
Avocent® ACS 6000 Advanced Console Server

Release Notes

Version 3.3.0-10

June 24, 2016

This document outlines:

1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug Fixes

1. Update Instructions

NOTE: Please refer to the ACS 6000 Installer/User Guide for detailed instructions on updating the ACS 6000 console server to version 3.3.0.

IMPORTANT NOTE: This version should be upgraded from version 2.5.0-11 or newer. Appliances with earlier versions should be upgraded to version 2.5.0-11 before the upgrade to version 3.3.0.

In order to have all features listed in this release available through DSView™ management software, DSView™ software version 4.5.0.263 (SP 5) or later and ACS 6000 console server plug-in version 3.3.0 are required.

When applicable, after the ACS 6000 console server firmware has been upgraded to version 3.3.0, it is mandatory that the web browser cache of any system which intends to be connected to the ACS 6000 console server web interface is cleared. To do this, press **Ctrl-F5** from the browser.

ACS 6000 console server firmware version 3.3.0 provides an internal mechanism which preserves the existing configuration when upgrading from previous firmware versions. However, it is strongly recommended that you back up the system configuration before firmware version upgrades.

2. Appliance Firmware Version Information

The following languages are supported by ACS 6000 console server version 3.3.0-10:

- English
- Japanese
- Simplified Chinese

Appliance/Product	Firmware Type	Version	Filename
Avocent® ACS 6000 Console Server	Opcode	3.3.0-10	avolmage_avctacs-3.3.0-10.bin avolmage_avctacs-3.3.0-10.bin.md5

3. Features/Enhancements

NOTE: Please refer to the ACS 6000 Installer/User Guide and/or Command Reference Guide for details about features supported by the ACS 6000 console server version 3.3.0.

Client Browser Support Information:

- Microsoft® Internet Explorer® 9, 10, and 11.
- Mozilla® Firefox® version 36.0.1 in Windows 7.
- Google Chrome™ browser version 45.0 in Windows 7.

Upgrades included:

- Programmable RESTful interface as a new menu in the context of serial sessions:
 - Enables the user to program HTTP GET or POST requests that can be executed through the terminal interface.
- Exclusive Network Failover or Multiple Routing Tables configuration, bringing back Multiple Routing Tables capabilities as implemented in previous ACS 6000 console server releases.

NOTE: The WebUI menu in version 3.3.0 has changed. The multi-route was added back and the heading “Routing” was added. This means CLI nodes have changed and the CLI backup scripts prior to ACS 6000 console server version 3.3.0 will have to be properly updated.

- Configuration Integrity through MD5 Tag:
 - Enables customers to generate and verify a digital signature (MD5) of the appliance configuration, which can then be used to automatically verify the integrity of an individual appliance configuration for change-detection capabilities.

NOTE: Saving configuration with Compressed File option is the only format that captures all parameters covered by the MD5 digital signature.

- Includes new event 19: ACS 6000 Appliance New Configuration MD5 Tag Detected.
- Stateless IPv6 enabled in factory default configuration (dual IP stack).
 - IPv6 operations are not permitted in the following functional areas:
 - Network Failover
 - Network Boot
 - Network PDUs
- Telnet disabled in factory default configuration.
- Multisession R/W access rights configuration for admin group (instead of having such access rights always granted; though they are still all granted by default).
- New Failover events:
 - Event 20: ACS 6000 Appliance Network Primary Failover has occurred
 - Event 21: ACS 6000 Appliance Network Primary Failover has been restored
- OpenSSH upgrade to version 7.1

NOTE: Microsoft® Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) implementation has been deprecated in Windows 7.

4. Bug Fixes

Bug fixes included in version 3.3.0-10:

- Double characters appearing on Telnet sessions with some clients. (L3-487234-455191324)
- RADIUS_Down_Local authentication which caused the service not to revert to local authentication when RADIUS server was unavailable. (L3-487234-491089663)
- Dial-in time-locked on version 3.x after time out. (L3-487234-454654726)

-
- DSView_Down_Local authentication on version 3.1.0-8. (L3-487234-472992429)
 - Enabling eth bonding was deleting default gateway. (L3-487234-510952654)
 - OpenSSH vulnerabilities on versions prior to 7.0. (L3-487234-514529955)
 - Versions 3.1 and earlier had an issue setting IPv6 syslog server. Once it was set, syslog would stop working for both IPv4 and IPv6. Users upgrading to version 3.3.0 will now have the reference to IPv6 syslog server removed. This will cause previously configured IPv4 syslog server to begin working and the user will be able to re-enter the desired IPv6 syslog server information.
 - Allows GDB connections to serial targets over TELNET protocol.
 - Allows TELNET “send break” command, in addition to the native “break sequence” recognition.
 - Solves a problem where Ethernet interfaces go down and come back up losing serial port IP Aliases sub-interfaces.
 - Allows for a “complete set” of multisession menu options to be displayed even before the connection to serial ports are fully established.
 - Version 3.3.0 introduced a change on serial port IPv4 aliasing handling. Connections using redundant qualifications for a serial port (IP address alias _and_ TCP port alias) are not allowed. For IPv6, as in previous releases, the connection is allowed as TCP port alias and takes precedence for disambiguation.
 - When a non-factory default appliance is enrolled in the DSView™ Management Software, if status polling and auto topology updates are enabled, port configuration should be added to the DSView software in the next polling (usually a few minutes after enrollment). An alternative procedure is to manually “resync” the appliance from DSView software UI at *ACS60000 - Appliance Setting - Serial Ports*.

Emerson and Emerson Network Power are trademarks or service marks of Emerson Electric Co. Avocent, the Avocent logo and DSView are trademarks or service marks of Avocent Corporation. All other marks are the intellectual property of their respective owners. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2016 Avocent Corporation. All rights reserved.