QuickSpecs

Overview

Aruba ClearPass Policy Manager Platform

**The most advanced Secure NAC platform available**

The Aruba ClearPass Policy Manager, part of the Aruba 360 Secure Fabric, provides role- and device-based secure network access control for IoT, BYOD, corporate devices, as well as employees, contractors and guests across any multivendor wired, wireless and VPN infrastructure.

With a built-in context-based policy engine, RADIUS, TACACS+, non-RADIUS enforcement using OnConnect, device profiling, posture assessment, onboarding, and guest access options, ClearPass is unrivaled as a foundation for network security for organizations of any size.

For comprehensive integrated security coverage and response using firewalls, UEM and other existing solutions, ClearPass supports the Aruba 360 Security Exchange Program. This allows for automated threat detection and response workflows that integrate with third- party security vendors and IT systems previously requiring manual IT intervention.

In addition, ClearPass supports secure self-service capabilities, making it easier for end users trying to access the network. Users can securely configure their own devices for enterprise use or Internet access based on admin policy controls. Aruba wireless customers in particular can take advantage of unique integration capabilities such as AirGroup, as well as ClearPass Auto Sign-On (ASO). ASO enables a user's network authentication to pass automatically to their enterprise mobile apps so they can get right to work.

The result is detailed visibility of all wired and wireless devices connecting to the enterprise, increased control through simplified and automated authentication or authorization of devices, and faster, better incident analysis and response through the integration and orchestration with third-party security solutions. This is achieved with a comprehensive and scalable policy management platform that goes beyond traditional AAA solutions to deliver extensive enforcement capabilities for IT-owned and BYOD security requirements.
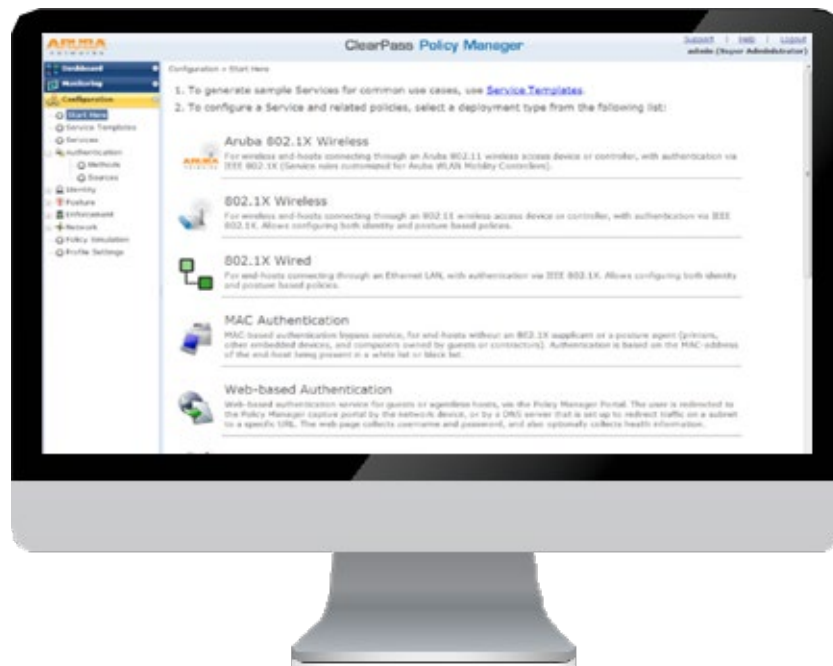
Aruba ClearPass Policy Manager Platform

Standard Features

Key Features
- Role-based, unified network access enforcement across multi-vendor wireless, wired and VPN networks.
- Intuitive policy configuration templates and visibility troubleshooting tools.
- Supports multiple authentication/authorization sources (AD, LDAP, SQL).
- Self-service device onboarding with built-in certificate authority (CA) for BYOD.
- Guest access with extensive customization, branding and sponsor-based approvals.
- Integration with key UEM solutions for in-depth device assessments.
- Comprehensive integration with the Aruba 360 Security Exchange Program.
- Single sign-on (SSO) support works with Ping, Okta and other identity management tools to improve user experience to SAML 2.0-based applications.

The ClearPass Difference
ClearPass is the only policy platform that centrally enforces all aspects of enterprise-grade access security for any industry. Granular policy enforcement is based on a user's role, device type and role, authentication method, UEM attributes, device health, traffic patterns, location, and time-of-day.

Deployment scalability supports tens of thousands of devices and authentications which surpasses the capabilities offered by legacy AAA solutions. Options exist for small to large organizations, from centralized to distributed environments.

Advanced Policy Management

Enforcement and visibility for wired and wireless
With ClearPass, organizations can deploy wired or wireless using standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT and headless devices that may lack support for 802.1X. For wired environments where RADIUS based authentication cannot be deployed, OnConnect, offers an alternative using SNMP based enforcement.

Authentication methods can be used to concurrently support a variety of use-cases. It also includes support for multi- factor authentication based on log-in times, posture checks, and other context such as new user, new device, and more.

Attributes from multiple identity stores such as Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers and internal databases across domains can be used within a single policy for fine- grained control.

Contextual data from these profiled devices allows for IT to define what devices can access either the wired, VPN, or wireless network. Device profile changes are dynamically used to modify authorization privileges. For example, if a Windows laptop appears as a printer, ClearPass policies can automatically deny access.

Secure device configuration of personal devices
ClearPass Onboard provides automated provisioning of any Windows, macOS, iOS, Android, Chromebook, and Ubuntu devices via a user driven self-guided portal. Network details, security settings and unique device identity certificates are automatically configured on authorized devices. Cloud identity services like Microsoft Azure Active Directory, Google G Suite and Okta can also be leveraged as identity providers with Onboard for secure certificate enrollment.

Device health checks
ClearPass OnGuard delivers endpoint posture assessments over wireless, wired and VPN connections. OnGuard's health-check capabilities ensure endpoints meet security and compliance policies before they connect to the network. OnGuard offers a variety of flexible deployment options including agentless, dissolvable agents and agent-based configuration.

Customizable visitor management
ClearPass Guest simplifies visitor workflow processes to enable employees, receptionists, and other non-IT staff to create temporary guest accounts for secure wireless and wired access. Highly customizable, mobile friendly portals provide easy-to-use login processes that include self- registration, sponsor approval, and bulk credential creation support any visitor needs - enterprise, retail, education, large public venue. Credentials can be delivered by SMS, email, printed badges, or input directly through cloud identity providers such as Facebook or Twitter.

Built in support for commercial oriented guest Wi-Fi hotspots with credit card billing and 3rd party advertising driven workflows make it simple to integrate into a wide variety of environments.

Standard Features

Aruba 360 Security Exchange Program

Integrate with security and workflow systems
Support for the Aruba 360 Security Exchange Program is an integrated component of ClearPass. Using features like REST- based APIs, RADIUS Accounting Proxy, and Syslog ingestion help facilitate workflows with UEM, SIEM, firewalls, help-desk systems and more. Context is shared between each component for end-to-end policy enforcement and visibility. The ClearPass Ingress Event

Engine provides 3rd party systems the means to share information in real-time using Syslog. This enables ClearPass to respond to changing threats for users and devices after they have authenticated to the network. By utilizing an open dictionary approach, anyone can write a parsing ruleset without the need for costly add-ons or locked in 3rd party ecosystems.

Advanced Reporting and Alerting
ClearPass Insight provides advanced reporting capabilities via customizable reports. Information about authentication trends, profiled devices, guest data, on-boarded devices, and endpoint health can also be viewed in an easy to use dashboard. Insight also has support for granular alerts and a watchlist to monitor specific authentication failures.

Hardware/Virtual Appliance Warranty
- Hardware
  1 year parts*
- Software
  90 days*

Notes: * Extended with support contract

Perpetual Licenses Warranty
- Software
  90 days*

Notes: * Extended with support contract, R1V82A

Expandable application software
- ClearPass Onboard – device configuration and certificate management
- ClearPass OnGuard – endpoint device health

Notes: Refer to ClearPass Onboard Datasheet

Configuration Information

Ordering Guidance
Please refer to the ClearPass Scaling & Ordering Guide for detailed information on appropriate sizing and required licensing to deploy ClearPass. This can be found on the Aruba support website in the **ClearPass documentation section.**

BTO Models

Rule #	Description	SKU
	Hardware Appliances	
Notes:	Includes 1 PSU and 1 US Power Cord	
1	Aruba ClearPass C3010 DL360 Gen10 HW-Based Appliance	R1V82A
1, 2	Aruba ClearPass C1000 S-1200 R4 HW-Based Appliance	JZ508A
	Aruba ClearPass C3010 DL360 Gen10 HW-Based Appliance	R1V82A
	Virtual Appliances	
	Aruba ClearPass Cx000V VM-Based Appliance E-LTU	JZ399AAE
	Configuration Rules	
1	Bring in (Min 1 // Max 1) Localized power cord based on the Aruba Localization Menu	
2	If JW124A is the selected localized power cord, do not add Localized Power Cord	
Notes:	The ClearPass C1000 S-1200 R4 and ClearPass C2000 DL20 Gen9 HW-Based Appliance include a U.S. power cord(will not be displayed in BOM). The ClearPass C2010 DL20 Gen10 and the ClearPass C3010 DL360 Gen10 HW-Based Appliance includes a C13 - C14 WW 250V 10Amp Jumper Cord. The redundant PSUs for all models include a C13 - C14 WW 250V 10Amp Jumper Cord. When configuring a ClearPass C3010 DL360 Gen 10 HW-Based Appliance, A country specific power cord will be automatically added to the BOM.	

Power Supplies

Rule #	Description	SKU
	Power Options	
	Std (Min 0 // max 99) User Selection (min 0 // max 99)	
1, 5	Aruba DL360 Gen10 500W Spare PSU	R1T38A
	Configuration Rules	
1	Bring in (Min 1 // Max 1) Localized power cord based on the Aruba Localization Menu	
5	This PSU is only supported on the R1V82A and R1V81A	
Notes:	Redundant Power Supply includes a IEC C13 - C14 Jumper Cable	

Related Options

Licenses

Remarks	Description	SKU
	Perpetual Licenses	
	Aruba ClearPass New Licensing Access 100 Concurrent Endpoints E-LTU	JZ400AAE
	Aruba ClearPass New Licensing Access 500 Concurrent Endpoints E-LTU	JZ401AAE
	Aruba ClearPass New Licensing Access 1K Concurrent Endpoints E-LTU	JZ402AAE
	Aruba ClearPass New Licensing Access 2500 Concurrent Endpoints E-LTU	JZ403AAE
	Aruba ClearPass New Licensing Access 5K Concurrent Endpoints E-LTU	JZ404AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints E-LTU	JZ405AAE
	Aruba ClearPass New Licensing Access 25K Concurrent Endpoints E-LTU	JZ406AAE
	Aruba ClearPass New Licensing Access 50K Concurrent Endpoints E-LTU	JZ407AAE
	Aruba ClearPass New Licensing Access 100K Concurrent Endpoints E-LTU	JZ408AAE
	Aruba ClearPass New Licensing Entry 100 Concurrent Endpoints E-LTU	R1U35AAE
	Aruba ClearPass New Licensing Entry 500 Concurrent Endpoints E-LTU	R1U36AAE
	Aruba ClearPass New Licensing Entry 1K Concurrent Endpoints E-LTU	R1U37AAE
	Aruba ClearPass New Licensing Entry 2500 Concurrent Endpoints E-LTU	R1U38AAE
	Aruba ClearPass New Licensing Entry 5K Concurrent Endpoints E-LTU	R1U39AAE
	Aruba ClearPass New Licensing Entry 10K Concurrent Endpoints E-LTU	R1U40AAE
	Aruba ClearPass New Licensing Entry 25K Concurrent Endpoints E-LTU	R1U41AAE
	Aruba ClearPass New Licensing Entry 50K Concurrent Endpoints E-LTU	R1U42AAE
	Aruba ClearPass New Licensing Entry 100K Concurrent Endpoints E-LTU	R1U43AAE
	Aruba ClearPass New Licensing Access Upgrade 100 Concurrent Endpoints E-LTU	R1U44AAE
	Aruba ClearPass New Licensing Access Upgrade 500 Concurrent Endpoints E-LTU	R1U45AAE
	Aruba ClearPass New Licensing Access Upgrade 1K Concurrent Endpoints E-LTU	R1U46AAE
	Aruba ClearPass New Licensing Access Upgrade 2500 Concurrent Endpoints E-LTU	R1U47AAE
	Aruba ClearPass New Licensing Access Upgrade 5K Concurrent Endpoints E-LTU	R1U48AAE
	Aruba ClearPass New Licensing Access Upgrade 10K Concurrent Endpoints E-LTU	R1U49AAE
	Aruba ClearPass New Licensing Access Upgrade 25K Concurrent Endpoints E-LTU	R1U50AAE
	Aruba ClearPass New Licensing Access Upgrade 50K Concurrent Endpoints E-LTU	R1U51AAE
	Aruba ClearPass New Licensing Access Upgrade 100K Concurrent Endpoints E-LTU	R1U52AAE
	Subscription Licenses (1 Year)	
	Aruba ClearPass New Licensing Access 100 Concurrent Endpoints 1yr E-STU	JZ409AAE
	Aruba ClearPass New Licensing Access 500 Concurrent Endpoints 1yr E-STU	JZ410AAE
	Aruba ClearPass New Licensing Access 1K Concurrent Endpoints 1yr E-STU	JZ411AAE
	Aruba ClearPass New Licensing Access 2500 Concurrent Endpoints 1yr E-STU	JZ412AAE
	Aruba ClearPass New Licensing Access 5K Concurrent Endpoints 1yr E-STU	JZ413AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 1yr E-STU	JZ414AAE
	Aruba ClearPass New Licensing Access 25K Concurrent Endpoints 1yr E-STU	JZ415AAE
	Aruba ClearPass New Licensing Access 50K Concurrent Endpoints 1yr E-STU	JZ416AAE
	Aruba ClearPass New Licensing Access 100K Concurrent Endpoints 1yr E-STU	JZ417AAE

Related Options

Remarks	Description	SKU
	Subscription Licenses (3 Year)	
	Aruba ClearPass New Licensing Access 100 Concurrent Endpoints 3yr E-STU	JZ418AAE
	Aruba ClearPass New Licensing Access 500 Concurrent Endpoints 3yr E-STU	JZ419AAE
	Aruba ClearPass New Licensing Access 1K Concurrent Endpoints 3yr E-STU	JZ420AAE
	Aruba ClearPass New Licensing Access 2500 Concurrent Endpoints 3yr E-STU	JZ421AAE
	Aruba ClearPass New Licensing Access 5K Concurrent Endpoints 3yr E-STU	JZ422AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 3yr E-STU	JZ423AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 3yr E-STU	JZ423AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 3yr E-STU	JZ423AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 3yr E-STU	JZ423AAE
	Subscription Licenses (5 Year)	
	Aruba ClearPass New Licensing Access 100 Concurrent Endpoints 5yr E-STU	JZ427AAE
	Aruba ClearPass New Licensing Access 500 Concurrent Endpoints 5yr E-STU	JZ428AAE
	Aruba ClearPass New Licensing Access 1K Concurrent Endpoints 5yr E-STU	JZ429AAE
	Aruba ClearPass New Licensing Access 2500 Concurrent Endpoints 5yr E-STU	JZ430AAE
	Aruba ClearPass New Licensing Access 5K Concurrent Endpoints 5yr E-STU	JZ431AAE
	Aruba ClearPass New Licensing Access 10K Concurrent Endpoints 5yr E-STU	JZ432AAE
	Aruba ClearPass New Licensing Access 25K Concurrent Endpoints 5yr E-STU	JZ433AAE
	Aruba ClearPass New Licensing Access 50K Concurrent Endpoints 5yr E-STU	JZ434AAE
	Aruba ClearPass New Licensing Access 100K Concurrent Endpoints 5yr E-STU	JZ435AAE
	Customized Guest Portal	
	Aruba ClearPass Guest Custom Skin Delivery E-LTU	JW470AAE

Notes: If Custom Skin Sku is selected, then fire Clic Notification and OCA Display Note under "Software" Tab of ClearPass - Policy Manager:
Once order is placed, please complete the form **https://forms.office.com/r/yunmJXTw5i** to ensure that the order is able to be processed quickly. Without this information orders may be delayed in delivery or rejected.

Technical Specifications

Appliance Specifications

	C1000 Appliance (JZ508A)	C2000 Appliance (JZ509A)	C2010 Appliance (R1V81A)	C3010 Appliance (R1V82A)
Hardware model	Unicom S-1200 R4	HPE DL20 Gen 9	HPE DL20 Gen10	HPE DL360 Gen10
CPU	(1) Eight Core 2.4GHz Atom C2758	(1) Xeon 3.5Ghz E3-1240v5 with four cores (8 threads)	(1) Xeon 4.0GHz E-2274G with four cores (8 threads)	(1) Xeon 2.3Ghz 5118 with twelve cores (24 threads)
Memory	8 GB	16 GB	16 GB	64GB
Hard drive storage	(1) SATA (7.3K RPM) 1TB hard drive	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) SAS (10K RPM) 600GB Hot-Plug hard drives, RAID-10 controller
Out of band management	N/A	HPE Integrated Lights-Out (iLO) Standard	HPE Integrated Lights-Out (iLO)	HPE Integrated Lights-Out (iLO) Advanced
Network interfaces	4 x 1GbE	2 x 1GbE	4 x 1GbE	4 x 1GbE
Serial port	Yes (RJ-45)	Yes (virtual serial via iLO)	Yes (DB-9)	Yes (DB-9)
Performance and scale	Please refer to the ClearPass Scaling and Ordering Guide	Please refer to the ClearPass Scaling and Ordering Guide	Please refer to the ClearPass Scaling and Ordering Guide	Please refer to the ClearPass Scaling and Ordering Guide

Form Factor

Rackmount	Included	1U SFF Easy Install Rail 1U Cable Management Arm	1U SFF Easy Install Rail 1U Cable Management Arm	1U SFF Easy Install Rail 1U Cable Management Arm
Dimensions (WxHxD)	17.2 x 1.7 x 11.3"	17.11 x 1.70 x 15.05"	17.11" x 1.70" x 15.05"	17.1 x 1.7 x 27.8"
Weight (Max Config)	8.5 lbs	Up to 19.18 lbs	Up to 19.18 lbs	Up to 36 lbs

Power

Power supply	200 watts max	HPE 900W AC 240VDC Power Input FIO Module*	HPE 500W Flex Slot Platinum Hot Plug Power Supply	HPE 500W Flex Slot Platinum Hot Plug Power Supply

Notes: *The HPE 900W Redundant Power Supply supports 100VAC to 240VAC and also supports 240VDC., R1V82A

Power cord	C13 - NEMA 5-15P US/CA 110V 10Amp Power Cord	C13 - NEMA 5-15P US/CA 110V 10Amp Power Cord	C13 - C14 WW 250V 10Amp Jumper Cord	C13 - C14 WW 250V 10Amp Jumper Cord
Power redundancy	N/A	Optional	Optional	Optional
AC input voltage	100/240 VAC auto-selecting	100/240 VAC auto-selecting	100/240 VAC auto-selecting	100/240 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting	50/60 Hz auto-selecting	50/60 Hz auto-selecting	50/60 Hz auto-selecting

Environmental

Operating temperature	5° to 35° C (41° to 95° F)	10° to 35° C (50° to 95° F)	10° to 35° C (50° to 95° F)	10° to 35° C (50° to 95° F)
Operating vibration	0.25 G at 5 Hz to 200 Hz for 15 minutes	Random vibration at 0.000075 G²/Hz, 10Hz to 300Hz, (0.15 G's	Random vibration at 0.000075 G²/Hz, 10Hz to 300Hz, (0.15 G's	Random vibration at 0.000075 G²/Hz, 10Hz to 300Hz, (0.15 G's
Operating shock	1 shock pulse of 20 G for up to 2.5 ms	2 G's	2 G's	2 G's
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)	3,050 m (10,000 ft)	3,050 m (10,000 ft)	3,050 m (10,000 ft)

Technical Specifications

Appliances
ClearPass is available as hardware or as a virtual appliance. Virtual appliances are supported on VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, CentOS KVM & Amazon EC2.
- VMware ESXi up to 7.0
- Microsoft Hyper-V 2012/2016 R2/2019 and Windows 2012/2016 R2 Enterprise
- KVM on CentOS 7.7
- Amazon AWS (EC2)

Platform
- Deployment templates for any network type, identity store and endpoint
- 802.1X, MAC authentication and captive portal support
- ClearPass OnConnect for SNMP-based enforcement on wired switches
- Advanced reporting, analytics and troubleshooting tools
- Interactive policy simulation and monitor mode utilities
- Multiple device registration portals - Guest, Aruba AirGroup, BYOD, and un-managed devices
- Admin/operator access security via CAC and TLS certificates

Framework and protocol support
- RADIUS, RADIUS CoA, TACACS+, web authentication, SAML v2.0
- RadSec (TLS encoded RADIUS)
- TEAP (tunneled EAP)
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP- Public, EAP-PWD)
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1 and 2, EAP-MD5
- OAuth2
- WPA3
- Windows machine authentication
- SMB v2/v3
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF), and RFC5424

Supported identity stores
- Microsoft Active Directory
- RADIUS
- Any LDAP compliant directory
- MySQL, Microsoft SQL, PostGRES and Oracle 11g ODBC-compliant SQL server
- Token servers
- Built-in SQL store, static hosts list
- Kerberos
- Microsoft Azure Active Directory
- Google G Suite

RFC standards
2246, 2248, 2407, 2408, 2409, 2548, 2759, 2865, 2866, 2869, 2882, 3079, 3579, 3580, 3748, 3779, 4017, 4137, 4301, 4302, 4303, 4308, 4346, 4514, 4518, 4809, 4849, 4851, 4945, 5176, 5216, 5246, 5280, 5281, 5282, 5424, 5755, 5759, 6614, 6818, 6960, 7030, 7170, 7296, 7321, 7468, 7815, 8032, 8247

Technical Specifications

Internet drafts
Protected EAP Versions 0 and 1, Microsoft CHAP extensions, dynamic provisioning using EAP-FAST, TACACS+, draft-ietf- curdle-pkix-00 EdDSA, Ed25519, Ed448, Curve25519 and Curve448 for X.509, draft-nourse-scep-23 (Simple Certificate Enrollment Protocol)

Profiling methods
- Active: Nmap, WMI, SSH, SNMP
- Passive: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, 'SPAN' Port, HTTP User-Agent, IF-MAP
- Integrated & 3rd Party: Onboard, OnGuard, ArubaOS, EMM/MDM, Cisco device sensor

IPv6 Support
- RADIUS
- TACACS+
- Clustering (intra-node communication)
- Web and CLI based management
- IPv6 addressed authentication & authorization servers
- IPv6 accounting proxy
- IPv6 addressed endpoint context servers
- Syslog, DNS, NTP, IPsec IPv6 targets
- IPv6 Virtual IP for high availability
- HTTP Proxy
- Ingress Event Engine Syslog sources

Information assurance validations
- FIPS 140-2 – Certificate #2577
- Common Criteria NDcPP + Authentication Server (ClearPass)
- USGv6 approved

Summary of Changes

Date	Version History	Action	Description of Change
04-May-2021	Version 11	Changed	Configuration Information section was updated.
06-Jul-2020	Version 10	Changed	Overview, Standard Features, Configuration Information and Technical Specification sections were updated. New SKU was added.
04-May-2020	Version 9	Changed	Configuration Information section was updated.
12-Mar-2020	Version 8	Changed	Technical Specification section was updated.
18-Nov-2019	Version 7	Changed	Configuration Information, section was updated. Obsolete SKUs were removed.
05-Aug-2019	Version 6	Changed	SKU added R1V82A Configuration Information, Related Options and Technical Specification sections were updated.
04-Mar-2018	Version 5	Changed	SKUs added: R1U35AAE, R1U36AAE, R1U37AAE, R1U38AAE, R1U39AAE, R1U40AAE, R1U41AAE, R1U42AAE, R1U43AAE, R1U44AAE, R1U45AAE, R1U46AAE, R1U47AAE, R1U48AAE, R1U49AAE, R1U50AAE, R1U51AAE, R1U52AAE Overview section updated
18-Dec-2017	Version 4	Changed	Minor edit on Configuration section
04-Dec-2017	Version 3	Changed	SKUs added: JZ508A, JZ509A, JZ510A, JZ399AAE, JX923A All document sections updated
07-Nov-2016	Version 2	Added	SKUs added: JW771A, JW772A
01-Nov-2016	Version 1	New	New QuickSpecs

Copyright

**Make the right purchase decision.
Contact our presales specialists.**

Chat   **Email**   **Call**

Get updates

**Hewlett Packard
Enterprise**

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

c05272683 - 15701 - Worldwide - V11 - 04-May-2021