Avocent® Universal Management Gateway 2000/4000/6000 Appliance
Release Notes
Version 2.8.0.16
November 19, 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 2.8.0.16 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 2.8.0.16, 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 60
Adobe Flash	11.3.300.262
Internet Explorer	8, 9, 10, 11
Firefox	31

Software	Version
Chrome	36

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 or later 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 2.8.0.16 is an update of the Avocent® Universal Management Gateway 2000/4000/6000 appliance firmware.

This version includes the *Trellis*™ Intelligence Engine version 3.3.0.82 for use with the *Trellis*™ Real-Time Infrastructure Optimization Platform, version 3.3.

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:

- Our next-generation KVM viewers are provided, including ActiveX when the KVM session is launched through the Internet Explorer browser and Java for other browsers. The KVM Viewers include the following features:
    - Session recording and playback
    - Session recording export to QuickTime video framework

  NOTE: The new viewers do not yet support smart cards.
- Samba client is now added for future support of Service Processor firmware updates from a remote share and other needs.
- SNMP trap destination configuration support is now available to enable traps to be sent to external trap handlers.
- Organization of target discovery functions in the Web interface is improved.
- Local serial console handling of input is corrected so that a carriage return is not inserted into the input after the 25th character entered.
- CLI handling of local user creation commands is corrected.
- CLI support of network interfaces is now consistent with the Web interface.

Expanded Service Processor firmware version support in this release includes:

- Dell iDRAC6 monolithic (R210/R410/R710) firmware version 1.98 is now supported.
- HP iLO3 firmware version 1.80 is now supported.
- HP iLO4 firmware version 2.02 is now supported.
- IBM IMM firmware version YUOOG7A is now supported.
- IBM IMM2 firmware version 1AOO64N is now supported.

Support Issues Addressed In This Release

Issue	Resolved Issue Description
487234-262298623 487234-266808310	KVM launches from the Web interface are improved to avoid the *Path Blocked* error.
487234-402148297	Detection of UMIQ module installations is improved to avoid conditions where the UMIQ module can be in an illegal state.
487234-363802922	Adding new service should now not cause an error where a duplicate service is detected.
487234-392229237	LDAP group names containing spaces can now be used correctly in LDAP authentication.
487234-401836066	DSView™ management software DirectCommand sessions will now launch properly.
487234-401271196	The serial viewer launched from the Web interface now connects correctly after the SSH port has been reconfigured.
487234-396194936	The local console will now allow special characters to be passed through in passwords.
487234-386944352	Detection of humidity sensors is improved. Please contact Technical Support for more information.

==========

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/Servers and Firmware

Service Processor	Firmware Version
Cisco UCS-B Chassis and Blades	2.2(1c)
Cisco UCS CIMC/Monolithic (C210)	1.4.3u
Dell DRAC 4 (PowerEdge 1850)	1.75 (Build 06.03)
Dell DRAC 5 (PowerEdge 2950)	1.65 (12.08.16)
Dell DRAC/MC	1.6.9
Dell iDRAC blades (M600/M605/M805)	1.65
Dell iDRAC6 blades (M610/M710)	3.60
Dell iDRAC6 monolithics (R210/R410/R710)	1.98
Dell iDRAC7 blade (M620)	1.56.55
Dell iDRAC7 monolithic (R320)	1.57.57
Dell M1000E Chassis	4.40
FSC iRMC (BX630 S2)	2.30G
FSC iRMC S2 (RX300 S4)	5.75A
HP BladeSystem	4.22
HP iLO 2 (DL580 G5)	2.25
HP iLO 3 (DL380 G7)	1.80
HP iLO 4 (DL360p Gen8)	2.02
IBM BladeCenter	BPET66G
IBM IMM (x3550 M2, x3650 M2)	YUOOG7A-1.46
IBM IMM2 (x3250 M4)	1AOO64N-4.55
IBM RSA II (x3550, x3850)	GGEP42A
IPMI 1.5	N/A
IPMI 2.0	N/A
SUN ALOM (Netra 240)	1.6.10
SUN ELOM (x2200 M2)	3.2
SUN ILOM (x4150)	2.0.2.6

Supported Service Processor Features

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

	New Feature / SP		New command support		Unsupported
✓	Supported feature	*	Supported if available	†	Features inherited from Chassis
G	Get only	S	Set only	G/S	Get and Set
D	Only via DirectCommand support in DSView™ 4 software				

General Notes and Known Issues

- 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 a Service Processor SP Console session is launched, an 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 button in the Web interface is currently not functional, but the log can be manually downloaded from the appliance. An example method to retrieve a log of SoL history from the appliance shell is:

    ssh -t admin:<SP_Name>@<UMG_IP> targetexec solhistory | tee sol.log

- The default state of the IPMI/DCMI privilege for IPMI-based SPs managed by the appliance is not displayed for Service Processors that were discovered prior to appliance firmware upgrade, although any Service Processor added to the appliance prior to appliance version 2.5.0.8 will use the Administrator IPMI/DCMI Privilege. Please delete and re-add the Service Processor to restore the correct display.
- 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.
- The initial Service Processor Discovery operation may stop before completion of the search of the specified range. Please restart the search range if this occurs.
- When connecting a Service Processor to a private port of the Avocent® Universal Management Gateway appliance for discovery, please ensure that the Service Processor has been configured for DHCP address assignment and reset prior to connection for successful discovery. If the appliance firmware is updated by USB boot or net boot, it may be necessary to disconnect the Service Processor and power-cycle or reset it, then reconnect the Service Processor for rediscovery after the appliance is restored to normal operation. If the Service Processor is reconnected before the appliance is restored, it may be necessary to manually discover the Service Processor by defining and launching a SP discovery range including the IP address range for the private port.
- After a Service Processor has been added or discovered into the Avocent® Universal Management Gateway appliance, dynamic data may not be available from the Web interface for up to five minutes and time-outs may be seen during this initial five minute period, depending on network delays between the Service Processor and the Avocent® Universal Management Gateway appliance.
- When a Service Processor chassis has been added or discovered into the Avocent® Universal Management Gateway appliance, the status of the chassis and blades is not updated.

Cisco UCS-B Chassis and Blades

- Blade Virtual Media launches can only be supported if the blade credentials are passed from the viewer back to the Service Processor unencrypted. A second Virtual KVM / Media button is presented in the Web interface to launch the vKVM session so that a Virtual Media session can be launched from the vKVM session using the unencrypted credentials. There is a confirmation prompt to continue the launch. If the Virtual KVM button is used to launch the vKVM session, a Virtual Media session launch from that vKVM session will fail as the Virtual Media credentials will be encrypted. The DSView™ software does not support the unencrypted Virtual Media launch. Also, launching a blade vKVM through a chassis login does not support the unencrypted Virtual Media launch.
- Chassis autologin sessions are not supported.
- SoL configuration for blades is not supported.
- Alerts are not generated when a Cisco UCS-B blade is removed or added from the chassis.
- The offline status of a Cisco UCS-B is not reported correctly when the blade is removed from the chassis.

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 Virtual Media sessions may not work in newer versions of Firefox and Chrome and are not supported. SP Access to the DRAC5 is possible with IE9.

- The Dell DRAC5 Virtual Media applet fails when launched using the VGA console of the Avocent® Universal Management Gateway appliance. Please use the remote Web interface from a Windows client for these operations.

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.

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.
- 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.
- Power information is not available from M600, M605 or M805 blades.
- SPAccess functionality for the M610 and M710 blades is currently not operational.
- Virtual Media connections to the iDRAC6 blade Service Processors are not supported from the appliance local port interface as the Service Processors do not natively support this environment.

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 Dell iDRAC7 Service Processor does not natively support Internet Explorer 11 without compatibility mode set in the browser. Please also set compatibility mode when SPAccess sessions are launched.

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 AutoLogin 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.
- The SoL baud rate selection should not be enabled in the appliance Web interface as the iLO3 does not support this function.
- The currently supported iLO3 firmware has been seen to have compatibility issues with the Firefox browser version 33, which also impacts the SPAccess vKVM operation.

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.
- The HP iLO4 Service Processor appears to have a limitation where the vKVM applet is not launched when clicking the Java launcher buttons after logging into the Service Processor directly using the Firefox browser. This function works correctly when the iLO4 is directly accessed using Internet Explorer and Chrome browsers, and when the SPAccess vKVM launch in the Avocent® Universal Management Gateway appliance Web interface.
- The HP iLO3 and iLO4 Service Processors can connect virtual media sessions when the client is the Avocent® Universal Management Gateway appliance local port or a PC running a Linux operating system using these steps:
    a. Select *Java IRC* within the Remote Console section.
    b. Enter the physical USB drive name in the Local Image File textbox in the iLO3/4 UI. The drive name will be similar to “/dev/sdc1”, where the sdc1 would be replaced with the actual drive name associated with the USB slot.

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 Virtual Media 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 Virtual Media 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 from a Windows client 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*.
- SPs 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 AutoLogin 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.
- The IBM IMM2 Service Processor does not natively support Internet Explorer 11 without compatibility mode set in the browser. Please also set compatibility mode when SPAccess sessions are launched.
- 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 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 event log and any user files in the /var/home and /download directories are not included in the image backup, so please export and save the events and any user files, if needed, when performing a backup operation.

- The backup image cannot be downloaded through the Web interface using the Internet Explorer 11 browser. Please use the Firefox or Chrome browsers for this function, or remove the backup using an external SFTP tool from the /download/images folder on the appliance.

Command Line Interface (CLI)

- Event syslog enable/disable configuration using the command line interface is currently not functional. Please use the appliance Web interface for this function.
- When disabling DSView™ software access, please reboot the appliance after the operation to ensure that all active connections to the DSView™ software are terminated.
- When enabling DSView™ software access, please delete the appliance and re-add it to the DSView™ software to restore secure mode operation.

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.
- When changing the DHCP server for private interfaces to be internal or external from the Administration/Targets/Port Configuration/DHCP Settings screen of the Web interface, network communication to the IP-based targets may be lost as the IP-based targets will retain the assigned network addresses from the previous DHCP server. To restore communication, reset the targets or disconnect and then reconnect the targets to the private port of the appliance so that the targets will request a new IP address from the new DHCP server.

Web Interface

- Occasionally the Web interface may stop responding and the cursor will continuously spin when hovering over the Web interface. If this occurs, please refresh or reload the browser tab to continue.
- 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.
- The event logs may become excessively large over time. To improve performance, please export and save the event logs, then clear all entries periodically.
- 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.
- Browsing in the Web interface consumes memory in the client browser that is not returned. Please close the browser session to recover client memory.
- Web interface sessions cannot be established using the Internet Explorer 8.0.6001.18702 (Cypher Strength 128-bit). Please upgrade to Internet Explorer 8.0.7601.17514 (Cypher Strength 256-bit), or a newer version of Internet Explorer to support this functionality.
- If the appliance is configured for an IPv6 network, Web interface sessions cannot be established using the Firefox browser version 25 or later. Please use an alternate browser to access the appliance.
- Web interface sessions cannot be established on some clients using Firefox browser version 31. Please browse to the About: Support page and reset Firefox, then try to establish the session again after the browser restarts.

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

- If a KVM session is canceled prior to being completely launched and a second KVM session is launched to the same target, a *Path Blocked -- wait a moment and try again* error may be seen. Please wait up to 150 seconds before repeating the launch. This delay can be avoided by allowing a session to completely launch prior to termination.
- A second KVM session launch from the appliance Web interface to the same UMIQ module on an appliance from the same client will fail. Use the DSView™ 4 software interface if this function is required.

- 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.
- The [Windows] key is passed through to the target even when the keyboard pass through is disabled.
- For Suse 11 targets, the mouse will not synchronize or align.
- For Red Hat 6.2 targets, the dual mouse feature is not functional until after the target is rebooted.
- For Macintosh targets, the mouse will not synchronize or align.
- 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.
- If a UMIQ module is disconnected from the appliance while a KVM session using that UMIQ module is active, the session will not be removed from the Active Sessions list until the *Delete Offline* configuration is selected for the given UMIQ module.
- 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

- A Virtual Media session can only be connected to the most recently established KVM session. To avoid this situation, please have only one active KVM session open.
- When launching an ActiveX KVM Viewer session, a small window or tab remains open after the KVM session has been closed. Please also close this extra window or tab.
- Macro changes made while in Full Screen mode are currently lost after switching to Normal view mode then switching back to Full Screen mode.
- On a Macintosh OS, the Virtual Media tool does not allow disks to be mapped after Virtual Media activation.
- 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.
- CAC or Smart Card readers are not currently supported by the KVM Viewer.
- The Pass all keystrokes to target setting is enabled by default and is re-enabled at the beginning of every new viewer session.
- Intermittently, option selection in the viewer is not stored. Please re-select the option as needed.
- Occasionally, the Scaling options under the View menu of the KVM Viewer are not visible after a KVM session is launched.
- Some portions of the KVM Viewer interface are not correctly localized for languages other than English.

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 auto detected Serial PDU port cannot currently be reconfigured as a Serial Console port.
- When a network PDU is added to the Avocent® Universal Management Gateway appliance, its port may have an incorrect value for the port number in the associated event message.
- 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 Web interface setting of outlet thresholds for Liebert® MPH2 or MPX2 PDUs is currently not functional. Please launch a Browser session to the native Liebert® MPH2 or MPX2 PDU Web interface to set outlet thresholds.
- PDUs may be deleted from the Avocent® Universal Management Gateway 2000 appliance only when the PDU is in a No Response state. When the PDU is deleted, all its outlets are also deleted. Individual outlets cannot be deleted from the appliance.
- When connecting the Liebert® MPH/MPX PDU to a private port of the Avocent® Universal Management Gateway appliance for discovery, please ensure that the PDU is power-cycled or reset after connection so that the appliance can be assigned a network address through DHCP to the PDU. If the appliance firmware is updated by USB boot or net boot, please power-cycle or reset the PDU after the appliance is restored to normal operation. If the PDU is power-cycled or reset before the appliance is restored, it may be necessary to manually discover the PDU by defining and launching a SP discovery range including the IP address range for the private port.
- 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.

- Target state transition events may be generated when a PDU is added to the appliance.

Environmental Sensors

- Humidity sensors may fail to be detected.
- The Digital Output relays DO1 and DO2 as defined on the back panel of the appliance and in the configuration settings in the Web interface are reversed.
- The Avocent PM 1000/2000/3000 PDU internal temperature sensor is not displayed in the Web interface with the environmental sensors under the Sensors tab. Please read the internal sensor information from Targets/PDU/Properties.