Cyclades™ACS 5000 Advanced Console Server Appliances
Release Notes
Version 3.3.0-10
August 30th 2011

This document outlines:

1. Update Instructions
2. Appliance Firmware Version and Language Support Information
3. Enhancements
4. Fixes
5. Known Issues / Restrictions
6. Configuration Details

===
Update Instructions
===

Please refer to your installation, administrator and user manual for detailed instructions to update the Cyclades™ ACS 5000 console server to version 3.3.0-10.

In order to have all features listed in this release available through DSView™ 3 management software, DSView™3 software version 3.7.1 and the Cyclades™ ACS 5000 console server plug-in version 3.3.5 are required. An appliance firmware package to upgrade from DSView™ 3 software is also available.

After Cyclades™ ACS 5000 console server firmware has been upgraded to version 3.3.0-10, it is mandatory that the Web browser cache of any system which intends to be connected to the Cyclades™ ACS 5000 console server Web interface is cleaned up.

Cyclades™ ACS 5000 console server firmware version 3.3.0-10 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.

===
Appliance Firmware Version and Language Support Information
===

Appliance/Product	Firmware Type	Version	Filename	Part Number
Cyclades™ACS 5000 console server (all models)	Opcode	V_3.3.0-10	FL0588-007.bin FL0588-007.bin.md5 FL0588-007.pkg	FL0588-007

English language supported.

```
================================================================
```
Enhancements
```
================================================================
```

Please refer to your installation, administrator and user manual for a detailed list of features supported by the Cyclades™ACS 5000 console server version 3.3.0.

Features of Patch Release 3.3.0-9:
1. Appliance's Serial Number can be retrieved by SNMP query. New CYCLADES-ACS5000-MIB.ASN file has the description of this OID.
2. 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.
3. 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.

```
================================================================
```
Fixes
```
================================================================
```

Cyclades™ ACS 5000 3.3.0-10 release contains the following fix:

1. Configuration upgrade from 3.3.0-5 or earlier version updates Power Mgmt configuration file (/etc/pmd.conf) without error (SAP 65642621)

Cyclades™ ACS 5000 3.3.0-9 release contains the following fix:

1. New mechanism tries to recover chain of Cyclades™ PM with 1.9.4 version (SAP 65613042).

```
================================================================
```
Known Issues / Restrictions
```
================================================================
```
Known issues present in this release:

1. Power management is taking longer to get all the information from the PM PDU during start up time when there are a large number of PM PDU units to be detected. During this phase, users can feel some slowness to access the appliance.

2. Configuration of alarm current threshold per segment is not available for Cyclades™ Intelligent Power Distribution Unit with 2-segment running firmware version 1.8.0 or early

3. Detection of Cyclades™IPDU with 2-segment will fail if the unit is daisy chained after an Avocent®PM PDU running version 1.3.0. This problem affects the Power Device Add operation through DSView™ 3 management software, because the chain will not be detected.

4. Detection of Cyclades™ IPDU with 2-segment running firmware version 1.9.1 will fail if the unit is daisy chained after a Cyclades™ IPDU running firmware version 1.9.2.

5. The support for '-F' option (force upgrade for the PDU without logical connection) was removed from pmfwupgrade command.

6. Using the Cyclades™ ACS 5000 console server Web interface, whenever a new user is configured with privileges to manage the outlets of a certain server (Ports -> Physical Ports -> Modify Selected Ports -> Power Management), it is necessary to press buttons "Try Changes" or "Apply Changes" before the new user can be seen in Applications (Applications -> PMD Configuration -> Users Management).

7. The upgrade of the Cyclades™ ACS 5000 console server firmware code may fail if the internal files are concurrently being accessed by another process or operation. If this occurs, please try firmware upgrading again until it succeeds. When the upgrade operation is performed from DSView™ 3 software, make sure to review the Operation Results and confirm it has finished successfully before the Cyclades™ACS 5000 console server can be rebooted. It is also recommended that the DSView™ 3 software status polling is disabled while firmware upgrade is run. NOTE: Please do not reboot the Cyclades™ACS 5000 console server if the firmware upgrade operation has failed. It will render the console server completely inoperable and require technical assistance.

8. The Cyclades™ ACS 5000 console server Boot Application will **not** be upgraded to support IPV6 protocol, which means that the Cyclades™ ACS 5000 console server boot configuration will **not** support IPV6 protocol. If firmware upgrade using IPv6 is necessary, the user can do it through FTP or scp using either WMI (Web Management Interface) or CLI (Command Line Interface).

9. IPv6 support will **not** be available for the following services:
    a. IPMI (Intelligent Power Management Interface)
    b. NIS Remote Authentication
    c. Port Virtualization (Clustering)
    d. NFS (Network File System)
    e. LPD (Line Printer Daemon)

10. Samba – client access to the File System with the Microsoft Windows® interface removed from the Cyclades™ ACS 5000 image due to size limitations.

11. When the Hostname Discovery feature is enabled, the "Physical Ports" screen doesn't automatically reflect Hostname changes in the servers connected to the Cyclades™ACS 5000 console server serial ports. It is necessary to log-out from the web interface, and then log-in again to refresh the browser cache and load the new names.

12. As DHCPv6 protocol does not provide IPv6 prefix lengths, just IPv6 addresses, there must be an IPv6 router providing advertisement messages with network prefixes to the ACS console server when it is configured to obtain its IPv6 address from a DHCPv6 server. If the prefix is not sent by a router, the ACS console server will become unreachable. This is a limitation of the DHCPv6 protocol.

13. When the IPv6 configuration method for the Ethernet interface is set to DHCP, DHCPv6 parameters (stateful IPv6 address, DNS server and Domain name) are

accepted even if the "Managed address configuration" and "Other configuration" flags sent by the IPv6 router are not set.

14. If the authentication method is NIS, the user is advised to create an entry for user id 0 in the authentication server; otherwise many of the Cyclades™ ACS 5000 console server applications may not work. Another option is to always use NIS/Local instead of NIS.

15. Some events that occur in the Windows® operating system environment may not be correctly formatted. For further information go to:
http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/Usage/Windows.aspx

==

Configuration Details

==

Please note the following Configuration Details for the release 3.3.0-9:

1. The polling rate configuration is now part of serial port configuration under [PORTS] section in /etc/pmd.conf file. The old "<PDU-ID>.pollrate" is obsolete. The upgrade procedure will get the lesser configured value to be the polling rate of all serial ports configured as Power Management.

Please note the following Configuration Details for the release 3.3.0-6:

1. It is necessary to configure Hardware flow control in the serial ports configured as dial-in profile (PPP not-auth or PPP) because most of external modem has this configuration by default.

2. It is necessary to explicitly specify the local and remote IPv6 addresses when using PPP connections with IPv6, otherwise the PPP connection will not work (see your installation, administrator and user manual for configuration details).

3. When adding an IPv4 community (SNMP Configuration) and the network is using dual-stack mode, you should configure as source an IPv4-mapped-Ipv6 address.

4. When editing file /etc/resolv.conf manually, there should be no spaces after the addresses configured for DNS servers.

5. It is necessary to edit the /etc/ssl_version.conf file to configure SSL version and cipher level. Follow the syntax:

SSLVER=<SSLv>

SSLCIPHER=<level>

Where:

<SSLv> - SSL version:

.. SSLv2 – only version 2

.. SSLv3 – only version 3

.. SSLv23 – both version 2 and version 3

<level> - level of the ciphers:

        .. DEFAULT

        .. HIGH

        .. MEDIUM

        .. LOW

6. When configuring X.509 Authentication in ssh server, the file /etc/ssh/authorized_keys must allow read and write permissions. This can be done by issuing the commands below:
   chmod 600 /etc/ssh/authorized_keys
   chmod 755 /
   config runconfig
   config savetoflash

7. The 'Hostname Discovery' feature
   It requires the following configuration in the serial port:
   a) Connection Protocol: Console (Telnet), Console(SSH) or Console(SSH/Telnet)
   b) DCD State: Regard
   c) Data Buffering: Enabled
   d) Data Buffering Destination: Local
   e) Data Buffering File Size (bytes): 100 or more
   f) Hostname Discovery: checked
   g) Timeout(seconds): 10

   It has by factory default the following configuration:
   a) Probe String: "\n"
   b) Answer String: "([A-Za-z0-9\._-]+)[ ]+[Ll]ogin[:]?[ ]?$"
      This answer will match most of Unix

   It uses the following regular expression in Answer String to match the hostname: ([A-Za-z0-9\._-]+).
   Examples of Answer String:
   a) Most of Linux machines, the hostname comes in the login prompt, for example "MY-Linux login:"
      The answer string "([A-Za-z0-9\._-]+)[ ]+[Ll]ogin[:]?[ ]?$" will get MY-Linux as the hostname of the server.
   b) Cisco routers, the hostname comes in the prompt, for example "Cisco2522>".
      The answer string "([A-Za-z0-9\._-]+)[>#]" will get the Cisco2522 as the hostname of the device
   c) ACS 6000 appliance, the hostname comes in the middle of the banner, for example "ACS6000 2.0.1.3-20090507 MY-ACS6048 ttyS0"
      The answer string "ACS6000 [^]* ([A-Za-z0-9\._-]+) ttyS" will get the MY-ACS6048 as the hostname of the ACS 6000.