W AC Power Supply	2	$2,573.00	$5,146.00
JG663A	HPE 7500 48p 1000BASE-T PoE+ SC Mod	5	$3,606.00	$18,030.00
JF290A	HPE 7500 8-port 10G SFP+ Module	2	$8,005.00	$16,010.00
JD092B	HPE X130 10G SFP+ LC SR Transceiver	10	$483.00	$4,830.00
H8B33A4	HPE 4Y Proactive Care Adv NBD Service	1	$0.00	$0.00
H8B33A4 R4B	HPE Networks 7510 Switch Support	1	$27,612.00	$27,612.00
	Cisco			
C3KX-NM-10GT=	CAT 3K-K10G-T NTWK MOD	1	$1,772.00	$1,772.00
	Palo Alto			
PAN-PA-3060	Palo Alto Networks PA-3060	2	$28,000.00	$56,000.00
PAN-PA-3060-GP-HA2	GlobalProtect Gateway subscription for device in an HA pair year 1, PA-3060	2	$3,920.00	$7,840.00
PAN-PA-3060-URL4-HA2	PANDB URL Filtering subscription for device in an HA pair year 1, PA-3060	2	$3,920.00	$7,840.00
PAN-PA-3060-WF-HA2	WildFire subscription for device in an HA pair year 1, PA-3060	2	$3,920.00	$7,840.00
PAN-SVC-PREM-3060	Premium support year 1, PA-3060	2	$4,945.00	$9,890.00
	VeriStor Professional Services			
Switching	Install and Integrate HP 7510 Chassis •5 x 48-port 1G modules •2 x 8-port 10G modules	1	$7,475.00	$7,475.00
Firewall	Install and Migrate Palo Alto 3060 HA Pair •Replaces ASA 5020 •Firewall Project Plan •Stage 1 - Pre-Implementation [1] •Stage 2 - Hardware/Software installation [1] •Stage 3 - Off-site configuration migration [1] •Stage 4 - On-site configuration migration and initial knowledge transfer [2] •Stage 5 - Hardware turn-up and cutover [1] •Stage 6 - On-site knowledge transfer [1] •Stage 7 - On-site follow-up and App-ID migration [1]	1	$14,949.00	$14,949.00

Total: $205,036.00

Account Executive: Justin Richardson
Phone: 678-990-1593
Email:jrichardson@veristor.com

All prices are in U.S. Dollars and are exclusive of sales, use or like taxes.
Pricing is valid for 30 days unless otherwise extended in writing by VeriStor.
FOB Origin - Customer will be responsible for Shipping cost once unit has been shipped.
Payment Terms: Net-30 Days