VERTIV™

Avocent® ACS6000 Advanced Console System

Release Notes

VERSION 3.6.0.8, FEBRUARY 13, 2018

Release Notes Section Outline

1 Update Instructions

These release notes refer to the Avocent® ACS6000 advanced console server. Please refer to your installer/user guide for detailed instructions on updating the Avocent® ACS advanced console server.

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 3.6.x.x or later.

In order to have all features listed in this release available through the Avocent® DSView™ management software, DSView™ software version 4.5 (SP7 or later) and ACS6000 console server plug-in version 3.6.0 are required.

ACS6000 console server firmware version 3.6.0 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

APPLIANCE/PRODUCT	VERSION	FILENAME
Avocent® ACS 6000 Advanced Console System	3.6.0.8	avoImage_avctacs_3.6.0.8.zip avoImage_avctacs_3.6.0.8.zip.md5.txt

3 Local Client Requirements

SOFTWARE	VERSION
Internet Explorer®	11
Edge	Use latest version available
Chrome	Use latest version available
Firefox	Use latest version available
Safari	8

To access the console port with the 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

- This release changes the branding to Vertiv™; the major difference in Vertiv™ branding will be the colors used in the web user interface (UI).
- This release adds support for a second NTP (time) server. The ACS console server will contact both NTP servers and use the best response.
- If the IPSec tunnel goes down due to an external link dropping, it will try to re-establish the tunnel. New parameters were added to control the “frequency” and “maximum time” the ACS console server will try to re-establish the tunnel. The frequency is how often the retry occurs and the maximum time controls how long the ACS console server continues to retry.
- This release also corrects a problem where the VPN tunnel drops for six seconds when the system rekeys. This changed the IPSec configuration.
- More IPSec configuration parameters are now added to the web UI in an advanced settings area. This allows the user to have more control over IPSec configuration.
- The following issues were resolved:
    - User home directory owned by root after a firmware downgrade.
    - Fixed an issue when authentication was set for TACACS+/Local and TACACS failed. Local and remote users were locked out.
    - Fixed an issue when the system only checks for a blank IP gateway field when the primary network interface is being configured with a static IPv4 address and the multiple routing tables feature is enabled.
    - Removed RC4 encryption ciphers from Apache2.
    - Fixed a *Warning file too large* error message reported when no file existed.
    - Resolved an issue related to the XML restore process when IPsec properties were missing from the input configuration.
    - Resolved an issue that was resetting port names after restoring a saved template.

5 Known Issues

HTTPS sometimes does not work in Firefox. Firefox does not load the certificate or it takes a long time to load. To correct this issue, select *Troubleshooting Information* in the Firefox help menu. On the top-right of the page, select *Refresh Firefox*. This will clean up the certificate.

6 Compatibility Matrix

AVOCENT® ACS ADVANCED CONSOLE SERVER VERSION	DSVIEW™ MANAGEMENT SOFTWARE PLUG-IN VERSION	DSVIEW™ MANAGEMENT SOFTWARE VERSION
3.6.0.8	3.6.0.4	4.5 SP7, 4.5 SP8