Avocent® ACS 6000 Advanced Console Server
Release Notes
Version 3.1.0.8 UPDATE!
July 24, 2015

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 Installation/Administration/User Guide for detailed instructions on updating the ACS 6000 console server to version 3.1.0.

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 or newer before the upgrade to version 3.1.0.8.**

In order to have all features listed in this release available through DSView™ management software, DSView™ software version 4.5.0.123 or later and ACS 6000 console server plug-in version 3.1.0.4 are required.

After the ACS 6000 console server firmware has been upgraded to version 3.1.0, 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 3.1.0 provides an internal mechanism which preserves the existing configuration when upgrading from firmware version 3.0.0. However, it is strongly recommended that you back up the system configuration before the firmware version upgrade.

==========

2. Appliance Firmware Version Information

==========

Appliance/Product	Firmware Type	Version	Filename
Avocent® ACS 6000 Console Server	Opcode	V_3.1.0.8	avoImage_avctacs-3.1.0-8.bin avoImage_avctacs-3.1.0-8.bin.md5

==========

3. Features/Enhancements

==========

NOTE: Please refer to the ACS 6000 Installation/Administration/User Guide and/or Command Reference Guide for details about features supported by the ACS 6000 console server version 3.1.0.

Client Browser Support Information:

- Microsoft® Internet Explorer® 11
- Mozilla® Firefox® version 36.0.1 in Windows 7.

- Google Chrome™ browser version 41.0 in Windows 7.

Upgrades included:

- Linux Kernel

  NOTE: The support for PCMCIA cards that are supported by previous firmware versions is affected by this upgrade. The card may not be detected in this release.

- **NEW!** OpenSSL to fix the POODLE issue
- Apache

Major features of the ACS 6000 console server version 3.1.0.8 include:

- Supports Multiple Session Menu functionality similar to one supported by the ACS 5000 console server.
- Supports Zero-touch Provisioning that automates the process of upgrading the firmware to an approved version and sets configuration on the ACS 6000 console server that is being deployed in the network.
    - The ACS 6000 console server will send the “Avocent_ACS6000_XXXXX” string in the DHCP Request as the vendor class identifier (option 60) where XXXXX is the appliance serial number.

  NOTE: Regarding the configuration template being applied to many ACS console servers, the user must take the precaution of editing file commands in the CLI script or XML that would result in actions like the ones described below:

    - configuring a static IP address
    - setting appliance’s host name
    - changing the boot image
- Supports configuration of a Primary Network Interface. A customer will be able to select the primary network interface that will define the system default gateway and system DNS servers.
- Supports Network Failover that allows an administrator to configure a secondary network interface that will take over when the primary network interface is not available. The primary network can become unavailable if it is down or a configured probe (IP address) has become unreachable.

  NOTE: The user should be aware of the following caveats with regard to the operation and configuration of Network Failover:

    - Both the primary and the secondary interfaces must be available and enabled.
    - The primary interface cannot be changed or disabled while Network Failover is enabled.
    - Disabling the secondary interface will disable Network Failover.
    - If *ppp0* is selected as the secondary interface, the user must ensure that the ppp0 interface is enabled. Disabling ppp0 will not disable Network Failover by default (as indicated in the previous statement).
    - When a VPN is selected for Network Failover, IPSec must be enabled.
    - During a failover event, if a VPN is selected for Network Failover, IPSec will restart; after the primary has recovered, IPsec will restart. As a result of this behavior, all existing VPN connections will restart when the failover event occurs, and after the primary has been restored.
    - If the AT&T Huawei broadband modem (E-368) is used as the Network Primary for Network Failover, then the trigger action must be one of “Unreachable IP … ”. The Primary Interface Down trigger is not supported with this modem.

- Before selecting the *Unreachable DSView* trigger, the user must ensure that the ACS console server is first enrolled in the DSView™ management software.
- Before selecting the *Unreachable IP Address* trigger, the user must ensure that the chosen IP address is reachable by the ACS console server by using a “ping” command. If the selected IP address is unreachable at the time of configuration, the Network Failover mechanism will immediately trigger.

- Supports fourth Generation Wireless Modem:
  - Devices:
    - NetGear – model 313U
    - Pantech – model UML295
    - Huawei – model E368 USB Connect Force 4G
    - Huawei – models E1550
    - ZTE – model MF662 USB Modem (APAC - 21.6Mbps)

  NOTE: The following information is required for the wwan to work properly:
  - APN: Should be verified with the service provider. For example, APN for AT&T is broadband.
  - PIN: If locked, SIM is used. Multiple incorrect attempts with PIN may result locking the SIM. PIN is not needed when unlocked SIM is used.
- Enhancements in Security Profile:
  - Allows customer to select TLS version 1.1 and/or 1.2. SSL version 2 and SSL version 3 are not supported.

    NOTE: TLS 1.0 is always supported since it is required for DSView™ software integration.
  - Allows customer to select *SFTP* or *SCP* to upload and download files via the user interface (UI).
    - Upload: Save Configuration
    - Download: Firmware Upgrade, Restore Configuration, X.509 Certificates, Rack PDU Firmware Upgrade
- Supports save configuration in the following formats: Compressed File, CLI script and XML

  NOTE: The Compressed File format shall be used for configuration enforcement. CLI script and XML formats shall be used if customer wants to edit the configuration before applying it to the appliance. Both formats take more time to be applied and may generate an error message in the UI.

==========

4. Bug Fixes

==========

Bug fixes include in version 3.1.0.8:

- Administrator can configure DSView™ software Access Rights via the CLI. (L3- 487234-379415669)
- Administrator can allow regular users to run cli-migration via sudo command. (L3- 487234-408492824)
- Admin user can launch ssh session against another server from his ACS console server shell session. (L3- 487234-414562739)
- The ACS 6000 console server will verify downloaded certificate. (L3-487234-393375812 and L3-487234-395302592)
- AD/LDAP group mapping authorization works. (L3-487234-411915097)

- Administrator can use RADIUS remote authentication without configuration of accounting server. (L3-487234-421186355 and L3-487234-413831233)
- Appliance accepts Server Name Indication extension in the request to download Serial Viewer. This will allow customer to use IE-HTTPS with FQDN to access appliance. (L3-487234-399895544)
- Configuration will be applied to appliance via apply configuration template during enrollment of the appliance. Sometimes the DSView™ software returns an error even though the configuration was applied. When this occurs, the customer needs to run the resync operation. (L3-487234-420238102)
- User can access the ACS 6000 console server serial target via the DSView™ software third party serial viewer as plink. (L3-487234-408492824)