Avocent® Universal Management Gateway 2000/4000/6000 Appliance Release Notes
Version 2.4.0.4
February 7, 2014

This document outlines:

1. Update Instructions

2. Local Client Requirements

3. Features and Enhancements

4. UMIQ Module Support

5. Service Processor Support

6. Known Issues

===

1. Update Instructions

===

Please refer to the installer/user guide for detailed instructions on updating the Avocent® Universal Management Gateway appliance.

If the current appliance version is older than 1.3.2.1, please update to appliance version 1.3.2.1 before upgrading to the latest 2.x.x.x version.   If your appliance(s) had already been upgraded multiple times using version 2.x.x.x versions, and you see problems configuring the Service Processors, please contact Technical Support for a recovery procedure.

IMPORTANT NOTE: When upgrading the appliance to 2.2.1.10 or later from 2.1.1.6 or earlier, please ensure power is retained on the appliance for at least 60 minutes to allow the upgrade to complete. The appliance upgrade process requires more time in this version as the FPGA is being upgraded. Also, please avoid rolling back the version from 2.2.1.10 or later to 2.1.1.6 or earlier since there will be a FPGA downgrade procedure. If there are any issues with upgrade or rollback, please contact Technical Support for additional assistance.

In order to have features listed in this release available through DSView™ 4 (v4.1.x) management software, the Avocent® Universal Management Gateway appliance plug-in version 2.4.0.3 or later is required.

Older versions of the DSView™ software and the Avocent® Universal Management Gateway appliance 1.x plug-in may work with this new firmware but could have limitations with the features or bug fixes of this release.

After upgrading the appliance to version 2.4.0.4, if KVM sessions launched via the DSView™ software display an error message, resync the appliance with the DSView™ software and try again.

NOTE: If the Web interface Session times out while transferring the firmware upgrade file, the upgrade process will be cancelled. If this occurs, lengthen or disable the Session Time-Out setting for the Admin user in the Web interface before starting the upgrade.

===

2. Local Client Requirements

===

Software	Version
Java (32-bit)	Java 6 Update 45, Java 7 Update 51
Adobe Flash	11.3.300.262
Internet Explorer	7, 8, 9
Firefox	3.6, 18
Chrome	26

NOTE: 64-bit editions of Java are not supported. Occasional KVM session "network error" failures have been seen using later updates of Java 7. Please use Java 6 Update 45 or Java 7 Update 5 to avoid these failures.

NOTE: If using Java 7 Update 51 and attempting serial and KVM session launches from the DSView™ software and the Avocent® Universal Management Gateway appliance, confirmation prompts may be presented by the Java Run-time Engine even though there are no specific security concerns listed in the details of the prompt.   The launches can be continued by clicking *Cancel* or *Continue* to follow through on the launch process.

NOTE: Please check the DSView™ software release notes for the latest client requirements for the DSView™ software.

===

3. Features and Enhancements

===

Firmware version 2.4.0.4 is an update of the Avocent® Universal Management Gateway 2000/4000/6000 appliance firmware.

This version includes the *Trellis*™ Intelligence Engine version 3.0.0.26 for use with the *Trellis*™ Real-Time Infrastructure Optimization Platform, version 3.0.1.

Please refer to the installer/user guide for a detailed list of features supported by the Avocent® Universal Management Gateway appliance.

New general features and resolved issues in this release include:

- Liebert® MPH/MPX Power Distribution Units (PDU) are now supported in the Avocent® Universal Management Gateway appliance and in the DSView™ 4 software.

- Liebert® MPH2/MPX2 Power Distribution Units (PDU) are now supported in the Avocent® Universal Management Gateway appliance.

- The next-generation 6K asset tags are now supported for Methode Asset Location appliances.

- Ports 10199 and 11099 are now blocked by default. These ports are only used for debugging and should not be open by default.

- Additional programs (/usr/bin/startsnmpsvr and /usr/bin/stopsnmpsvr) are available to start and stop the SNMP daemon, if needed, for special applications.

- The /etc/dhcpd.conf network configuration file may now be edited by an admin user if needed for special applications.

- HP iLO4 blades are now recognized underneath an HP BladeSystem chassis so that blade-specific information is presented and SPAccess blade-through-chassis sessions are functional.

- A newly launched serial session will no longer resend the last transmission from the previous serial session to the serial target.

- Disabled serial or PDU targets will now remain disabled and not automatically re-enable the target.

SPM and SPAccess improvements in this release include:

- HP iLO 1 Service Processors are no longer supported.

- HP BladeSystem firmware version 4.01 is now supported.

- IBM IMM firmware version YUOOF7C is now supported.

- IBM BladeCenter firmware version BPET66B is now supported.

- Cisco UCS-C firmware version 1.4.3(u) is now supported.

- Dell iDRAC6 firmware version 1.96 for monolithic servers is now supported.

- Dell M1000e firmware version 4.50 is now supported.

Support Issues Addressed In This Release

Issue	Resolved Issue Description
487234-308956025	The event numbers associated with notification rules do not change when notifications are enabled or disabled.
487234-308955507	The Japanese translation for "Session Times Out" was corrected.
487234-334094209	Sensor data from Service Processors will now be returned whether or not the power is removed from the server. Some Service Processors, such as the Dell iDRAC6 monolithic, do not return sensor data when the server is turned off. After the server power is restored, refresh the Targets/SP/Sensors tab display if needed to update the sensor display.
487234-301196555	SPAccess sessions may now be successfully launched directly to Dell M610/M710 (iDRAC6) blade servers with iDRAC6 Service Processor firmware 3.50; however, sessions launched through the chassis are still failing. Please add or discover the individual iDRAC6 blades separately from the chassis (if this has not already been done), then launch SPAccess sessions directly to the iDRAC6 blade server.
487234-312578162	The wobbling KVM display seen on some servers at boot time was corrected.
487234-262298605	The LDAP authentication order can now be set using the command-line interface.
487234-262305781	LDAP Group Mapping can now be set with Group Name containing a space.
487234-342666428	When the Network mode is changed from Normal to Failover, the eth0 IP address is used to automatically set the bond0 IP address, and the interface is automatically set to bond0. When the Network mode is changed from Failover to Normal, the interface is automatically set back to eth0.
487234-309147479	An appliance reboot will no longer attempt to reinstall the *Trellis*™ platform Intelligence Engine.
487234-326095449	Static routes are now retained through an appliance reboot.
487234-315760700	Disconnected or unresponsive temperature sensors are now shown as "N/A" instead of "-40F".

===

4. UMIQ Module Support

===

NOTE: Attaching either the UMIQ-V1 or UMIQ-V2 module to a Windows target requires the USB CCID driver to be installed. If the user is prompted by the Windows New Hardware Wizard, the *Next* button should be selected.

NOTE: The Video Viewer included with the DSView™ 4 software does not support non-automatic Keyboard/Video/Mouse (KVM) video sharing when the first video session is launched. When video sharing is needed, please configure the appliance to automatically share video by navigating (within the DSView™ software) to *Unit Overview-Target Settings-KVM Settings-KVM Devices* and selecting *Automatic Sharing*.

NOTE: When using the DSView™ 4 software and moving a UMIQ module from one port to another port on the Avocent® Universal Management Gateway appliance, the appliance must be resynced in the DSView™ 4 software to correctly update the port. Also, if the *Automatically Delete Offline Modules* configuration is selected, delay at least ten seconds between disconnecting the UMIQ module from the appliance before reconnecting it to a different port.

===

5. Service Processor Support

===

Tested Service Processors and Firmware

Service Processor	Firmware Version
Cisco UCS CIMC/Monolithic (C210)	1.4.3t
Dell 10G iDRAC	1.53 (Build 3)
Dell DRAC 4	1.75 (Build 06.03)
Dell DRAC 5	1.65 (12.08.16)
Dell DRAC/MC	1.6.9
Dell iDRAC blades (M600/M605/M805)	1.65
Dell iDRAC6 blades (M610/M710)	3.50 (except SPAccess Blade-through-Chassis)
Dell iDRAC6 monolithics (R210/R410/R710)	1.96
Dell iDRAC7 blade (M620)	1.40.40
Dell iDRAC7 monolithic (R320)	1.40.40
Dell M1000E Chassis	4.40
FSC iRMC	2.30G
FSC iRMC S2	5.68A
HP BladeSystem	4.01
HP iLO 2	2.23
HP iLO 3	1.61
HP iLO 4	1.30
IBM BladeCenter	BPET62U
IBM IMM (x3550 M2, x3650 M2)	YUOOF7C
IBM IMM2	1AOO40Z 25 Apr 2013
IBM RSA II	GGEP42A
IPMI 1.5	N/A
IPMI 2.0	N/A
SUN ALOM	1.6.10
SUN ELOM	3.2
SUN ILOM	2.0.2.6

Supported Service Processor Features

Service Processor	Sensors	Power Information	Power Config	Power Control	Alert Destination	FRU Information	Get Time	Set Time	LED Control	LED Status	System Event Log	SoL Session	SOL Configuration	Browser UI	Browser AutoLogin	SSL	Telnet Session	SSH Session	Auto-login SSH	vKvm	Virtual Media
IPMI 1.5	✓			✓	✓	✓	✓	✓	✓		✓			*		*	*	*			
IPMI 2.0	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	*		*	*	*			
IDRAC 7 (12G)	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	*	*	*	*	*	*	*	*
IDRAC 6 (11G)	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	*	*	*	*	*	*	*	*
Dell DRAC 5	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓	*	*	*	*	*	*	✓	✓
Dell 10G	✓			✓	✓	✓	✓	✓	✓		✓										
Dell DRAC 4				✓	✓		✓				✓	✓		D	D	*	*	*	*	D	D
HP ILO 4	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	*	*	*		*	*	✓	✓
HP ILO3	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓	*	*	*		*	*	✓	✓
HP ILO2	✓	✓		✓	✓				✓	✓	✓	✓		*	*	*	*	*	*	✓	✓
Sun ELOM	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓	D	D	*	*	*	*	D	D
Sun ILOM	✓			✓		✓	✓	✓	✓		✓	✓		D	D	*		*	*	D	D
Sun ALOM	✓			✓							✓	✓					*	*	*		
IBM IMM2	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	*	*	*	*	*	*	*	*
IBM IMM	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	*	*	*	*	*	*	*	*
IBM RSA II	✓			✓			✓	✓	✓	✓	✓	*		D	D	*	*	*	*	D	D
Cisco UCS-C (Monolithic)	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	*	*	*	*	*	*	✓	✓
Fujitsu/Siemens IRMC	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓	D	D	*	*	*	*	D	D
Fujitsu /Siemens IRMC II	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	*	*	*	*	*	*	✓	✓
Dell M1000E	✓	✓			✓			✓	✓	✓	✓			*	*	*	*	*	*		
Dell M1000E (Blade)				✓					✓	✓	✓	✓		†	†	†	†	†	✓		
Dell DRAC/MC	✓	✓		✓	✓		✓	✓	✓	✓	✓			D	D	*	*		*		
Dell DRAC/MC (Blade)				✓					✓	✓				D	D					D	D
HP BS	✓	✓			✓		✓	✓	✓		✓			*	*	*	*	*	*		
HP BS (Blade)	✓	✓		✓		✓				✓		✓		†	†	†	†	†			
IBM BC	✓	✓			✓		✓	✓	✓	✓	✓			*	*	*	*	*	*		
IBM BC (Blade)	✓	✓		✓								✓						†	†	†	†
Generic														*				*	*		

🟩	New Feature / SP	🟨	New command support	⬜	Unsupported	
✓	Supported feature	*	Supported if available	†	Features inherited from Chassis	
D	Only via DirectCommand support in DSView™ 4 software					

General Notes

- Do not manage the same Service Processor from multiple Avocent® Universal Management Gateway appliances at the same time. Some Service Processors may show erratic behavior when sessions limits are exceeded, or with simultaneous access. This may manifest in the appliance Web interface as being unable to discover, manually add Service Processors or errors when viewing and managing SP settings.

- When upgrading the appliance firmware, Service Processors previously added with IPMI 2.0 profiles will not be updated, even if the Service Processor is now a newly supported profile in the upgraded Avocent® Universal Management Gateway appliance release. If the full capabilities of the specific Service Processor are needed, delete and then re-add the Service Processor to use the newly defined profile.

- When attaching a Service Processor chassis on one of the private ports on the back of the Avocent® Universal Management Gateway appliance for automatic discovery, make sure the chassis and all the blade servers in the chassis are configured for DHCP. All manageable components must be configured for DHCP for automatic discovery to work correctly.

- Some Service Processors may take several minutes to query SEL records. If the command takes more than 1 minute, the Web interface query may timeout. If this occurs, check the SEL record list via the SP's native Browser UI or CLI and empty the list.

- Service Processors that support virtual media may have problems mapping removable media devices when the client is the Avocent® Universal Management Gateway appliance local port or a PC running a Linux operating system. Potential workarounds include:

    a. Make sure the Service Processor's firmware is the latest supported by the Avocent® Universal Management Gateway appliance (see table at the beginning of the Service Processor Support section in these release notes).

    b. Create a CD (ISO) or disk (IMG) image file containing the data to be accessed by the server. Service Processors that do not properly mount a remote block device will usually mount an image file, even if the file is stored on that same block device.
    NOTE: On the IBM BladeCenter, only ISO images map correctly.

- After many SPAccess sessions in some browsers, it is possible that all available cookies may be consumed. If the browser presents an error message that no more cookies are available, please close all open tabs and windows for that browser to clear the cookies.

- When adding a Service Processor, the alias does not accept a space. If a user needs a space in the name, after adding, they can modify the name via Administration/Targets.

- When adding a Service Processor, options are presented for "Cisco Chassis" and "Oracle ILOM 3". These options are not yet supported and should be ignored.

- When a Service Processor SP Console session is launched, a "SoL Session Launched" event is logged in the appliance event log, and in the DSView™ 4 software event log if the appliance is managed using DSView™ 4 software.

- Power state transitions from Service Processors may not be identified and displayed in the appliance Web interface or DSView™ 4 software for up to fifteen minutes after the transition occurs.

- The Serial-over-LAN Data Buffering Download Log feature is currently not functional.

NOTE: The Java JRE-7u51 has introduced strict security requirements where native Service Processor vKVM applets will fail to launch until the Service Processor supports the Java security requirements. The Service Processor vendor should provide firmware updates to resolve these issues. Until the updates are in place, consider workaround options that are consistent with your corporate security requirements.

Dell DRAC4 and DRAC5

- When the maximum number of sessions in DRAC4 or DRAC5 has been reached, a new AutoLogin or vKVM SPAccess session will fail. The failure can be recovered by resetting the SP via Telnet or SSH. The command for SP reset is 'racadm racreset'.

- The DRAC5 does not support use of the forward slash ("/") in login passwords. Avoid use of the forward slash in the password definition.

- DRAC5 firmware supports only IE7 and Firefox2 browsers. SP Access sessions, especially vKVM and VM sessions may not work in newer versions of Firefox and Chrome and are not supported. SP Access to the DRAC5 is possible with IE9.

Dell DRAC6 Monolithics

- Sensor data is not returned from iDRAC6 monolithics when the Dell server is turned off. After the server power is restored, refresh the Targets/SP/Sensors tab display, if needed, to update the sensor display.

- The vKVM feature of the SP's native Web interface defaults to ActiveX. For better integration with the SP Access feature, it is recommended to change the default setting on the SP to launch the Java viewer by default.

Dell DRAC6 Blades

- On the M1000e, occasionally clicking the *Launch iDRAC GUI* button for one of the blades will not complete a single sign-on login due to a Dell limitation. Please log in manually in these cases.

NOTE: When M600, M605 or M805 blades are discovered by the appliance as standalone Service Processors, occasionally the SPAccess Browser and SPAccess Browser-Autologin buttons are not enabled in the Web interface or in the DSView™ 4 software. If this occurs, please delete the Service Processor from the appliance, reset the Service Processor, and then add the Service Processor back into the appliance.

Dell M1000e CMC

- The login process for the M1000e may take up to 20 seconds after proper username and credentials are presented, so it may take several seconds to access some features in the Avocent® Universal Management Gateway appliance Web interface. For example, displaying power information may take 15-20 seconds for an M1000e chassis.

- When connecting an M1000e chassis to a private port of the appliance, SPAccess AutoLogin sessions to blades either directly or through the chassis may intermittently abort if using FF or IE. If this is seen, try using Chrome.

- Each SPAccess session launched to blades in a blade chassis using blade-through-chassis (use of the single sign-on feature of the chassis to access the blades indirectly through the chassis) opens a separate session on the chassis, so it is possible that all active sessions for the chassis may be consumed if multiple sessions are launched in a short period of time. If this happens, please log out of active blade sessions and allow time for the chassis to time out its sessions.

- SPAccess sessions may now be successfully launched directly to Dell M610/M710 (iDRAC6) blade servers with iDRAC6 Service Processor firmware 3.50; however, sessions launched through the chassis are still failing. Please add or discover the individual iDRAC6 blades separately from the chassis (if this has not already been done), then launch SPAccess sessions directly to the iDRAC6 blade server.

Dell iDRAC7 Monolithics and Blades

- SPAccess Browser-only sessions may not work to an iDRAC7 when using the VGA Console. Manually launch a new tab and browse using (https://<IP>) to the SP using the Browser Tabs on the VGA Console.

- The Virtual Media session for a iDRAC Service Processor sometimes will not load when accessed using the VGA Console of the appliance. If this occurs, please use the appliance remote Web interface for Virtual Media access.

FTS iRMC

- Power data can be retrieved from FSC iRMC service processors only if their firmware includes the DCMI IPMI extensions (such as the Intel Node Manager).

FTS iRMC S2

- Power data can be retrieved from FSC iRMC S2 service processors only if their firmware includes the DCMI IPMI extensions (such as the Intel Node Manager).

- iRMC S2 SPs that use log in passwords containing the ampersand (&) character cannot be discovered or managed by the Avocent® Universal Management Gateway appliance. The SP can be discovered and managed when the login passwords do not contain the ampersand character.

- The vKVM (Video Redirection) viewer will not start if the user starts a Browser or Auto-login session and manually browses to the Video Redirection (non-Java Web Start) in the iRMC browser UI. The user should instead use the JWS launcher for video redirection.

HP iLO 2

- The iLO 2 does not support use of the single or double quotation marks in login passwords. Avoid use of quotation marks in a password definition.

- The HP iLO 2 Virtual Media applet fails when launched using the VGA console of the Avocent® Universal Management Gateway appliance. Please use the remote Web interface for these operations.

HP iLO 3

- Single quotation mark characters are not permitted in username and passwords entered in the SP browser UI for the iLO 3.

- The indicator blink control should not be enabled in the appliance Web interface as the iLO3 does not support this function.

HP iLO 4

- Single quotation mark characters are not permitted in username and passwords entered in the SP Browser UI for the iLO 4.

- The indicator blink control should not be enabled in the appliance Web interface as the iLO4 does not support this function.

HP BladeSystem and Blades

- The HP Integrity blade product line is not supported as these blades use a different management interface than the Proliant blades.

- The HP BladeSystem firmware supported by the Avocent® Universal Management Gateway appliance does not support the Chrome browser. Use Firefox or IE browsers for SP Access sessions to the BladeSystem.

- Occasionally, all HP iLO blades within a HP BladeSystem chassis are not discovered as standalone targets when adding these blades as new targets. Please attempt to discover these blades again to complete the add target operation.

- Each SPAccess session launched to blades in a blade chassis using blade-through-chassis (use of the single sign-on feature of the chassis to access the blades indirectly through the chassis) opens a separate session on the chassis, so it is possible that all active sessions for the chassis may be consumed if multiple sessions are launched in a short period of time. If this happens, please logout of active blade sessions and allow time for the chassis to timeout its sessions.

IBM RSA-II

- When a vKVM session is connected on an RSA-II server, a second login with the same user ID will cause the original vKVM session to be disconnected. This includes a second login through the Avocent® Universal Management Gateway appliance which will use the same user ID. This behavior is by design in the RSA-II servers.

- Intermittent load failures of the vKVM and VM applets on RSA-II servers have been recorded when the JRE is allowed to keep temporary files on the computer. When using these vKVM and VM applications on RSA-II servers, Avocent recommends setting the JRE to disallow temporary file storage through the Java Control Panel.

- vKVM operation to RSA-II servers is incompatible with JRE-6u13. Clients should use JRE-6u14 or later for these applications.

- The native browser UI for the IBM 3950 RSA-II server will not allow login if the password contains special characters unless the SP firmware is upgraded to A3EP40A or later.

IBM BladeCenter and Blades

- If the SP discovery feature is used to manage the IBM BladeCenter, the IBM BladeCenter needs to be configured so that its "lockout period after 5 login failures" is one minute, if this setting is consistent with corporate security requirements. This setting is located within the IBM BladeCenter web interface under *System-MM Control-Login Profiles-Global Login Settings.* Otherwise, the IBM BladeCenter must be manually added to the appliance.

- When adding an IBM BladeCenter to an Avocent® Universal Management Gateway appliance, the user account of the IBM BladeCenter provided to the Avocent® Universal Management Gateway appliance must have its "Maximum simultaneous active sessions" set to 0.

- The IBM BladeCenter Virtual Media applet fails when launched using the VGA console of the Avocent® Universal Management Gateway appliance. Please use the remote Web interface for these operations.

IBM IMM Monolithics

- IMM-based monolithic servers purchased with the "IMM Standard" option do not support vKVM. The Avocent® Universal Management Gateway appliance cannot detect the "IMM Standard" configuration prior to web interface login, so the user is not notified until after the vKVM login attempt.

- The IMM Monolithic servers do not support use of the special characters ':', '&', '\' and '<' in login passwords.

- If the SP discovery feature is used to manage any type of IBM IMM or BC server, the IMM needs to be configured so that its "lockout period 5 login failures" is one minute. This setting is located within the IMM web user interface under *System -IMM Control-Login Profiles-Global Login Settings*.

- SP's may deny login requests if there are too many users / connections - this can result in '500 - Internal Server Error' messages being displayed when starting SPAccess sessions to the IMM. Check if there are multiple sessions connected to the SP using the SP's native Web interface and close them. It may also be necessary to reset the SP to restore connectivity.

- Remote Control sessions launched from the IMM's native Web Page in an SPAccess Browser or Auto-login session may fail to start using the Chrome browser. If this issue is seen, try using Firefox or IE9.

IBM IMM2 Monolithics

- SPAccess sessions to IMM2-based monolithic servers may not function correctly using the Google Chrome version 28 browser.   Please upgrade the browser to version 29 or later.

- When logging out of a SPAccess session to a IMM2-based server, all page elements are not downloaded. Refreshing the browser window will restore all page elements.

Sun ALOM, ELOM, ILOM

- ILOM servers must have their http service running to be properly discovered using the SP Auto-Discovery or IP Discovery features. If the http server is not running, the ILOM must be added to the Avocent® Universal Management Gateway appliance using the Manual SP Add feature.

- ALOM servers lack a management web interface natively. The Avocent® Universal Management Gateway appliance does not support custom implementations of ALOM that include a Web interface.

- ELOM and ALOM SPs that use login passwords containing special characters cannot be discovered or managed by the Avocent® Universal Management Gateway appliance. These SPs can be discovered and managed when the login passwords do not contain special characters.

IPMI 1.5

- Some IPMI 1.5 Dell 10G servers might be discovered as Dell 10G servers when using auto-discovery. They should be manually added as IPMI 1.5 devices if this is seen.

IPMI 2.0

- SP Access Browser sessions to LO100 servers added to the appliance with IPMI 2.0 profiles are not supported.

==

6. Known Issues

==

Upgrading
- KVM sessions may fail after the upgrade of an appliance that had been previously added to the DSView™ management software prior to the upgrade. Resyncing the Avocent® Universal Management Gateway appliance in question will restore KVM functionality.

- An appliance firmware version that is older than the currently installed appliance firmware should not be used in an upgrade operation. Please use the rollback operation to revert to an older firmware version.

Backup/Restore/Restore to Factory Defaults
- The NTP server address is not restored on a Restore from Factory Defaults operation. Please manually set the address as needed.

Command Line Interface
- Event syslog enable/disable configuration using the command line interface is currently not functional. Please use the appliance Web interface for this function.

- An unexpected exception may occur in appliance setting configuration, but the configuration change still occurs. Please ignore the exception message.

VGA Console

- When rebooting the system, there is a small chance that the *Restarting system* message followed by machine restart will appear on the VGA Console. If this occurs, a power cycle of the Avocent® Universal Management Gateway appliance will be needed to recover the KVM appliance.

- The TG3 used in some Avocent branded LCD trays may exhibit delayed mouse movement when used with the Avocent® Universal Management Gateway appliance VGA console.

- The VGA console does not support the Avocent® Universal Management Gateway appliance firmware upgrade feature. You can, however, use the firmware upgrade feature via the Avocent® Universal Management Gateway appliance Command Line Interface (CLI) console by logging in as an admin user and selecting *Update Firmware* from the menu.

- If the user attempts to login to the appliance with an expired account when the language is set to non-US English, an *Account has Expired* error message is not displayed.

Authentication
- SSH connections can be made to disabled Serial Ports; however, the connection to the Serial Target itself will not be established.

Networking

- You cannot set a bridged interface as the default gateway. Likewise, if you add the default gateway to a bridged connection, you will lose your default gateway.

- On the initial attempt to set the first valid firewall policy, an *Unknown Policy error occurred* error may appear, but the policy is actually defined. This error does not reoccur on subsequent valid policy definitions.

Web interface

- When rebooting the system, there is a small chance that a login failure will occur on the remote or local Web interface. If this failure persists, a power cycle of the Avocent® Universal Management Gateway appliance will be needed to recover the appliance.

- If the log detail has been changed to Trace, and another user with the same username logs in and back out, the debug level may revert back to default.

- The Avocent® Universal Management Gateway appliance uses a polling mechanism to determine the Service Processor power state. Due to this, there will likely be a delay between when the state changes and the Avocent® Universal Management Gateway appliance updates its user interface.

- A Server Processor's status may remain as *Powered On* if that Service Processor has lost power. If there is a concern about the power status, perform a ping test against the IP address of the Service Processor to validate.

- The default login page of a Web interface session does not match the default language setting of the browser and must be set manually when using the Internet Explorer browser.

- The Image Dump progress popup message remains after the Image Dump is completed and must be closed manually.

- Some columns, by default, are not wide enough to accept the maximum number of characters the entries

in the columns can have. In these cases, the columns can be manually adjusted in width.

- When performing a Factory Reset on a UMIQ module, an exception error may be displayed.

- Event time tags in the Avocent® Universal Management Gateway appliance Web interface event log are actually displayed in local time and should not include a "(UTC)" indication.

- When moving time within the appliance forward for a period of more than a few minutes, the CPU utilization may increase significantly. Please reboot the appliance to restore normal operation.

- An incorrect error message is displayed when an invalid DHCP range is entered in the Dynamic Ranges table of the /Administration/Targets/Port Configuration/DHCP Settings screen.

- A Service Processor Discovery log and the Event log Export functions provide a .CSV file that uses '|' separators instead of ','.

- The Avocent® Universal Management Gateway 2000 appliance does not update the Event Viewer Log page when switching to a different page and back to the Event Viewer Log page. The Event Viewer Log page will reload when the *Next* button is clicked to advance to the next page of Event Log, then the *Prev* button is clicked to return to the original Event Log page.

- The Avocent® Universal Management Gateway 2000 appliance does not currently support filtering of events shown on the Event Viewer Log pages. The events can be filtered by exporting the Event Log and then filtering the events using a separate tool.

- If the Web browser cache history is cleared during an active Web interface session, an HTTP request error will occur on the next Web interface screen refresh. If this occurs, please close the browser window and log in to the appliance Web interface again.

Asset Location

- Due to a Methode CCM limitation, the CCM must be power-cycled when it is disconnected from one Avocent® Universal Management Gateway appliance before it is reconnected to another Avocent® Universal Management Gateway appliance.

KVM/UMIQ Module

- On a heavily utilized Avocent® Universal Management Gateway appliance, a KVM session may fail with the *path is blocked* or *Resource could not be located* error.

- If UMIQ module targets are lost after rebooting an appliance, it is suggested to disable the Automatically Delete Offline Modules setting in the Admin-Targets-KVM Management-Default Settings page.

- It may be necessary to enable then re-disable mouse acceleration before the mouse pointer can be synchronized with a Linux machine.

- A target computer with a video resolution less than 1400 x 900 and a screen refresh of 70 Hz cannot be scaled to a higher KVM resolution.

- When using the DSView™ 4 software and moving a UMIQ module from one port to another port on the Avocent® Universal Management Gateway appliance, the appliance must be resynced in the DSView™ 4 software to correctly update the port. Also, if the *Automatically Delete Offline Modules* configuration is selected, delay at least ten seconds between disconnecting the UMIQ module from the appliance before reconnecting it to a different port.

- Event time tags for UMIQ module-related events in the Avocent® Universal Management Gateway appliance Web interface event log are not adjusted for UTC and are not displayed in sync with other Web interface event log events.

- Occasionally, the port number of a UMIQ module is not updated in the Avocent® Universal Management Gateway appliance Web interface when moving the UMIQ module from one port or the other. The UMIQ module may need to be completely unplugged from the appliance and server, then reattached. If DSView™ 4 software is managing the appliance, the appliance would need to be resynced in DSView™ 4 software.

KVM Viewer

- When a KVM viewer is launched, a new tab or window is created. In Internet Explorer and Firefox, this tab/window closes automatically. In Google Chrome, it is persistent and has to be closed manually.

- On a Macintosh OS, the Virtual Media tool will crash with *The Virtual Media native library cannot be loaded* error.

- On a Macintosh OS, the Manual Video Adjust and Session Options do not work if the KVM session is launched from the Web interface. They do work, however, if the KVM session is launched from the DSView™ software.

- On a Macintosh OS, when trying to access a KVM session that is in use, a user gets a blank pop-up instead of getting a pop-up informing the user that the session is in use.

- If a CAC or Smart Card reader attached to the client is disconnected and re-connected, no active KVM sessions will recognize the reader. To get CAC or Smart Card reader functionality in the KVM session, the session will need to be closed and re-opened.

- In some instances, the KVM Viewer will incorrectly show the correct mapped status of a CAC or Smart Card.

- The KVM Viewer unexpectedly closes after changing the scaling properties on a KVM session with active VM mapping.

- Changing scaling settings in a KVM session causes a second video viewer menu to show for the same session.

- Virtual Media (Linux) - Copying files from the target to USB Drive on KVM client is slow and the file dialog box on the target closes too early. If the file transfer dialog box is not shown, the file will still be copied. This issue does not occur on a Windows client.

- Virtual Media - Cannot map ISO file burned on a CD/DVD to a target. The ISO file can be coped to a HDD and successfully mapped.

- KVM screen re-scaled when mapping a Smart Card using the KVM Viewer in IE7. Suggested workaround is to use Firefox 3.6 if Smart Card functionality is required.

- Some USB Drives may have a very slow write transfer rate when connected to the local USB port and using the KVM Viewer on the local port. If this is seen, please try another USB drive. Transfers using a remote KVM Viewer are not affected.

Serial Targets

- The bit rate for serial ports has been successfully tested at 230.4 Kbps, but there is a potential limitation where only 115.2 Kbps may be supported. If there is a problem using 230.4 Kbps, please reconfigure the appliance and serial target to 115.2 Kbps.

Power Distribution Unit (PDU)

- If a PDU has an issue where it is not responding to the appliance, the non-responsive status is not shown in the outlets of the PDU within the appliance Web interface or DSView™ 4 software.

- An autodetected Serial PDU port cannot currently be reconfigured as a Serial Console port.

- If the Energy Consumption start time is unknown, a *01/01/70 12:00 AM* value will be displayed.

- Before adding the Liebert® MPH/MPX PDU to the Avocent® Universal Management Gateway appliance for power control or configuration, please ensure that the PDU has a unique community name with RW permissions. The Liebert® MPH/MPX PDU will allow duplicate community names to be configured with RO and RW permissions, but then will only allow RO operations.

- If both serially-connected (such as the Avocent Power Management PM 1000, PM 2000 and PM 3000 Power Distribution Units) and IP-connected (such as Liebert® MPH/MPX) PDUs are connected to the Avocent® Universal Management Gateway appliance, a reboot of one of the serially-connected PDUs will cause the rebooted PDU to be displayed with a duplicate name of one of the IP-connected PDUs. Restarting the Web interface session will restore the display of the correct name to the serially-connected PDU.

- Power cycle operations to Liebert® PDU outlets will always fail when launched through the command-line interface and will occasionally fail when launched through the Web interface. Please launch the on/off operations separately to achieve the cycle operation.

- The SNMP community settings for each Liebert® MPH/MPX PDU shown on the Administration/Targets/Rack PDU/Network PDU tab will be displayed as *LiebertEM* name and *RO* type following a reboot of the appliance.

- The default name assigned to a Liebert® MPH2 or MPX2 PDU does not follow the default naming convention to prefix the name with the appliance MAC address. When the appliance is used with the DSView™ software and there are multiple appliances managing the same PDU target, each instance of that same PDU target must be assigned a unique name.

- The Web interface display for Liebert® MPH2 or MPX2 PDU Phases does not include voltage, power consumption, apparent power or power factor.

- The Web interface display for Liebert® MPH2 or MPX2 PDU Branches always displays zero for power consumption, apparent power and power factor.

- The Avocent® Universal Management Gateway appliance can support up to 32 total network-based PDUs (such as the Liebert® MPH/MPX/MPH2/MPX2) in the Avocent® Universal Management Gateway 2000 appliance, 64 total network-based PDUs in the Avocent® Universal Management Gateway 4000 appliance, and 128 total network-based PDUs in the Avocent® Universal Management Gateway 6000 appliance. Up to four PDUs may be daisy-chained per appliance port.

Environmental Sensors

- Humidity sensors may fail to be detected.