Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.18.2, DECEMBER 17, 2021

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 2.4.2 or later. Appliances with version 2.0.3 or earlier must upgrade to version 2.12.4 before upgrading 2.18.2.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.18.2	firmware-acs8-2.18.2.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.18.2	firmware-acs8-2.18.2.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	96
Firefox	93
Chrome	96
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

- Updated HTML5 Serial Viewer to version v2.0.8, with improved features (expanded scroll buffer, copy and paste, for example). [CAS-27167-M6R1D7]
- Upgraded OpenSSH to version 8.7p1.
- Added TLSv1.3 support.
- Modified the HTTPS TLS version configuration to set a minimum protocol version instead of a list of specific version combinations.
- Added some missing user interface (UI) resources to the Restful API, such as poolOfPorts, monitoring pages, and so on.
- Added support for SNMPv3 traps.
- Updated the Vertiv™ Avocent® ACS8000 Trap MIB to support the SNMPv2/v3 trap format.
- Added changes to support integration with the new Vertiv™ Avocent® ADX Ecosystem.
- Updated username and password requirements for Vertiv™ Geist™ Power Distribution Units (PDUs).
- Added the ability to edit Auto Discovery Commands by clicking on the link of the name in the table.
- Modified the Active Sessions page to show the browser IP address as the client IP for HTML5 viewer sessions.
- Added more debug information to be gathered by the dbgmon script including active sessions and /var/log contents.
- Included the following cellular-related improvements:
    - Improved cellular modem debugging capability by adding a “Modem PPPD Log” (under the Monitoring tab) which displays the most recent entries in the pppd.log file.
    - Added a “Debug Level” on the cellular modem Dial-Out On Demand page to control the level of debug information included in the pppd.log file. This value should be set to 0 for normal operation.
    - Changed the options for the Device Status of a cellular modem on the Dial-Out On Demand page to be more descriptive. AlwaysOn means the modem is always on (this used to be called Enabled). Failover means the modem is controlled by failover logic (this used to be called Disabled). Disabled now means the modem is never turned on.
    - Eliminated the SIM PIN/Password button on the cellular Dial-Out On Demand page. The necessary fields are now automatically displayed when a pin or password is required.
    - Modified the UI to block attempts to disable cellular modem when the modem is currently configured as a failover interface.

5. Issues Resolved

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

- Added the Object Class parameter to the LDAP authentication server settings. [CAS-45224-G5B7J1]
- Added cellular parameters for EPSMode and PDP type to fix an issue where the cellular connection would drop every few minutes. [CAS-44677-S7W5R9]
- Fixed issues with new units failing to boot properly due to zero length key and/or certificate files. [CAS-46170-B0W3T8], [CAS-46048-P4P9M2]
- Modified Ethernet driver’s resource error handling (lockup after large number of small packets). [CAS-14621-N6Q5K0]
- Fixed issue with reporting the wrong Auto Discovery command for a port after the command has been deleted.
- Fixed issue with Auto Discovery Status page listing ports that do not have Auto Discovery enabled.
- Improved logic which detects cellular versus analog modem presence.
- Fixed security scanner complaints about missing X-Content-Type-Options Header by adding the header to the webserver. [CAS-10549-Q1N0C6]
- Fixed stale SNMPv3 user information stored in the snmpd configuration. [CAS-45254-N9N3X5]
- Fixed serial viewer access from the Vertiv™ Avocent® DSView™ management software when using an external authentication service which requires the username to be in the format ‘domain\username’.

- Fixed a *malformed line* message appearing in the Command Line Interface (CLI) when the appliance is configured for a language other than English.
- Fixed the Monitoring page to not be visible to users with limited rights.
- Fixed CLI configuration restore issues involving DNS servers on cellular appliances.
- Fixed issues with stale or incorrect information on the cellular Dial-Out On Demand page including updating the IMSI value after unlocking the SIM.
- Fixed issue with the cellular modem's internal baud rate being set incorrectly by the UI wizard after a factory default.

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 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. 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.

PORT RANGE	DESCRIPTION	SERVICE
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.
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
2.18.2	2.18.0.1	4.5 SP7, 4.5 SP8, 4.5 SP9, 4.5 SP10, 4.5 SP11, 4.5 SP12, 4.5 SP13 and 4.5 SP14