Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.32.3, MARCH 13, 2026

Release Notes Section Outline

1. Update Instructions

These release notes apply to both the Vertiv™ Avocent® ACS800 and Vertiv™ Avocent® ACS8000 advanced console systems. Please refer to your installer/user guide for detailed instructions on updating either version of your system.

IMPORTANT NOTE: **This version must be upgraded from version 2.14.4 or later. Appliances with version 2.0.3 or earlier must be upgraded to version 2.12.4, then to version 2.14.4, and finally to version 2.32.3. Appliances with versions from 2.4.2 to 2.12.4 must first be upgraded to version 2.14.4, then to version 2.32.3.**

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.32.3	firmware-acs8-2.32.3.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.32.3	firmware-acs8-2.32.3.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	145
Firefox	147
Chrome	145
Safari	15.6.1

To access the console port with factory default settings, you need terminal emulation software running at 9600 bits per second, 8 bits, 1 stop bit, no parity, and no flow control.

4. Features and Enhancements

Release 2.32.3

- Firmware Upgrades:
  - OpenSSH 10.2p1
  - OpenSSL v3.0.19
  - Net-SNMP 5.9.5.2
- Firmware Additions:
  - Added support for a custom port number in TACACS.
  - Added support for ServerTech PRO4X as a serial PDU using the USB console of the PDU. This included adding a USB whitelist entry for the PDU.
  - Added support for ServerTech PRO4X as a network PDU.
  - Added support for usernames and passwords with ServerTech and Raritan PDUs. No longer uses the default username and password.

Release 2.32.2

- Firmware Upgrades:
  - Updated Duo client to the latest version, including the new CA bundle. [CA-0001149250]

Release 2.32.1

- Firmware Upgrades:
  - OpenSSH 10.0p2
  - Linux Kernel 5.10.234
  - OWFS 3.2p3
  - Sudo 1.9.17p1
- Firmware Additions:
  - Python3-pip
  - Python3-setuptools
- Added support for the Vertiv™ Liebert® SN-L Leak Detection Sensor when it is connected to a Vertiv™ PowerIT Rack Power Distribution Unit (rPDU).
- Added support for the Vertiv™ PowerIT IMD5 7.x firmware.
- Added support for the Eaton G4 PDU.
- Added cellular modem diagnostics reporting for improved troubleshooting.
- Added support for resetUsbConsole to the serialPorts in the RestAPI.

5. Issues Resolved

Release 2.32.3

- Fixed various RestAPI validation cases.
- Fixed a problem with RestAPI authentication when using bad credentials with TACACS.
- Updated detection procedure for Vertiv™ PowerIT rPDUs with 7.x firmware.
- Corrected a memory leak when using the RestAPI with basic authentication.

Release 2.32.1

- Resolved issue with the Command Line Interface (CLI) command `list_configuration` hanging (CA-0001092688).
- Resolved issue with the cellular Vertiv™ Avocent® ACS LTE default route.
- Fixed RestAPI validation for probeStrings and matchStrings.
- Improved RestAPI handling of special characters in digitalIn name and location fields.
- Resolved multiple issues with the Firewall field configuration in the RestAPI.
- Fixed outlet information reading on the Vertiv™ PowerIT Metered rPDU.
- Corrected SSH settings configuration when using Secure security profile with FIPS mode.
- Corrected outlet detection for Servertech 48DCWC PDU (CAS-569892).
- Modified the HTML5 Serial Viewer to use cookies for SID transmission.

  NOTE: The user must now enable cookies when using the serial viewer.
- The eth0/eth1 Auto-Negotiation setting is now periodically toggled off when the network link is down, and a SFP module is detected with a valid optical signal. This allows ZTP to run when the fiber connection requires Auto-Negotiation to be disabled.

6. Known Issues

- The ethtool option to read SFP module information (-m) can cause the network driver to lock up.
- Testing showed that the HTML5 Serial Viewer has the capacity to handle up to 12,500 characters when pasting text into its viewing window.
- SSH passthrough with the Vertiv™ Avocent® DSView™ 4.5 management software does not work in FIPS 140-2 mode.
- Do not use /mnt/hdCnf for storing files; filling this location may cause issues with the appliance. Files should be stored in the /mnt/hdUser partition instead.
- When using IE11 or Firefox, if users leave a page without saving changes, they are presented with a dialog box allowing them to check a box to prevent future dialog boxes. If users check that box, they will no longer receive informative dialog boxes.
- Users must toggle IPSec on/off for changes made to the established IPSec tunnel to take effect.
- The NTP client will not accept an update from an NTP server using its local clock as the clock source if reported timing parameters are outside the allowed range.
- The Vertiv™ Avocent® ACS console system uses reverse path filtering configured in STRICT mode, which means the console system will drop packets when the receiving packet source address is not routable through that interface.
- If sensors are used in conjunction with a Power Distribution Unit (PDU), it is recommended to connect the sensors to the PDU before the PDU is discovered by the Vertiv™ Avocent® ACS console system.
- When restoring a configuration that was saved as a CLI script, the restoration may take longer if PDUs are a part of the configuration.
- The Ethernet interfaces are set to Auto-Negotiation by default. This supports copper for speeds of 10 Mbps, 100 Mbps, or 1000 Mbps, depending on the connection speed to the other end. This supports a fiber connection of up to 1000 Mbps.
- EAP authentication only works with Windows XP.
- If a user is removed from all groups, that user will automatically inherit the access rights of the built-in USER group. For strict security, make sure the built-in "user" group has no permissions set. Then, create custom groups for any user-group permissions that are needed. This ensures that when a user is removed from all groups, the user does not receive any additional permissions as a result of belonging to the default "user" group.
- HTTPS sometimes has issues with Firefox where a certificate loads slowly or does not load at all. To resolve this issue, select the Firefox application menu (represented by three horizontal lines) in the top-right corner of the screen. Select *Help*, then *More troubleshooting information*. On the Troubleshooting Information screen, select *Refresh Firefox*. This should clean up the Firefox certificates.

- The older, Java-based JNLP Viewer is no longer supported when FIPS 140-2 mode is enabled. Only the HTML5 Viewer is supported in this mode.

7. External Network Port Usage

PORT RANGE	DESCRIPTION	SERVICE
0	ICMP	Open to allow network connectivity verification over ICMP.
20	FTP	Open to allow appliance firmware upgrade (data).
21	FTP	Open to allow appliance firmware upgrade (command).
22	SSH	Open to allow SSH sessions to the appliance.
23	TELNET	Open to allow Telnet sessions to the appliance.
25	SMTP	Open to allow email notifications.
49	TACACS+	Open to allow connection with the Remote TACACS+ Server.
67 (UDP)	DHCP Server	Open for the DHCP Server.
68 (UDP)	DHCP Client	Open for the DHCP Client.
80	HTTP	Open to allow web UI operation.
123	NTP	Open to allow appliance time to be set.
161	SNMP	Open to allow connectivity to SNMP-based targets and clients.
162	SNMP	Open to send and receive SNMP traps.
389	LDAP	Open to allow connectivity to the LDAP Remote Server.
443	HTTPS	Open to allow web UI operation and HTML5 serial sessions.
500	VPN / IPSEC	Open to allow ISAKMP to negotiate the IKE phase 1.
514	Syslog	Open to allow Syslog server functionality.
546 (UDP)	DHCPv6	Open to allow the DHCPv6 client to request an IP address.
636	LDAPS	Open to allow connectivity to the LDAPS Remote Server.
1812	RADIUS	Open to allow connectivity to the RADIUS Remote Server.
3211 (UDP)	AIDP	Open to allow the Vertiv™ Avocent® DSView™ management software to discover the appliance.
3211 (TCP)	ASMP	Open to allow the Vertiv™ Avocent® DSView™ management software to read/write appliance parameters.
3502	HTTPS	Open to allow Vertiv™ Avocent® DSView™ management software connectivity.

PORT RANGE	DESCRIPTION	SERVICE
3871	ADSAP2	Open to allow Vertiv™ Avocent® DSView™ management software-launched sessions and appliance authentication using the management software.
4122	SSH	Open to allow SSH connectivity between the Vertiv™ Avocent® DSView™ management software and the appliance.
4500	VPN/IPSec	Open to allow NAT Traversal.
4514	Syslog	Open to allow Vertiv™ Avocent® DSView™ management software Syslog functionality.
6701	SMS	Open to allow SMS event notification.
7001-7049	TELNET	Open to allow Telnet access to serial port connections.
8080	REST API (HTTP)	Open to allow the REST API to access the appliance.
48048	REST API (HTTPS)	Open to allow the REST API to access the appliance.

8. Compatibility Matrix

VERTIV™ AVOCENT® ACS ADVANCED CONSOLE SYSTEM VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE PLUG-IN VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE VERSION
2.32.3	2.32.3.1	4.5 SP12, 4.5 SP13, 4.5 SP14.1, 4.5 SP15, 4.5 SP16, 4.5 SP17, and 4.5 SP18.3.