Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.26.3, JANUARY 22, 2024

Release Notes Section Outline

1. Update Instructions

These release notes refer to both the Vertiv™ Avocent® ACS800 and 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 upgrade to version 2.12.4, then to 2.14.4, then to version 2.26.3. Appliances with versions from 2.4.2 to 2.12.4 must first upgrade to version 2.14.4, then to 2.26.3.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.26.3	firmware-acs8-2.26.3.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.26.3	firmware-acs8-2.26.3.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	120
Firefox	121
Chrome	120
Safari	15.6.1

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

4. Features and Enhancements

Release 2.26.3

- Increased the size of the login banner to support up to 1500 characters (CAS-64917-C6N5N8 FER-0060).
- Added an acknowledgement checkbox option to the login banner to support STIG requirements (CAS-69395-K3L4J2 FER-0107).
- Added support for customizing the SSH Host Key Algorithms (CAS-66476-S6H4T5, CAS-69807-D1H5V9).
- Added support for customizing the SSH Cipher Levels while in FIPS mode (CAS-68832-P7P1H9 FER-0103).
- Improved SSH security by eliminating deprecated algorithms.

IMPORTANT NOTE:

This release improves the security for the algorithms supported by the appliance for SSH access.

- **The hmac-sha1 MAC Algorithm and the ssh-rsa Host Key Algorithm have been eliminated from Custom/High and Secure profiles. The Secure profile now uses the equivalent of the Custom/High SSH level. This means that Secure profile eliminates the following SSH algorithms:**
  - **ciphers: chacha20-poly1305, aes128-gcm, aes256-gcm**
  - **macs: hmac-sha1, umac-64-etm, hmac-sha1-etm, umac-64, umac-128**
  - **host keys: ssh-rsa**
- **In FIPS mode, the Secure and Custom/High profiles eliminate the following SSH algorithms:**
  - **kex: ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256**
  - **ciphers: aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc,aes128-gcm@openssh.com, aes256-gcm@openssh.com**
  - **macs: hmac-sha1, hmac-sha2-256, hmac-sha2-512, hmac-sha1-etm@openssh.com**

Upgrading to this firmware release on an appliance that uses these profiles will immediately eliminate these SSH algorithms. If problems arise with SSH after upgrading, these algorithms can be manually re-added using the Custom security profile and the "Custom" SSH level. In the Custom SSH level, individual macs, kex, encryption and hostkey algorithms can be specified.

Release 2.26.1

- Added support for NTP with IPv6 (CAS-69442-W5K7T4).
- Added support on the Monitoring - Serial Ports page for reporting transmitter and receiver byte counts for USB console devices as is already done for the regular serial ports.
- Added support for serial port speeds of 300, 600, and 1800.
- Added support for the APC 9000 Series of PDUs (CAS-66602-R3Y8K4 and CAS-69313-P6B2K1).

Release 2.26.0

- Added support for native Cisco Duo as the second factor of MFA.
- Added support for testing the NTP client via the UI.
- Improved the Vertiv™ Avocent® ACS6000 to Vertiv™ Avocent® ACS8000 migration scripts to better handle static IP addresses and eliminate dependency on discovery protocols.
- Updated RestAPI to add serial ports “clone” and clear Vertiv™ Avocent® DSView certificate functionality.
- Added support for the Vertiv™ Geist™ SRT sensor.
- Added an option for ignoring the DNS settings provided by the cellular provider.
- Added multi-route support for cellular (LTE).
- Added support for the following power devices:
  - Vertiv™ Geist™ Rack Transfer Switch (RTS)
  - Vertiv™ Liebert™ PSI5 UPS (SNMP only)

- Vertiv™ Edge Lithium-Ion UPS (SNMP only)
- Vertiv™ Liebert® APS UPS (SNMP only)
- Vertiv™ Geist™ rack Power Distribution Unit (rPDU) interface cards (Vertiv™ MRIC-RP Mid-Range Interface Card – Rack Power)

- Upgrades:
  - Linux Kernel 4.19.289
  - Apache 2.4.57
  - OpenSSL 3.0.8
  - OpenSSH 9.3p2 and PKIX-SSH 14.1.1
  - HTML5 Serial Viewer 4.6.1

5. Issues Resolved

Descriptions for the issues resolved with each release are listed in the following sections:

Release 2.26.3

- Fixed a problem with discovering some Raritan and ServerTech PDUs with new PDU firmware (CA-0000765022).
- Retry network port activation if the link is down with auto-negotiation disabled (CA-0000638528).

Release 2.26.1

- Fixed a memory leak in the pmd_ng process that occurred on appliances where Network PDUs are actively being polled. [CAS-63747-P2J0R4].
- Fixed a problem with analog modem occasionally failing to answer [CAS-66412-X5S7T9].

Release 2.26.0

- Fixed a problem with changing firewall rules back to “any” from a different setting.
- Fixed a problem in the cell modem scripts which caused a long delay in a cellular modem with no SIM card.
- Added an error message to indicate the JNLP Viewer is not supported when the FIPS module is enabled.
- Fixed a problem with Event Notification to Vertiv™ Avocent® DSView when the Vertiv™ Avocent® ACS console system FIPS module is enabled.
- Fixed a problem with restore of a compressed configuration putting the cellular unit in a incorrect state.
- Added a “route” option for the IPsec profile for VPNs that don’t use a virtual IP address [CAS-55549-R1D1C2].
- Allowed access to /mnt/hdUser/backup folder for configuration backups [CAS-62497-Z0L5C9].
- Fixed a problem where static routes are lost if the Ethernet interface drops intermittently [CAS-60842-X0T3Y9].
- Fixed a problem with the RestAPI logout not closing the session.
- Fixed the error message displayed when a downloaded certificate is not intended for this appliance [CAS-61846-F1V7Y8].
- Modified the cellular modem initialization sequence to not needlessly de-register and re-register with the provider [CAS-64319-M9Q8H0].
- Fixed the Vertiv™ Avocent® DSView data/event logging during failover.
- Improved URL validation for automated certificate management (ACME) [CA-0000678452].
- Added support for usernames in email address format for Cellular PPP authentication [CA-0000678452].
- Fixed the bug in the secure profile SSH Configuration when FIPS module is enabled (broken in 2.22)
- Fixed the HTML5 Serial Viewer problem for accounts with passwords that include spaces [CAS-61663-V8D4D2].

6. Known Issues

- 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 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 appliance.
23	TELNET	Open to allow Telnet sessions to appliance.
25	SMTP	Open to allow email notifications.
49	TACACS+	Open to allow connection with Remote TACACS+ Server.
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.

PORT RANGE	DESCRIPTION	SERVICE
162	SNMP	Open to send and receive SNMP traps.
389	LDAP	Open to allow connectivity to 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.
636	LDAPS	Open to allow connectivity to LDAPS Remote Server.
1812	RADIUS	Open to allow connectivity to Radius Remote Server.
3211 (UDP)	AIDP	Open to allow the Vertiv™ Avocent® DSView™ software to discover the appliance.
3211 (TCP)	ASMP	Open to allow the Vertiv™ Avocent® DSView™ software to read/write appliance parameters.
3502	HTTPS	Open to allow Vertiv™ Avocent® DSView™ software connectivity.
3871	ADSAP2	Open to allow Vertiv™ Avocent® DSView™ software-launched sessions and appliance authentication using the Vertiv™ Avocent® DSView™ software.
4122	SSH	Open to allow SSH connectivity between the Vertiv™ Avocent® DSView™ software and the appliance.
4500	VPN/ IPSec	Open to allow NAT Traversal.
4514	Syslog	Open to allow Vertiv™ Avocent® DSView™ 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
2.26.3	2.26.2.1	4.5 SP12, 4.5 SP13, 4.5 SP14.1, 4.5 SP15 and 4.5 SP16