Vertiv™ Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.22.1, AUGUST 19, 2022

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 2.22.1.

2. Appliance Firmware Version Information

APPLIANCE/PRODUCT	VERSION	FILENAME
Vertiv™ Avocent® ACS800 advanced console system	2.22.1	firmware-acs8-2.22.1.fl
Vertiv™ Avocent® ACS8000 advanced console system	2.22.1	firmware-acs8-2.22.1.fl

3. Local Client Requirements

SOFTWARE	VERSION
Edge	103
Firefox	102
Chrome	103
Safari	15.5

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 support for the ip_gre loadable kernel module, which allows a GRE tunnel to be established using commands from the Linux shell.
- Added a “no negotiate” option for eth0 and eth1 under *Network-Devices*.
- Added NTP authentication under *System-Date and Time*.
- Added a phytool utility for debugging Ethernet PHYs.
- Added /var/log/btmp file for use by OpenSSH to record failed logins.
- Added settings in the custom security profile:
  - Added user-configurable cipher suite settings for the SSH server.
  - Added user-configurable HTTPS/TLS cipher list settings.
- Added a new Local/LDAP authentication option to reduce local lookup time. (CAS-49790-V7B8D3)
- Improved the cellular modem signal quality check with an indicator of how many bars the modem detects (like a phone).
- Enabled debug warning flags for IPSec and cellular debug:
  - Flags added to the top tab bar for settings that might impact performance. These are links that are displayed until the debug is disabled or until you click on the link, which then takes you to the page where the debug can be disabled.
  - A flag is displayed in the IPSec log level is set to “Debug(1)” or higher.
  - A flag is displayed if the cellular modem debug level is greater than zero (0).

New Diagnostics Feature

This release adds the new Diagnostics system tool which can enable various types of debug logging and export log files to your client computer. The Diagnostics tool has the following options:

- Debug Dump: This option generates the /mnt/hdUser/dbgdump.log file. The timestamp of any existing file displays.
- Debug Monitor: This option is a debug process that can be enabled and disabled. While enabled, the state of the appliance is captured at regular intervals and the timestamp of the most recent debug file in /mnt/hdUser displays.
- Debug USB: This option captures debug information as a USB device is enumerated. The timestamp of the /var/log/usbdebug.log file displays.
- Debug IPSec: This option allows you to set the debug log level for IPSec. There is a default log level and two subsystem levels for narrowing down the debug type you wish to see. The timestamp of the /var/log/ipsec.log file displays.
- Enhanced Debug Logging: This option allows you to enable or disable debug for either Power Management or Serial. The debug appears in the /var/log/dlog.log file.

The Diagnostics tool has the following buttons:

- Run: This button starts the selected debug option. Some options start a script running, while others gather information.
- Stop: This button disables the selected debug option; this stops the currently running script.
- Export: This button downloads the log file for the selected debug option.
- Cancel: This button exits the Diagnostics page.

IPSec Enhancements

- Added the ability to connect and disconnect IPSec (VPN) tunnels from the web user interface (UI), and also added the ability to view diagnostic information about IPSec (VPN) tunnels.

- Added enhancements on the IPSec (VPN) connection page:
  - Added Connect button, including a warning message if the Connect button is used when IPSec is disabled or there are unsaved changes on the page.
  - Added a Disconnect button.
  - Added a Ping button to test a connection.
  - Added a Diagnostics section (hidden by default) which can display the status of the connection and the result of the last Connect/Disconnect action.
- Added enhancements on the Monitoring-IPSec Tunnel Status page:
  - Added Connect and Disconnect buttons.
  - Changed table column names to show the Remote Subnet, Local IP and Local Virtual IP (instead of the phase I/II algorithms).
  - Added the ability to drill down into a connection and see details about it.
- Added the ability to specify a pass phrase when uploading IPSec (PKCS12) files:
  - Added an optional Pass Phrase field on the *System Tools-IPSec (PKCS12) Files* page; this pass phrase protects the PKCS12 file.
  - Added a Passphrase field to the /network/ipsec/certificate/download resource for the REST API.
- Enhanced the IPSec service for it to restart upon failover to speed up the process of establishing a new IPSec tunnel.
- Added capability of Daemon Stopped/Started events to now be issued when the IPSec service stops and starts.

General Upgrades

- OpenSSH v9.0p1
- OpenSSL v1.1.1o
- Apache2 v2.4.53
- HTML Serial Viewer v2.9.1
- expat v2.4.7 (XML Parser Library)

5. Issues Resolved

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

- Fixed supporting a Vertiv™ Geist™ Power Distribution Unit (PDU) daisy-chain with offline PDUs or relocated PDUs.
- Fixed lockup of the Vertiv™ Liebert® GXT5 UPS if it powers up while being managed serially by the Vertiv™ Avocent® ACS advanced console system.
- Fixed an issue to remove information from the ipsec.secrets file when an IPSec (VPN) connection is deleted or modified.
- Fixed an issue preventing SNMPv3 users from being created when FIPS mode is enabled. (CAS-48404-T5V3Y8)
- Changed the factory default HTTPS TLS minimum version from 1.1 to 1.2 as part of the default custom profile. This only impacts the default version, and the device can be configured to use TLS 1.3.
- Improved processing of the REST API /security resource so that it does not unnecessarily restart daemons.
- Resolved an issue so that the HTTPS port number and REST API port number can now be set to the same value.
- Resolved an issue so that the REST API HTTPS port number can now be set by a REST API request.
- Fixed an error with the modem resource caused by a blank mgetty cell_ping value.
- Fixed an issue with login failing with no error message when two remote Auth Servers are configured. (CAS-44670-J4K4G9)

- Improved session cleanup capability to allow for user-specific cleanup. (CAS-48124-S7B7G5)
- Fixed issue with restoring old CLI format configurations that were set to Secure mode.
- Fixed issue with the import_acs5000 script's handling of TACACS authentication settings.
- Fixed issue with page errors on the Cellular DialOut page when the Advanced Settings checkbox was checked.
- Changed event trap 125 (modem status change) to only be generated when status actually changes.
- Disabled support for the HTTP OPTIONS method to prevent warnings from security scans.

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.

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.

PORT RANGE	DESCRIPTION	SERVICE
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
2.22.1	2.22.0.1	4.5 SP12, 4.5 SP13, 4.5 SP14.1 and SP15