Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.34.2, NOVEMBER 20, 2026

Release Notes Section Outline

1. Update Instructions
2. Appliance Firmware Version Information
3. Local Client Requirements
4. Features and Enhancements
5. Issues Resolved
6. Known Issues
7. External Network Port Usage
8. Compatibility Matrix

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 2.34.2. Appliances with versions from 2.4.2 to 2.12.4 must first be upgraded to version 2.14.4, then to version 2.34.2.**

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.34.2	firmware-acs8-2.34.2.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.34.2	firmware-acs8-2.34.2.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	154
Firefox	157
Chrome	155
Safari	15.6.1

© 2026 Vertiv Group Corp. All Rights Reserved.

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 2.34.2

- Firmware Upgrades:
    - OpenSSL 3.5.8 with FIPS 140-3 support
    - OpenSSH 10.5p1
    - Linux Kernel 6.18.45
    - Apache HTTP Server 2.4.68
    - Apache apr 1.7.6
    - Python 3 v3.14.6
    - owfs 3.2p4
    - pexpect 4.9.0
    - pip 26.1.2
    - setuptools 83.0.0
- Firmware Additions:
    - libmodbus 3.1.7
    - zstd 1.5.2
- The console system enables users who are authorized for device management to monitor managed devices and send commands such as on, off, open or close to managed devices. The ACS can manage certain devices using either Modbus RTU via a serial connection, or via network connection using Modbus TCP or SNMP.
- Adds REST API support for Device Management.
- Adds support for more 1-Wire sensor models and enhances the 1-Wire Sensors page and REST API.
- Adds Bonding Mode configuration to the Web UI.
- IPv6 Stateless Address Autoconfiguration (SLAAC) addresses are no longer configured when an interface uses the IPv6 Static or DHCPv6 method.
- Adds the GXT5 Battery Not Qualified event, APC rPDU2 MIB support, Geist firmware download through the REST API, and longer encrypted passwords in the CLI.
- Adds Manual and Startup frequency options for scheduled tasks.
- The event log can now be selected in the Export File list.
- Adds support for a persistent syslog file for events.
- Adds REST API support for IPv6 firewall rule options, Federal Information Processing Standards (FIPS) mode reboot, and the Zero Touch Provisioning (ZTP) log.
- Adds support for VTI/XFRM to the kernel (FER-0365).
- Adds reporting of client IP address on login and session events. (FER-258 CA-0001004473).

© 2026 Vertiv Group Corp. All Rights Reserved.

- Adds support for LACP bonding mode (CAS-47888-L9B1D3).

5. Issues Resolved

Descriptions of the issues resolved with this release are listed below:

Release 2.34.2

- Removes compromised intermediate CA certificates from the appliance trust store.
- Adds support for 4096-bit ACMEv2 key sizes (CAS-68832-P7P1H9 FER-0103, CA-0001078545 FER-290).
- SLAAC addresses left over from earlier configuration are flushed when an interface comes up using the IPv6 Static or DHCPv6 method. (CA-0001213566)
- Several fixes were made for the network driver lockup caused by ethtool -m (CA-0001207514).
- Fixes XML configuration restore from an HTTP source so that Apache (web server) configuration changes are restored.
- Fixes several issues in the save/restore configuration templates, including the restore of port alert strings.
- Fixes how serial port status is shown for RS-485 pinouts and for ports that are in use.
- Fixes validation and error handling on several REST API resources.
- Fixes the timeout and authorization access of sessions authenticated with ADSAP2 (Avocent DSView Secure Authentication Protocol 2).
- Fixes a parse error during cell registration on certain cellular carrier (CA-0001280458).
- Fixes 1-Wire sensor detection glitches, renaming, reset values and SN-TH temperature and humidity errors.
- Fixes the bootlogd pseudo-terminal setup and restores the vt102 terminal type on the console port.
- Account lockout messages are eliminated, and the lockout failure message stays generic after an upgrade.
- Network Time Protocol (NTP) is secure by default. Upgrades preserve the existing NTP authentication setting.
- Fixes an issue with arbitrary file overwrite when saving a configuration (CA-0001243864).
- Problem with "no Controls section in XML" with shared cli sessions (CA-0001132134).
- Adds restrictions and validation of auto-discovery command names to prevent RestAPI problems.
- Modifies SIDs to replace MD5 with more secure SHA256.

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 DSView 4.5 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

- 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.
- Setting MD5 NTP server key values via the CLI may fail to authenticate to the NTP server if the keys contain certain special characters. MD5 is no longer recommended for NTP but was provided for legacy support several years ago. If it must be used, keys should be entered via RestAPI or GUI instead of CLI.
- 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 using sensors 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 10 Mbps, 100 Mbps or 1000 Mbps based on the speed of the connection to the other end. This supports 1000 Mbps for a fiber connection.
- 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 needed. This ensures that when a user is removed from all groups, the user does not get any added permissions from 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 (the 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.

© 2026 Vertiv Group Corp. All Rights Reserved.

PORT RANGE	DESCRIPTION	SERVICE
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.
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.

© 2026 Vertiv Group Corp. All Rights Reserved.

8. Compatibility Matrix

VERTIV™ AVOCENT® ACS ADVANCED CONSOLE SYSTEM VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE PLUG-IN VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE VERSION
2.34.2	2.34.2.1	4.5 SP12, 4.5 SP13, 4.5 SP14.1, 4.5 SP15, 4.5 SP16 4.5 SP17, and 4.5 SP18.3.

© 2026 Vertiv Group Corp. All rights reserved. Vertivā and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions.