# Vertiv™ Avocent® ACS8xxx Advanced Console System

## Release Notes

VERSION 2.28.4, SEPTEMBER 13, 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 2.28.4. Appliances with versions from 2.4.2 to 2.12.4 must first upgrade to version 2.14.4, then to 2.28.4.**

## 2. Appliance Firmware Version Information

| APPLIANCE/PRODUCT | VERSION | FILENAME |
|---|---|---|
| Vertiv™ Avocent® ACS800 advanced console system | 2.28.4 | firmware-acs8-2.28.4.fl |
| Vertiv™ Avocent® ACS8000 advanced console system | 2.28.4 | firmware-acs8-2.28.4.fl |

## 3. Local Client Requirements

| SOFTWARE | VERSION |
|---|---|
| Edge | 128 |
| Firefox | 128 |
| Chrome | 129 |
| 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 2.28.4

- Updated OpenSSH to version 9.8p1 to resolve the “RegreSSHion” vulnerability (CVE-2024-6387).
- Enabled IPv6 DHCP by default.

  **NOTE: This means the console system will start sending periodic DHCPv6 request packets on the network unless DHCPv6 is disabled via the UI.**
- Added support for sending DHCPv6 options 15, 16 and 17.
- Modified the cellular modem to disable voice call registration on North American carriers.
- Added an optional field to Network Failover to set a custom failover IP address to update the Vertiv™ Avocent® DSView™ management software in failover mode. This is useful for certain site-to-site VPN configurations.

### Release 2.28.3

- Upgrades:
  - Putty v0.81
  - HTML5 Serial Viewer 4.13.1
  - OpenSSH v9.6p1
- Added display of the user-defined serial port name to the Monitoring/Serial Ports info (CAS-71356-V0Z1F6 FER-0170).
- Added basic support for GRE Tunnels to the user interface.
- Added support for SNMPv3 authentication types SHA256/SHA512 and encryption types AES192/AES256 (FER-0117 CA-0000772338).
- Added support for including trap forwarder information in SNMP traps being forwarded (FER-0116 CA-0000769700).
- Updated the Java Viewer Certificate.
- Updated DHCPv6 client to support getting ZTP bootfile. This enables ZTP to be initiated over IPv6.
- Modified the DHCP client to automatically request options 66 and 67 from the DHCP Server when ZTP is enabled on the console system (CA-0000845390).
- Added code to correct the cellular modem settings to handle the upcoming 3G network sunset involving European carriers.

## 5. Issues Resolved

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

### Release 2.28.4

- Fixed issue with high CPU utilization causing access problems on cellular units (CA-0000894629).
- Fixed issue with the Subject Alternative Names (SAN) field of certificate generation not allowing hyphens (CA-0000899252).
- Fixed issue with the Serial Viewer not working when FIPS 140-2 is enabled (CA-0000893918).
- Fixed issue where errors occurred when trying to import a root certificate (CA-0000910220).
- Disable inadvertent closure of serial HTML5 viewer sessions when "Ctrl + ]" is pressed (CA-0000837113).
- Fixed issue with bonding in the Vertiv™ Avocent® ACS6000 migration scripts (CA-0000907621).

### Release 2.28.3

- Fixed issue where TLS 1.0 and 1.1 was not working when enabled in the security profile.
- Fixed issue where the /system/config RestAPI resource was not using the directory parameter properly.

- Fixed issue with the RestAPI to allow bonding and failover as the rest of the UI does.
- Fixed issue where daisy-chained Vertiv™ Geist™ PDUs were disappearing from the ACS list over time (CA-0000815049).
- Fixed issue with the Vertiv™ Avocent® ACS8xxx advanced console system discovering daisy-chained Vertiv™ Geist™ PDUs with the new Geist™ 6.x firmware (CA-0000844086).
- Fixed issue where the RestAPI firewall rules "move" resource was not working correctly.
- Fixed issue where a session was being created and not removed during a DHCP renewal if a bad configuration file was supplied to the appliance via DHCP (CA-0000796165).
- Fixed issue where the Security Profile custom cipher settings were not displaying correctly in the Vertiv™ Avocent® DSView™ 4.5 management software.
- Fixed issue where "session_flushin" error messages were appearing in dlog when event parameters were changed.
- Fixed issue where “99 of 7 bars” was displaying if the number of cellular bars could not be read from the cellular modem.
- Fixed issue with DOM-based cross site scripting vulnerability (CAS-65332-Z5F0T3).

## 6. Known Issues

- 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 to 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 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. |
| 67 (UDP) | DHCP Server | Open for DHCP Server. |
| 68 (UDP) | DHCP Client | Open for 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 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 DHCPv6 client to request IP address. |
| 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. |

| PORT RANGE | DESCRIPTION | SERVICE |
|---|---|---|
| 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 |
|---|---|---|
| 2.28.4 | 2.28.4.1 | 4.5 SP12, 4.5 SP13, 4.5 SP14.1, 4.5 SP15, 4.5 SP16, and 4.5 SP17. |