VERTIV™

Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.4.2, AUGUST 24, 2018

Release Notes Section Outline

1 Update Instructions

These release notes refer to both the Avocent® ACS800 and ACS8000 advanced console systems. Please refer to your installer/user guide for detailed instructions on updating either version of your system.

2 Appliance Firmware Version Information

Appliance/Product	Version	Filename
Avocent® ACS 800 advanced console system	2.4.2	Firmware-acs8-2.4.2.fl
Avocent® ACS 8000 advanced console system	2.4.2	Firmware-acs8-2.4.2.fl

3 Local Client Requirements

Software	Version
Internet Explorer®	11
Edge	40
Firefox	57
Chrome	62
Safari	8

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 support for Geist™ Power Distribution Units (network and serial PDUs).
- Added optional TFTP server support.
- Added HTML5 viewer support for the Avocent® DSView™ management software.
- Updated Linux kernel.
- Upgraded OpenSSH and OpenSSL.
- Made general improvements in handling and displaying PDU parameters.
- Added security updates and improvements.
- Added adjustment where serial port names are no longer modified when a configuration template is applied from the Avocent® DSView™ management software.
- Added adjustment where the appliance now returns the exit code for a remote SSH command instead of returning 1 as the value.
- Added adjustment where changing network settings no longer triggers an extraneous power supply change event/message.
- Fixed IE10 display issues.
- Fixed configuration integrity checksum issue after restoring a compressed configuration.
- Fixed backward compatibility issues with XML configurations created using firmware version 1.2.9.
- Added update to allow DNS domain and search fields to be cleared.
- Added update to displays a more specific error message when an invalid IPv4 address is entered for network boot mode.
- Disabled the second NTP server address field if the first NTP server field is left blank on the On-Board Web Interface (OBWI).
- Fixed display issues with the Net-PDU overview page.
- Fixed issue with the serial port session LED not turning off when the session is closed.
- Fixed issue where serial ports were left disabled after restoring a CLI configuration on an appliance without an internal modem.
- Fixed HTML5 serial viewer issues after restoring a configuration file.
- Fixed CLI access to IPSec VPN connection settings.
- Added support for remote echo commands to the appliance via SSH.
- Added adjustment where MD5/DES is no longer available in IPSec and SNMPv3 settings when FIPS mode is enabled.
- Added fixes for the USB modem callback issue. Toggle DTR setting added to the Dial-In Settings for USB modems under Pluggable Devices. The default callback dial prefix changed to "ATDT" instead of "ATD".

- Fixed issue with user account lock-out after failed login.
- Fixed segmentation fault in the migration CLI's show config command.
- Added fixes for the following network failover related issues:
  - Reverse path filter temporarily set to loose mode when a ping triggered failover occurs to allow recovery detection.
  - Network failover disabled while restoring CLI configuration scripts to allow changes to network device settings.
  - A debug message is now logged to syslog when IP change requests to the Avocent® DSView™ software fail during network failover.
- Updated syslog-ng and periodically checked to ensure syslog-ng is running.
- Changed the priority level on a start multi-session debug message to normally hide it.
- Fixed the CLI configuration of power outlets from a PDU/UPS assigned to a CAS serial port.
- Fixed the CLI configuration of serial port alerts.
- Fixed an HTTPS certificate download error message.
- Fixed issue with a failed login lockout causing the change password dialog box to be displayed.
- Added fix so that the JNLP viewer now works again with the HIGH SSH cipher setting.
- Fixed display issue with IE11 and setting manual date/time.
- Fixed issue where root user is unable to connect to a Pool of Ports in raw mode.
- Fixed web display issue where the font color is not switched properly between green and black.
- Added adjustment where IPSec advanced settings are now saved in the XML configuration.
- Added adjustment where IPSec web page now flags an error if the RSA certificate authentication method is selected with a blank Local PKCS12 file.
- Removed SSHv1 support.
- Enhanced appliance to default to more secure SSH/SSL settings.
- Fixed issues with the Avocent® ACS5000 advanced console server configuration importer tool.
- Fixed issue with TCP Flags in firewall rules not getting saved.
- Fixed issue with the default user group having access to the IPSec Monitoring status.
- Corrected issue with pam-radius module sending the NAS-IP-Address in the wrong byte order.
- Fixed issue with the pluggable-device enable state not getting restored correctly from a compressed configuration file.
- Removed extraneous power management debug statement from the system log.
- Allowed an IPv6 address to now be entered for a remote Socket-Client.

- Fixed issues with port LED left on when port is disabled or the port profile type is changed.
- Fixed issue where BOOTVERSION is empty in the /firmware file.
- Fixed the default strings returned for the Avocent® ACS800 advanced console system's SNMP sysdescr and syslocation OIDs.
- Updated the parameters used to generate the appliance's self-signed SSL certificate.
- Generated the restapi's certificate/key on the appliance instead of using a static pre-generated set.
- Fixed issue with the display of the timezone list.
- Fixed issue where the ADSAP2 daemon would start incorrectly listening on port 65535.
- Fixed issue with session timeout handling after the system time is rolled back.
- Added adjustment where appliance now monitors and restarts serial and session daemons when found not running.
- Fixed issue where port aliases enabled after a security profile change are not accessible.
- Added ability to disable 1-wire support on the Security Profile page.
- Fixed issue with monitoring the IPv4 Routing Tables when Multiple Routing Tables are enabled.

5 Known Issues

- 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.
- If the configuration is changed on an established IPsec tunnel, the user must toggle IPsec on/off for the new configuration 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 Avocent® ACS console server uses reverse path filtering configured in STRICT mode, which means the console server 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 Avocent® ACS console server.
- 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.
- A reboot is required after enabling or disabling Bonding.
- 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 does not work in Firefox. Firefox does not load the certificate, or it takes a long time to load it. To correct this, go to the Firefox Help menu and click *Troubleshooting Information*. On the top-right of the page, click *Refresh Firefox*. This will clean up the Firefox certificates
- The format of the sendmsg command is “sendmsg username message”.

6 Compatibility Matrix

AVOCENT® ACS ADVANCED CONSOLE SYSTEM VERSION	DSVIEW™ MANAGEMENT SOFTWARE PLUG-IN VERSION	DSVIEW™ MANAGEMENT SOFTWARE VERSION
2.4.2	2.4.0.1	4.5 SP7, 4.5 SP8, 4.5 SP9