

Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.24.2, MARCH 20, 2023

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 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 2.24.2. Appliances with versions from 2.4.2 to 2.12.4 must first upgrade to version 2.14.4, then to 2.24.2.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.24.2	firmware-acs8-2.24.2.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.24.2	firmware-acs8-2.24.2.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	109
Firefox	109
Chrome	109
Safari	15.6

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

General Feature Updates

- Added basic support for the ACME protocol to automatically update IPsec and HTTPS certificates.
NOTE: Refer to the `/usr/local/docs/acme.txt` file.
- Added SAN (Subject Alternative Name) to Certificate and CSR (Certificate Signing Request) fields.
- Updated OpenSSL to v3.0.7:
 - The OpenSSL 3.0 FIPS provider has been issued FIPS 140-2 Validation Certificate #4282.
 - The OpenSSL 3.0 FIPS provider now requires the 2048-bit certificate for the Vertiv™ Avocent® DSView management software.
 - The OpenSSL 3.0 FIPS provider does not support the PKCS12 key derivation function used for MAC verification of PKCS12 files. Existing PKCS12 files can be converted using the "openssl pkcs12" command line tool with the "-nomac" option.
- Added migration scripts to help automate the process of replacing Vertiv™ Avocent® ACS6000 advanced console servers with new Vertiv™ Avocent® ACS8000 advanced console systems.
NOTE: Refer to the `/usr/local/migrate/README.txt` file.
- Improved functionality related to the import of Vertiv™ Avocent® ACS6000 advanced console server config files.
- Added a status line on the `System--Security--DSView` page to indicate that the Vertiv™ Avocent® ACS advanced console system is being managed.
- Added support for non-blocking requests to the RestAPI certificate and firmware resources.
- Added a new RestAPI `/system/certificate/upload` resource for passing a certificate in the body of the RestAPI request.

General Upgrades

- StrongSwan 5.9.6
- HTML Serial Viewer v4.2.1
- Apache 2.4.54
- PKIX-SSH 13.4.1

5. Issues Resolved

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

- The following items were fixed specifically in version 2.24.2:
 - After downloading and installing a PEM file composed of a certificate and a key, the Vertiv™ Avocent® ACS advanced console system is unreachable via HTTPS.
 - In a Vertiv™ Avocent® ACS advanced console system, the default certificate for connecting to the Vertiv™ Avocent® DSView™ management software was changed to 2048 bits in version 2.24.1. After upgrading the console system, this broke existing connections if the console system was using a 1024 bit certificate for connecting to the management software.
- Fixed a problem with the Servertech PDU 48DCWC only showing half the ports (CAS-55555-K2W2R3).
- Rotated the RestAPI logs to save space.
- Added support for changing the empty default password via the RestAPI (CAS-49988-Y0V9R4).
- Fixed a problem with lldp and ipv6 settings not being restored with templates (CAS-50446-J1N0Z9).
- Updated Japanese translations.

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 you leave a page without saving changes, you are presented with a dialog box allowing you to check a box to prevent future dialog boxes. If you check that box, you will no longer receive informative dialog boxes.
- You 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.
- 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.
- If the Vertiv™ Avocent® ACS console system is in FIPS mode, unsecure mode and also using a 1024 bit certificate, then the console system is unable to communicate with the Vertiv™ Avocent® DSView™ management software.

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
2.24.2	2.22.0.1	4.5 SP12, 4.5 SP13, 4.5 SP14.1, 4.5 SP15 and 4.5 SP16