Avocent® ACS 5000 Advanced Console Server
Release Notes
Version 3.3.0.17 Update!
July 24, 2015

This document outlines:

1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug Fixes
5. Configuration Details
6. Known Issues

==========

1. Update Instructions

==========

NOTE: Please refer to the ACS Installation/Administration/User Guide for detailed instructions on updating the ACS console server to version 3.3.0.17.

In order to have all features listed in this release available through DSView™ management software, the latest versions of the DSView™ software components are required:

DSView™ Software	DSView™ Version	Plug-in Version
DSView™ version 3 software	3.7.2	3.3.5
DSView™ version 4 software	4.5.0	3.3.6

An appliance firmware package to upgrade from DSView™ software is also available.

After ACS 5000 console server firmware has been upgraded to version 3.3.0.17, it is mandatory that the Web browser cache of any system which intends to be connected to the ACS 5000 console server Web interface is cleaned up. To do this, press **Ctrl-F5** from the browser.

Avocent® ACS 5000 console server firmware version 3.3.0.17 provides an internal mechanism which preserves existing configuration when upgrading from firmware versions 1.0.2 and later. However, it is strongly recommended that you back-up system configuration before the firmware version is upgraded.

==========

2. Appliance Firmware Version Information

==========

Appliance/Product	Firmware Type	Version	Filename
Avocent® ACS 5000 Console Server	Opcode	V_3.3.0-17	zImage_acs5k_330-17_AB_150615.bin zImage_acs5k_330-17_AB_150615.bin.md5
Avocent® ACS 5000 Console Server	DSView software package	V_3.3.0-17	acs5k_v330-17_2015-06-25.pkg acs5k_v330-17_2015-06-25.pkg.md5

==========

3. Features/Enhancements

==========

NOTE: Please refer to the ACS 5000 Installation/Administration/User Guide and/or Command Reference Guide for details about features supported by the ACS 5000 console server version 3.3.0.

Upgrades included in ACS 5000 console server version 3.3.0.17:

- Openssl upgrade to address the POODLE vulnerability.

Upgrade included in ACS 5000 console server version 3.3.0.16:

- Bash version 2.0.5b (patches 001-013) that has fixes for the following: CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278

Major features of the ACS 5000 console sever version 3.3.0.9 include:

- Appliance's serial number can be retrieved by SNMP query. New CYCLADES-ACS5000-MIB.ASN file has the description of this OID.
- The configuration of Polling Rate is by serial port configured as Power Management instead of by PDU. The unit of polling rate is now seconds.
- Linux Kernel applied patches that fix the following security issues: CVE-2011-0726, CVE-2011-1171, CVE-2011-1172, CVE-2011-1182 and CVE-2011-1593.

==========

4. Bug Fixes

==========

Patch release version 3.3.0.13 bug fixes include:

- Adsap2 works without memory leak in IPv6 networks (L3-65675139)
- ts_menu and Serial Viewer get the ssh port from the security profile to establish connection with serial target (L3-65702750).

Patch release version 3.3.0.10 bug fixes include:

- Configuration upgrade from 3.3.0.5 or earlier version updates Power Mgmt configuration file (/etc/pmd.conf) without error (L3-65642621)

Version 3.3.0.-9 bug fixes include:

- New mechanism tries to recover chain of PM PDU with 1.9.4 version (L365613042).

==========

5. Configuration Details

==========

Please note the following configuration details for the release 3.3.0.17:

- It is necessary to edit the /etc/ssl_version.conf file to configure the SSL version and cipher level.
- Default configuration settings for /etc/ssl_version.conf are as follows:
    a. TLS version: default = tls1_2
    b. SSL cipher list (SSLCIPHER): default = DEFAULT (the default openssl cipher list)
- Configuration syntax:

  SSLVER=<TLSv>

  SSLCIPHER=<level>

Where:

<TLSv> - TLS version:

.. tls1 – TLSv1.0 (TLS version 1.0)

.. tls1_1 – TLSv1.1 (TLS version 1.1)

.. tls1_2 – TLSv1.2 (TLS version 1.2)

<level> - level of the ciphers:

.. DEFAULT

.. HIGH

.. MEDIUM

.. LOW

==========

6. Known Issues

==========

- Remote authentication from Tacacs+ server fails when Tacacs+ version is set to V0.
- Remote Authentication fails when Kerberos is selected as the Authentication Type.