

# Vertiv™ ACS8xxx Advanced Console System

## Release Notes

VERSION 2.16.2, JULY 15, 2021

### 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. Compatibility Matrix

### 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 2.4.2 or later. Appliances with version 2.0.3 or earlier must upgrade to version 2.12.4 before upgrading 2.16.2.

### 2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.16.2	firmware-ac8-2.16.2.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.16.2	firmware-ac8-2.16.2.fl

### 3. Local Client Requirements

SOFTWARE	VERSION
Edge	91
Firefox	89
Chrome	91
Safari	14

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

- Added functionality so that the Vertiv™ Avocent® ACS advanced console system may now act as a DHCP server. Select *Network – DHCP Server* for configuration settings; the default for the DHCP server is disabled.
- Added hostname discovery to the Vertiv™ Avocent® ACS advanced console system via a command feature that allows the appliance to automatically log into a target device, execute a command and read the response to find the hostname of the target device. Pre-defined commands are located at *Ports- Serial Ports- CAS Profile- Auto Discovery- Commands*; users may also define additional commands.
- Added an Auto Discovery Status to the Monitoring page to show the port, type and discovered hostname.
- Added a Scheduled Tasks feature allowing users to run pre-defined tasks and custom tasks on a periodic basis. Users may create custom tasks using shell or python scripts.
- Added support for a cellular modem IP test to run as a scheduled task.
- Added a way to read the serial port's transceiver activity status via SNMP to support detection of device targets lacking DCD signal output.
- Upgraded to the following:
  - OpenSSH 8.4p1
  - sudo 1.9.5p2
  - OpenSSL 1.1.1k
  - Apache 2.4.46
  - GnuTLS 3.7.1
  - net-snmp v5.9

## 5. Issues Resolved

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

- Fixed the following issues with the Vertiv™ Avocent® DSView™ management software:
  - Fixed Vertiv™ Avocent® DSView™ software serial sessions failing if there was a space in the target name. [CAS-31518-LOQ7T9]
  - Fixed Vertiv™ Avocent® DSView™ software user interface issues (missing parameters). [CAS-40033-Q4B9C1]
  - Fixed other web user interface pages which would not display correctly in the Vertiv™ Avocent® DSView™ software. [CAS-39867-S7N3B0]
  - Fixed Vertiv™ Avocent® DSView™ software Upgrade Firmware task failing when multiple Vertiv™ Avocent® ACS advanced console system units are upgraded in parallel.
  - Fixed Digital In sensor page; it was not showing the correct state for the Alarm field between the Vertiv™ Avocent® DSView™ software and the Vertiv™ Avocent® ACS advanced console system.
  - Fixed Vertiv™ Avocent® DSView software SSH passthrough to the Vertiv™ Avocent® ACS advanced console system with FIPS mode enabled.
- Fixed the following issues with Power Distribution Units (PDUs):
  - Fixed an issue with refreshing a Vertiv™ Geist™ PDU chain. Added a display of agent serial numbers for a downstream Vertiv™ Geist™ PDU.
  - Fixed Vertiv™ Geist™ PDU firmware upgrade timeout issue.
  - Fixed PDU status message display issue.
- Fixed various cli save/restore configuration issues.
- Fixed autodetect of a cellular modem (detect timed-out and reported as analog modem).
- Included a fix to create a user's .ssh directory automatically when OpenSSH client is used.
- Included modifications to cellular call setup to align with AT&T's discontinuation of 3G services.

- Corrected a tab alignment issue with IE11 browser.
- Excluded dynamic values from the MD5 configuration integrity check (sensor values and DHCP lease file).
- Added support for HTTP Strict Transport Security response header under *System- Security- Security Profile- HTTP Strict Transport Security*. [CAS-10549-Q1NOC6, CAS-15946-R3S1V7, CAS-37576-F5M4S2]
- Resolved an issue with Vertiv™ Liebert® GXT5 UPS Events 376 and 382 involving continually sending event 382 SNMP traps. [CAS-39029-TOP2F8]
- Updated HTML5 viewer login credentials when the password is changed on the initial web user interface login page.
- Updated Java Serial Viewer certificate to authenticate serial sessions; the previous viewer certificate expires in September 2021.
- Updated PPP Daemon so it now logs modem messages to `/var/log/pppd.log`,
- Updated login banner to allow Japanese characters.

## 6. Known Issues

- In the default Security Profile, TLS 1.1 is enabled; users may disable it on the Security Profile page. In a future release, TLS 1.1 will be removed from the default Security Profile.
- 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 are advised to update their passwords in order to benefit from security improvements contained within this release.
- SNMPv3 traps are sent in the clear (unencrypted) regardless of configuration settings.
- 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. 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 will not load, or loading takes a long time. This can be corrected in the Firefox Help menu by selecting *Troubleshooting Information*, then *Refresh Firefox* (top-right of the page). This should clean up the Firefox certificates.

## 7. Compatibility Matrix

VERTIV™ AVOCENT® ACS ADVANCED CONSOLE SYSTEM VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE PLUG-IN VERSION	VERTIV™ AVOCENT® DSVIEW™ MANAGEMENT SOFTWARE VERSION
2.16.2	2.16.0.9	4.5 SP7, 4.5 SP8, 4.5 SP9, 4.5 SP10, 4.5 SP11, 4.5 SP12 and 4.5 SP13