HPE Networking Instant On 1960 Switch Series

Release Notes

Instant On

Hewlett Packard Enterprise

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

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

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

All third-party marks are property of their respective owners.

Chapter 1
Release Notes

Description

This release note covers software versions for the 3.4.0 branch of the software.

Product series supported by this software:

- HPE Networking Instant On 1960 Switch Series

Important Information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

HPE Networking Instant On recommends always updating to the latest version of software to ensure the best performance for your switch.

Version History

All released versions are fully supported by HPE Networking Instant On, unless noted in the table.

Version number	Release date	Remarks
3.4.0	2026-06-26	Release of version 3.4.0 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.3.4	2026-03-26	Release of version 3.3.4 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.3.2	2025-12-11	Release of version 3.3.2 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.3.0	2025-08-28	Release of version 3.3.0 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.2.0	2025-03-11	Release of version 3.2.0 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.1.0	2024-11-25	Release of version 3.1.0 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.
3.0.0	2024-07-02	Release of version 3.0.0 of the HPE Networking Instant On 1960 software. Released, fully supported, and posted to the web.

Version number	Release date	Remarks
2.9.1.17	2024-03-15	Release of version 2.9.1.17 of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.
2.9.0.53	2023-11-01	Released, fully supported, and posted to the web.
2.8.1.35	2023-09-19	Released, fully supported, and posted to the web.
2.8.0.17	2023-03-16	Release of version 2.8.0.17 of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.
2.7.0.103	2022-11-09	Release of version 2.7.0.103 of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.
2.6.0.73	2022-06-23	Release of version 2.6.0.73 of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.
2.5.0.67	2022-02-07	Release of version 2.5.0.67 of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.
2.4.0	2021-11-01	Initial release of the Aruba Instant On 1960 software. Released, fully supported, and posted to the web.

Products Supported

This release applies to the following product models:

Product number	Description
JL805A	HPE Networking Instant On Switch 12p 10GBT 4p SFP+ 1960
JL806A	HPE Networking Instant On Switch 24p Gigabit 2p 10GBT 2p SFP+ 1960
JL807A	HPE Networking Instant On Switch 20p Gigabit CL4 4p Gigabit CL6 PoE 2p 10GBT 2p SFP+ 370W 1960
JL808A	HPE Networking Instant On Switch 48p Gigabit 2p 10GBT 2p SFP+ 1960
JL809A	HPE Networking Instant On Switch 40p Gigabit CL4 8p Gigabit CL6 PoE 2p 10GBT 2p SFP+ 600W 1960
S0F35A	HPE Networking Instant On Switch 8p Gigabit CL4 4p SR2.5G CL6 PoE 2p 10GBT 2p SFP+ 480W 1960

Compatibility/Interoperability

The switch web agent supports the following web browsers:

Operating system	Browser
Windows 7	Chrome version 87 or higher Firefox version 84 or higher
Windows 10	Chrome version 87 or higher Firefox version 84 or higher
Mac OS X 10.15	Safari version 14 or higher Chrome version 87 or higher Firefox version 84 or higher
Linux OS 2.6, 3.11	Chrome version 87 or higher Firefox version 84 or higher

HPE Networking Instant On recommends using the most recent version of each browser as of the date of this release note.

Enhancements

This section lists released builds that include enhancements found in this branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

Version 3.4.0

There are no new feature enhancements in this release.

Version 3.3.4

There are no new feature enhancements in this release.

Version 3.3.2

There are no new feature enhancements in this release.

Version 3.3.0

There are no new feature enhancements in this release.

Version 3.2.0

There are no new feature enhancements in this release.

Version 3.1.0

Type	Description
Stacking	In stack topologies, each switch will now display its own serial number and MAC address, instead of just showing the information of the conductor switch.
Security	Added the setting to ensure all types of RADIUS responses from the specified RADIUS server include the Message-Authenticator attribute. By default, this setting is disabled.

Version 3.0.0

Type	Description
IGMP	IGMP querier limit is increased from 16 to 32.
WebUI	Local web management pages are updated with the HPE Networking Instant On brand.

Version 2.9.1.17

Type	Description
Transceivers	Added support for the following HPE Networking Instant On transceivers: ■ S0G21A: HPE NW ION 10G SFP+ LC LR 10km SMF XCVR ■ S0G20A: HPE NW ION 1G SFP LC LX 10km SMF XCVR ■ S0G18A: HPE NW ION 10GBASE-T RJ45 30m Cat6A XCVR

NOTE

Added support for HPE Networking Instant On 10GBase-T transceivers.

Version 2.9.0.53

Type	Description
SNMP	Added an SNMP Filter Configuration interface to the SNMP webpage.
Stacking	Provided a warning message informing the customer a reboot is required to activate stacking interfaces.

Version 2.8.1.35

There are no new features or enhancements in this release.

Version 2.8.0.17

There are no new features or enhancements in this release.

Version 2.7.0.103

Type	Description
Interoperability	Multiple enhancements have been made to improve interoperability with third-party devices.
SNMP	Update to ensure switches use the default SNMP engineID following config-file upload.
WebUI	Added HTTP or HTTPS RADIUS device management authentication settings.
WebUI	Fixed maximum number of stack ports supported in online help.
WebUI	Corrected errors in the online help.

Version 2.6.0.73

Type	Description
SNMP	Removed restriction to allow SNMP management from non-management VLANs.

Version 2.5.0.67

There are no new feature enhancements in this release.

Version 2.4.0

There are no new feature enhancements in this release.

Fixes

This section lists released builds that include fixes found in this branch of the software. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

The Symptom statement describes what a user might experience if this is seen on the network. The Scenario statement provides additional environment details and trigger summaries. When available, the Workaround statement provides a workaround to the issue for customers who decide not to update to this version of software.

The number that precedes the fix description is used for tracking purposes.

Version 3.4.0

Type	Bug ID	Description
Security	33406-0001	**Symptom/Scenario:** Resolves security vulnerabilities in zlib open-source: CVE-2016-9840, CVE-2016-9841, CVE-2016-9843, CVE-2022-37434, and CVE-2018-25032 **Workaround**: N/A
Security	33406-0002	**Symptom/Scenario:** Resolves security vulnerabilities in OpenSSH open-source: CVE-2016-10708, CVE-2017-15906, CVE-2018-15473 and CVE-2020-14145 **Workaround**: N/A
Security	33406-0003	**Symptom/Scenario:** Resolves security vulnerabilities in Linux OS: CVE-2022-48839 **Workaround**: N/A
VLAN	SMBS-223	**Symptom/Scenario:** The switch could crash if a new VLAN interface is initially set to use DHCP and is later changed to use a static IP address. **Workaround**: N/A
Port Security	SMBS-188	**Symptom/Scenario:** When Port Security is enabled, IP phones may fail to rejoin the voice VLAN after being disconnected and reconnected. **Workaround**: Disable Port Security on ports intended to be used on the Voice VLAN
MSTP	SMBS-230	**Symptom/Scenario:** The MSTP port configuration is missing from the Support File when multiple MSTP instances are configured. **Workaround**: N/A

Version 3.3.4

Type	Bug ID	Description
WebUI	33403-0001	**Symptom/Scenario:** HTTPS certificate private key is displayed when the web session is connected over HTTP. **Workaround**: N/A
Stacking	SMBS-215	**Symptom/Scenario:** Stacking ports do not generate an SNMP trap for link up/ link down events. **Workaround**: Stacking ports link up/ link down events can be viewed in the syslog.

Version 3.3.2

Type	Bug ID	Description
SNMP	SMBS-210	**Symptom/Scenario:** Retrieving interface statistics using SNMP may return an invalid value. **Workaround**: N/A
Security	33205-0001	**Symptom/Scenario**: Upgraded iputils open-source software to version 20250605. This includes fixes for CVE 2025-47268, CVE 2025-48964. **Workaround**: N/A
Security	33205-0002	**Symptom/Scenario**: Upgraded sqlite open-source software to version 3.50.4. Resolves CVE-2025-6965. **Workaround**: N/A
Security	33205-0003	**Symptom/Scenario**: Upgraded rsync open-source software to version 3.4.1. Resolves CVE-2024-12085, CVE-2024-12086, CVE-2024-12087, CVE-2024-12088. **Workaround**: N/A
Security	33205-0004	**Symptom/Scenario**: Updated jquery-validation open-source software to version 1.21.0. Resolves CVE-2025-3573. **Workaround**: N/A

Version 3.3.0

Type	Bug ID	Description
Security	SMBS-191	**Symptom/Scenario:** Resolved an issue where EAPoL unicast frames were dropped instead of forwarded to all ports. **Workaround**: N/A
Security	33009-0001	**Symptom/Scenario**: OpenSSL is now upgraded to 3.0.15. This includes fixes for CVE-2024-13176. **Workaround**: N/A
Security	33009-0002	**Symptom/Scenario**: dnsmasq is now upgraded to 2.90-1. This includes fixes for CVE-2023-28450, CVE-2022-0934, CVE-2021-3448. **Workaround**: N/A

Version 3.2.0

Type	Bug ID	Description
SNMP	3190-0004	**Symptom/Scenario:** After a factory reset, the switches could lose the SNMPv3 default engine ID. **Workaround**: Manually edit and upload the startup configuration file by adding the line **snmp-server engineid local default** at the second-to-last line of the file.
ACL	3208-0001	**Symptom/Scenario:** When multiple ACLs are bonded to multiple interfaces simultaneously, the web page may display incorrect values and become unstable when trying to delete all the bindings. **Workaround**: Avoid refreshing the webpage while ACL binding or unbinding to multiple interfaces is in progress.

Type	Bug ID	Description
Security	SMBS-191	**Symptom/Scenario:** When EAPoL Flood mode is enabled, the switch fails to forward EAPoL packets out all ports. **Workaround**: N/A.

Version 3.1.0

Type	Bug ID	Description
SNMP	3190-0002	**Symptom/Scenario:** The OID for the manufacturer's name of the physical component has been updated to HPE Networking Instant On.
WebUI	3190-0003	**Symptom/Scenario:** Added minor cosmetic changes in the device shown in web management dashboard.

Version 3.0.0

Type	Bug ID	Description
GUI	28135-0003	**Symptom/Scenario**: WebUI becomes unresponsive when the firmware is uploaded using an incompatible device image or when the firmware downgrade prevention feature is enabled. **Workaround**: Refresh the web page.

Version 2.9.1.17

Type	Bug ID	Description
VLAN	29053-0003	**Symptom/Scenario**: Added a mechanism to prevent deleting switch ports from all VLANs. **Workaround**: None.
WebUI	29117-0003	**Symptom/Scenario**: Added minor cosmetic changes in the web management platform. **Workaround**: None.
Routing	SMBS-145	**Symptom/Scenario**: When configuring a static route to an individual host, the web-interface prevents use of subnet mask 255.255.255.255. **Workaround**: Manually modify the running config file with static route and subnet mask configurations then upload it to the switch.

Version 2.9.0.53

Type	Bug ID	Description
ACL	29053-0002	**Symptom/Scenario**: Applying an ACL to an interface or VLAN can generate an error message indicating lack of resources. **Workaround**: Attempt to apply the ACL a second time.
IGMP	SMBS-68	**Symptom/Scenario**: Enabling IGMP Snooping for eight or more VLANs simultaneously causes the switch to reset. **Workaround**: Enable IGMP snooping in smaller groups of VLANs.

Type	Bug ID	Description
Security	SMBS-97	**Symptom/Scenario**: The switch does not allow uploading valid CA-signed certificates larger than 3 kB in size. **Workaround**: : Upload a valid certificate smaller than 3 KB.
WebUI	29053-0001	**Symptom/Scenario**: Corrected error message text when creating a user account that already exists. **Workaround**: None.

Version 2.8.1.35

Type	Bug ID	Description
Diagnostics	228135-0001	**Symptom/Scenario**: In the support file, the cable test section displays only 14 interfaces. **Workaround**: Review GUI to get the Cable Test results.
WebUI	29117-0003	**Symptom/Scenario**: Missing information in support files. In this version, the support files include Device SKU, Management information (Device IPv4, HTTP management parameters and Management VLAN), Class of Service, and DoS Protection. **Workaround**: Review GUI to get configured values.

Version 2.8.0.17

Type	Bug ID	Description
Web	28017-0004	**Symptom/Scenario**: When performing a firmware update in a stacking configuration there is no feedback to the customer about the status of the update. **Workaround**: None.
Configuration	28017-0003	**Symptom/Scenario**: Copying an image to stack when connected through HTTPS could produce a crash. **Workaround**: Copy the image before adding the switch to a stack.
Diagnostics	SMBS-11	**Symptom/Scenario**: The IPv4 and IPv6 Ping Interval time settings are missing. **Workaround**: None.
SNMP	28017-0002	**Symptom/Scenario**: SNMP users show corrupted Group Names in the UI. This affects only the UI but SNMP works correctly. **Workaround**: None.

Version 2.7.0.103

Type	Bug ID	Description
Configuration File	270103-0001	**Symptom/Scenario**: Errors can appear when a user is copying running-config file to backup-config. **Workaround**: Copy running-config file to startup-config file and later to backup-config.
VLAN	26073-0002	**Symptom/Scenario**: VLAN Interface configuration does not update the PVID value of a port when the port is added to a VLAN with untagged membership.

Type	Bug ID	Description
		Workaround: Modify the PVID manually to match the VLAN in which the port was included.
Diagnostics	270103-0003	**Symptom/Scenario**: The Ping Timeout time setting is labeled incorrectly as Interval. The ping interval time is not configurable and set to one second by default. **Workaround**: None.
RADIUS	270103-0004	**Symptom/Scenario**: VLANs created by RADIUS authentication show a wrong name. **Workaround**: None.
WebUI	270103-0005	**Symptom/Scenario**: Web session remains open after setting the user password for the first time. **Workaround**: Users should re-login after resetting the default username or password.
SNMP	SMBS-15	**Symptom/Scenario**: SNMP groups with the word **default** in its name cannot be deleted. **Workaround**: None.
SNMP	SMBS-21	**Symptom/Scenario**: If the SNMP local engine ID field is manually deleted from the config-file, an invalid value will be displayed in the webUI. **Workaround**: Factory reset will regenerate and properly display a unique SNMP engine ID.
LLDP	SMBS-30	**Symptom/Scenario**: Resolved issue recognizing certain special characters in the LLDP TLV's which generates **Connection to the device is lost** pop-ups. **Workaround**: None.

Version 2.6.0.73

The following issues are resolved in this release:

Type	Bug ID	Description
Spanning Tree Protocol	26073-0002	**Symptom/Scenario**: Loops may occur on the network when the TCN (Topology Change Notification) feature is enabled on all switch ports. **Workaround**: Disable TCN Guard.
WebUI	26073-0001	**Symptom/Scenario**: The SFP/SFP+ ports tool tip is missing from the graphical Device Image. **Workaround**: Navigate to the Port Configuration or Event log to identify the transceiver type.

Version 2.5.0.67

The following issues are resolved in this release:

Type	Bug ID	Description
ACL	25067-001	**Symptom/Scenario**: Second ACL applied to an interface isn't properly saved. **Workaround**: Reboot the device to apply the second ACL.
Web UI	25067-002	**Symptom/Scenario**: The current copyright statement is not up to date. **Workaround**: N/A.

Version 2.4.0

There are no new resolved issues in this release.

Known Issues

Version 3.4.0

Type	Bug ID	Description
IPv6	SMBS-224	**Symptom/Scenario**:IPv6 remains enabled after restoring a startup configuration with IPv6 disabled and management VLAN set to 1. **Workaround**: Manually disable IPv6 or set the VLAN ID to a value not equal to 1.

- A mandatory software update is implemented to support updated hardware components.
- The 3.3.0 version prevents HPE Networking Instant On1960 switches firmware from being downgraded to an earlier version.

Version 3.3.4

Type	Bug ID	Description
Port Security	SMBS-188	**Symptom/Scenario**: With Port Security enabled, IP Phones may fail to rejoin the Voice VLAN after reconnection. **Workaround**:Disable Port Security on ports intended to be used on the Voice VLAN.

Version 3.3.2

Type	Bug ID	Description
Port Security	SMBS-188	**Symptom/Scenario**: IP Phones may fail to rejoin the Voice VLAN when the Port Security feature is enabled. **Workaround**:Disable Port Security on ports intended to be used on the Voice VLAN.

Version 3.3.0

Type	Bug ID	Description
Port Security	SMBS-188	**Symptom/Scenario**: With Port Security enabled, IP Phones may fail to rejoin the Voice VLAN after reconnection. **Workaround**: Disable Port Security on ports intended to be used on the Voice VLAN.

Version 3.2.0

There are no new known issues in this release.

The 3.2.0 version prevents HPE Networking Instant On 1960 switches firmware from being downgraded to an earlier version.

Version 3.1.0

Type	Bug ID	Description
SNMP	3190-0004	**Symptom/Scenario**: After a factory reset, the switches could lose the SNMPv3 default engine ID. **Workaround**: Manually edit the startup config file by adding the line "**snmp-server engineid local default**" at the end of the file.

Version 3.0.0

There are no new known issues in this release.

Version 2.9.1.17

Type	Bug ID	Description
GUI	28135-0003	**Symptom/Scenario**: Attempting to upload firmware using an incompatible device image or with firmware downgrade prevention enabled will cause the UI to hang. **Workaround**: Refresh the web page.

Version 2.9.0.53

Type	Bug ID	Description
VLAN	29053-0003	**Symptom/Scenario**: After deleting a VLAN, ports with untagged membership are not reassigned to a VLAN. **Workaround**: Manually add the affected ports a VLAN.

Version 2.8.1.35

Type	Bug ID	Description
GUI	28135-0003	**Symptom/Scenario**: Attempting to upload firmware using an incompatible device image or with firmware downgrade prevention enabled will cause the UI to hang. **Workaround**: Refresh the web page.

Version 2.8.0.17

There are no new known issues in this release.

Version 2.7.0.103

Type	Bug ID	Description
Diagnostics	SMBS-11	**Symptom/Scenario**: The IPv4 and IPv6 Ping and Traceroute Interval time settings are missing. **Workaround**: None.

Version 2.6.0.73

Type	Bug ID	Description
Diagnostics	26073-0003	**Symptom/Scenario**: The Ping Interval time setting is labeled incorrectly as Timeout. **Workaround**: None.
SNMP	26073-0004	**Symptom/Scenario**: If the SNMP engine ID field is manually deleted from the Configuration file, an invalid value will be displayed in the webUI. **Workaround**: Factory reset will regenerate and properly display a unique SNMP engine ID.
VLAN	26073-0005	**Symptom/Scenario**: VLAN Interface Configuration does not update the ports PVID value when added to a VLAN with untagged membership. **Workaround**: Modify the port VID manually to match the VLAN in which the port was included.

Version 2.5.0.67

Type	Bug ID	Description
Web UI	25067-003	**Symptom/Scenario**: The SFP+ ports tool tip is missing from the graphical device Image. **Workaround**: Navigate to the port configuration or event log to identify the transceiver type.
HTTP	25067-006	**Symptom/Scenario**: HTTP soft session timeout may fail when using non-default values. **Workaround** – Utilize the default value (10 minutes).

Version 2.4.0

There are no new known issues in this release.

Contacting Support

Main Site	instant-on.hpe.com
Support Site	instant-on.hpe.com/contact-support
Instant On Social Forums and Knowledge Base	community.instant-on.hpe.com
EULA	instant-on.hpe.com/eula/
Security Incident Response Team	Site: support.hpe.com/connect/s/securitybulletinlibrary Email: networking-sirt@hpe.com