VERTIV™

Avocent® Universal Management Gateway 2000/4000/6000 Appliance

Release Notes

VERSION 4.2.3.16, JUNE 28, 2019

Release Notes Section Outline

1 Update Instructions

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

NOTE: After you have followed the instructions in the installer/user guide and completed the update, please reboot the appliance. If you are using the *Trellis*™ platform, see section 11 in these release notes for more information and next steps.

Important Notes

- If the current appliance version is older than 2.6.0.14, please contact Technical Support for additional assistance with net booting the appliance to version 3.1.2.10 prior to upgrading to the latest version.
- When upgrading the appliance to version 2.2.1.10 (or later) from 2.1.1.6 (or earlier), please ensure power is retained on the appliance for at least three hours 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 upgrades or rollback, please contact Technical Support for additional assistance.

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.

NOTE: Please allow at least three hours for the upgrade process to complete once it is started.

Compatibility with the Avocent® DSView™ Management Software

NOTE: All references to "DSView™ software" within these release notes refer to version 4.5, Service Pack 5 (SP5) or later, unless otherwise specified.

To upgrade your system for this release:

NOTE: The client computer must use a 32-bit browser with a 32-bit Java JRE to launch sessions from the Avocent® DSView™ management software. Java JRE 8u181 and 10.0.1 were used in testing.

1. Upgrade the Avocent® DSView™ management software to SP5 (Service Pack 5) or later. If there are DSView™ software log in issues using the Internet Explorer browser after upgrading, ensure that the SSLv2 and SSLv3 options are disabled in the browser.
2. Upgrade the Avocent® Universal Management Gateway appliance plug-in to version 4.2.3.16 or later.
   NOTE: The appliance plug-in must be at the same version or newer than the appliance firmware for correct operation.
3. Upgrade the Avocent® Universal Management Gateway appliance to version 4.2.3.16.
4. Execute the appliance resync action for the Avocent® Universal Management Gateway appliance within the Avocent® DSView™ software.
5. If this upgrade sequence could not be followed and the Avocent® Universal Management Gateway appliance cannot properly be managed using the Avocent® DSView™ software, please remove the appliance from the software and then re-add the appliance again.

After upgrading the appliance to version 4.2.3.16, if KVM sessions launched via the Avocent® DSView™ software display an error message, resync the appliance with the software and try again.

2 Local Client Requirements

SOFTWARE	VERSION
Java (32-bit)	Java 8 Update 201
Internet Explorer	11
Firefox	62
Chrome	68
Edge	EdgeHTML 13

NOTE: If the Firefox browser prompts that the Flash plug-in should be updated when the appliance Web interface is accessed, please update the Flash plug-in to the latest version before continuing, if possible.

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: If using Java 7 and attempting KVM or SP SSH, Telnet, or SoL session launches from the Avocent® Universal Management Gateway appliance, ensure that the TLS1.1 and TLS1.2 boxes are checked and the SSL 2.0 box is unchecked in the Advanced tab of the Java Control Panel.

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

After upgrading the Avocent® Universal Management Gateway appliance to version 2.9.0.25 or later, the web user interface may not open in Firefox if the correct TLS options are not selected.

To ensure the correct TLS options are selected in Firefox:

1. Enter **about:config** in your browser.
2. Enter **security.tls** in the Search bar.
3. Under the Preference Name section, ensure the security.tls.version.max Value is set to 3.
4. Under the Preference Name section, ensure the security.tls.version min Value is set to 1.
5. Close all browser sessions.
6. Open a new session and verify that you have access to the Avocent® Universal Management Gateway appliance Web interface.

NOTE: If the appliance Web interface cannot be accessed using the Internet Explorer 11 or a Firefox browser, follow these steps to reset the browser.

To reset the browser for Internet Explorer 11:

1. Select *Internet Options- Advanced* and click the *Reset* button.
2. Follow the prompted instructions to reboot the computer, then re-open Internet Explorer 11.
3. Press **Ctl+Shift+Del** on the keyboard to clear the cache and history. On the Delete Browsing History window, select all checkboxes except the Preserve Favorites website data checkbox, then click *Delete*.
4. Select *Internet Options- Content* and select the *Clear SSL State* button.
5. Close and re-open Internet Explorer 11.

To reset the browser for Firefox:

1. Click the *Menu* (hamburger) icon, then select *Privacy*.
2. Select *Clear your recent history*. The Clear All History window opens.
3. Select *Everything* as the time range to clear, and select the appropriate details to clear, including *Cookies* and *Cache*.
4. Click *Clear Now*, then close and re-open the browser to launch the appliance Web interface again.

NOTE: If using Java 8 Update 60 or later, a KVM session cannot be started if the encryption setting of either the Video or the Keyboard/Mouse is set to128-bit SSL. Because this setting is not supported by these Java versions, please do not use it.

NOTE: If using Java with the Microsoft Edge browser in a Windows 10 client, Java must be installed using the Internet Explorer 11 browser.

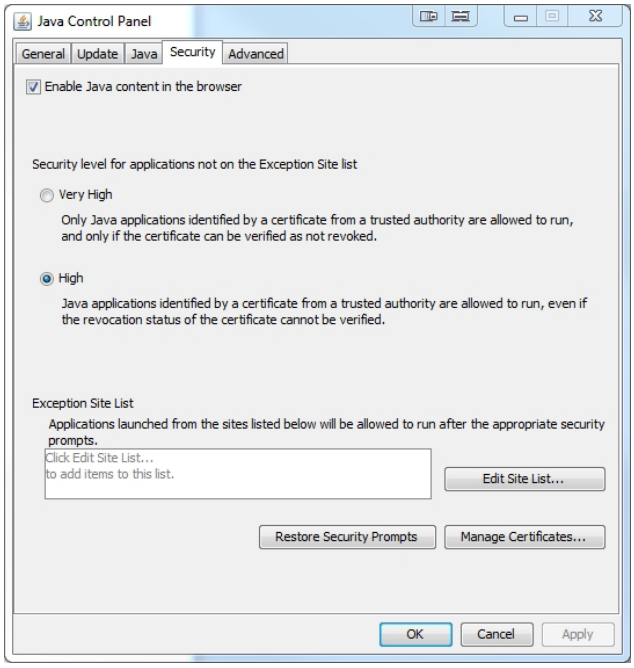
IMPORTANT NOTE: The Java KVM viewer certificate existing in older firmware versions is expiring on February 17, 2019. Unless you use the HTML5 viewer with virtual media capabilities (introduced in firmware version 3.4.1.10), update to this newest firmware (version 4.2.3.16) or edit the Java Console Security settings on each computer client by that date, you will be unable launch KVM sessions.

To edit the Java Console security settings:

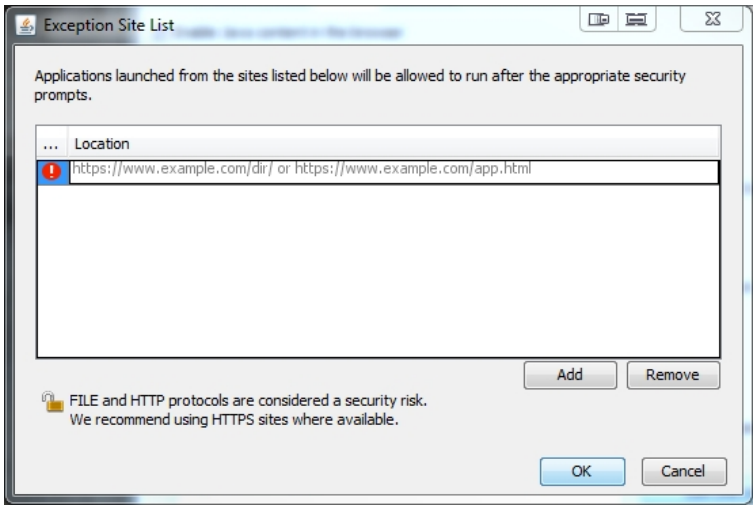
NOTE: If using Java 10, menus may vary, but the same workaround applies.

1. From your Windows Control Panel, click *Java*.
2. When the Java Control Panel opens, click the *Security* tab.

3. Select the High radio button to indicate the desired security level, then click the *Edit Site List* button. This will enable you to add the expired certificate information to the Exception Site List so that you can continue using it.



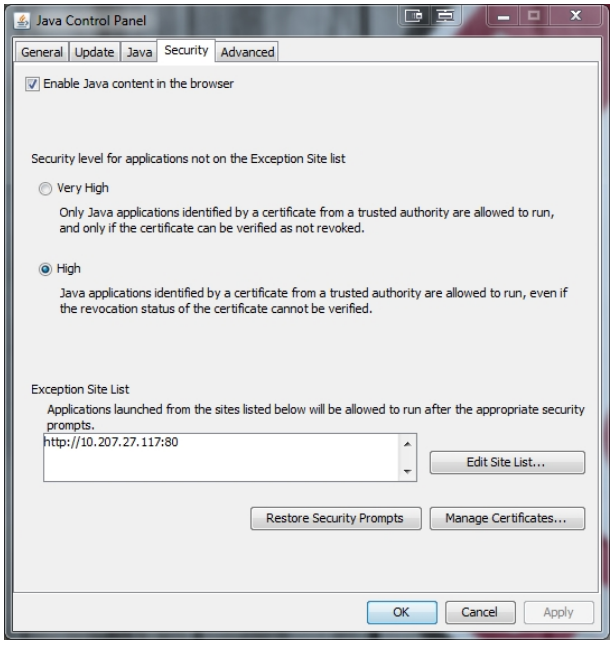
4. When the Exception Site List window opens, click the *Add* button and enter your appliance IP address in the following format: **http://**<applianceIP>**:80**



5. Click *Add* again, then click *Continue* when the Security Warning pop-up appears. This allows an HTTP address in the Exception Site List.

6. When the Exception Site List window opens again, click *OK*.

7. Back in the Java Control Panel, your appliance IP address is now listed in the Exception Site List. Click *OK* to be able to launch a KVM session that will allow use of the of the expired viewer certificate.



3 Features and Enhancements

Firmware version 4.2.3.16 is an update of the Avocent® Universal Management Gateway 2000/4000/6000 appliance firmware. 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:

- The UMIQ-E operating mode is now supported. See the UMIQ and UMIQ-E Module Support section of these release notes for more information.
- The Geist I-03 PDU firmware version 5.3.2 is now supported and can be upgraded through the appliance.
- The Vertiv™ Liebert® RPC2™ communications module (Vertiv™ MPX™, Liebert® MPH™ and Vertiv™ MPH2™ PDUs) firmware version 14.0.0.3 is now supported and can be upgraded through the appliance.

Appliance Support Issues Addressed in this Release

ISSUE	RESOLVED ISSUE DESCRIPTION
CAS-05145-L9T5C0	A dynamic DHCP range may now be successfully added through the appliance UI without failures.
CAS-02477-Z0N7B8	Mouse sync is no longer advertised in scenarios such as BIOS mode access where the sync feature is unavailable.
CAS-03885-G4M8N7	Ports 7001 to 7040 (used for Telnet session to serial ports) are now blocked in the appliance firewall by default; unblock these ports if needed.
487234-867017894	Alternate port 4206 (used for HTML5 KVM sessions) is now blocked in the appliance firewall by default.

4 UMIQ and UMIQ-E 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 Avocent® DSView™ 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*.

Using UMIQ-E Modules

NOTE: UMIQ-E mode is only recommended when there is a specific customer need to use it. The current UMIQ-V2 has a long field history of reliable performance in its use cases.

The UMIQ-E (enhanced) module is a new operating mode of the UMIQ-V2 KVM module. When *UMIQ-E* mode is selected, the module can be connected to the Avocent® Universal Management Gateway appliance through the public Ethernet ports (GB1 or GB2) and be accessed through the customer intranet if a network connection can be established between the Avocent® Universal Management Gateway appliance and the module. In order for KVM sessions to be maintained through USB power loss, use the UMIQ-PS external power supply in this configuration. Up to 40 UMIQ-E or UMIQ modules can be managed by the Avocent® Universal Management Gateway appliance, and limitations on the number of KVM sessions are the same for both modules.

The UMIQ-E module has the following limitations:

- The UMIQ-E module may get hung up when there are large file transfers using virtual media with simultaneous mouse movement. Avoid moving the mouse during file transfers.
- Discovery of the UMIQ-E module is not currently persistent such that if the UMIQ-E module or the Avocent® Universal Management Gateway appliance loses power, the module must be rediscovered. Discovery of the UMIQ-E module is persistent when the appliance IP address is locally configured in the module.
- Low power mode when directly connected to the Avocent® Universal Management Gateway appliance is not supported. Use the UMIQ-PS external power supply to ensure UMIQ-E module power is maintained.
- Smart Cards are not supported.
- FIPS mode is not supported.
- In some cases (such as encrypted video and virtual media file transfer), UMIQ-E module performance is less optimal than UMIQ module performance.

Please see the Avocent® Universal Management Gateway Appliance Installer/User Guide for more information on the following:

- Networking requirements: For optimal KVM performance, there are specific networking requirements for the UMIQ-E module.
- Conversion procedures: Following the provided instructions in the installer/user guide allows you to convert UMIQ modules to UMIQ-E modules.
- General module information: The installer/user guide details local configuration, discovering/adding modules, launching sessions, factory resets and other general module procedures.

Other UMIQ-E Module Notes

- The UMIQ-E module is shown as “UMIQ-E” on the Targets page and the Administration-Targets-KVM Management-Devices page.
- The UMIQ-E module EID number begins with 500441 when listed on the Administration-Targets-KVM Management-Devices page.
- When locally configuring the UMIQ-E module, the configuration site is available from either of the following:
    - The Vertiv web site: https://www.vertiv.com/en-us/support/tools-applications/umiq-e-configuration/
    - The Avocent® Universal Management Gateway appliance: Select *Administration-Targets-KVM Management-Configure UMIQ-E* in the appliance Web interface.

5 Smart Card Support

Tested Smart Card Readers

CARD READER ALIAS	DESCRIPTION
SCM335	SCR335 SCM Microsystems
Precise 250	Precise Biometrics Precise 250 MC
KOBIL KAAN	KOBIL KAAN Base
Lenovo Gemplus	Lenovo Gemplus
Cherry 1044	Cherry GmbH Smart Terminal 1044
OMNIKEY 5125	OMNIKEY CardMan 5125
OMNIKEY 5121	OMNIKEY CardMan 5121
OMNIKEY 3121	OMNIKEY CardMan 3121 SC
SCR 3311	SCR 3311 SCM Microsystems
SCR 3310	SCR 3310 SCM Microsystems 905057

Smart Card Test Samples

CARD READER ALIAS	DESCRIPTION
SC1	Oberthur CS PIV End Point v1.08
SC2	SN: 1111-00024038 (T-0,1)
SC3	409061459963280D2A24 64K V2C S6C 353723 (T-0)
SC4	DOD CAC GEMALTO TOPDLGX4144
SC5	20505000734830727826 64K V5.2 O5B-1
SC6	4820502B121613CBE736 128k v5.5-n (T-0)
SC7	Oberthur ID-One PIV (Type A) Large D 4820-502B-2007-00104440 (T-1)

The combinations of card readers (rows) and cards (columns) in the following table were successfully tested using the remote Java viewer (J), the remote Active X viewer (A), and/or the local port viewer (L).

Tested Combinations of Card Readers and Cards

CARD READER	SC1	SC2	SC3	SC4	SC5	SC6	SC7
SCM335	JA	JA	JA	JA	JA	J* A	J* AL
Precise 250	JA	JA	JA	JA	JA	J* A	--
KOBIL KAAN	JAL	JAL	JAL	JAL	JAL	J* AL	J* AL
Lenovo Gemplus	JA	JA	JA	JA	JA	J* A	J* A
Cherry 1044	JAL	JAL	JAL	JAL	JAL	J* AL	J* AL
OMNIKEY 5125	JAL	JAL	JAL	JAL	JAL	J* AL	J* AL
OMNIKEY 5121	JAL	JAL	JAL	JAL	JAL	J* AL	J* AL
OMNIKEY 3121	JAL	JAL	JAL	JAL	JAL	J* AL	J* AL
SCR 3311	JAL	JA	JA	JA	JA	J* A	J* AL
SCR 3310	JAL	JA	JA	JA	JA	J* A	J* AL

*__NOTE:__ With Java KVM viewer 5.04.04 build 363, card removal does not always trigger card unmapping. You must unmap the card through the Java KVM viewer Tools menu to ensure the smart card is unmapped from the target. (Avocent® Universal Management Gateway appliance 3.4.0.16 rdist, Java KVM viewer 5.04.04 build 363, Active KVM viewer 5.04.04 build 349.)

6 External Sensor Support

NOTE: The following external sensors were tested with the port connection and test scenarios where sensors were automatically discovered and monitored by the appliance.

Tested External Sensors

EXTERNAL SENSORS	PORT CONNECTION	TEST SCENARIOS
SN-Z01 Single Temperature Probe	TH1/TH2	• Single SN-Z01 sensor connected to each port sequentially. • Reported as SN-T as it cannot be distinguished from the corresponding SN-T sensors from the info returned. • Not chainable as limited by cabling.
SN-Z02 Three Temperature Probe	TH1/TH2	• Single SN-Z02 sensor connected to each port sequentially. • Reported as three SN-T sensors as it cannot be distinguished from the corresponding SN-T sensors from the info returned. • Not chainable as limited by cabling.
SN-Z03 Three Temperature 1 Humidity	TH1/TH2	• Single SN-Z03 sensor connected to each port sequentially. • Reported as two SN-T and one SN-TH as it cannot be distinguished from the corresponding SN-T/SN-TH sensors from the info returned. • Not chainable as limited by cabling.
SN-3C Modular Dry Contact	TH1/TH2	• Single SN-3C sensor connected to each port sequentially. • Chain of five SN-3C sensors connected to each port sequentially, where the cable was less than 20 meters in total length.

EXTERNAL SENSORS	PORT CONNECTION	TEST SCENARIOS
SN-2D Modular 2-Door Contact	TH1/TH2	• Single SN-2D sensor connected to each port sequentially. • Chain of ten SN-2D sensors connected to both ports simultaneously, where each cable was less than 20 meters in total length.
SN-TH Modular Temp/Humidity Sensor	TH1/TH2	• Single SN-TH sensor connected to each port sequentially. • Chain of five SN-TH sensors connected to each port sequentially, where the cable was less than 20 meters in total length.
SN-T Modular Temperature Sensor	TH1/TH2	• Single SN-T sensor connected to each port sequentially. • Chain of five SN-T sensors connected to each port sequentially, where the cable was less than 20 meters in total length.
SN-L Leak Sensor	TH1/TH2	• Single SN-T sensor connected to each port • Not chainable.
IRM-S01T Temperature	SNSR	• Single IRM-S01T sensor connected to the port • Chain of two IRM-S01T sensors connected to the port, where the cable was less than 20 meters in total length.
IRM-S02TH Temperature + Humidity	SNSR	Single IRM-S02TH sensor connected to the port.
AD-S Smoke	DI1/DI2	Single AD-S sensor connected to each port sequentially.
AD-IM Motion	DI1/DI2	Single AD-IM sensor connected to each port sequentially.

7 PDU Support

Tested PDUs and Firmware

CARD READER ALIAS	FIRMWARE VERSION	COMMENTS
Geist I-02	3.3.3	Supported in a limited manner, including firmware upgrade and web access through an SPAccess browser session. Outlet control and monitoring are not yet supported.
Geist I-03	5.3.2	Supported in a limited manner, including firmware upgrade and web access through an SPAccess browser session. Outlet control and monitoring are not yet supported.
Vertiv™ RPC2 (MPX™, MPH™, MPH2™)	14.0.0.3	The PDU userid/password must be supplied to enable firmware upgrade functionality.

8 Service Processor Support

Tested Service Processors/Servers and Firmware

SERVICE PROCESSOR	FIRMWARE VERSION	COMMENTS
Cisco UCS-B Chassis and Blades	4.0(1d)	N/A
Cisco UCS CIMC/Monolithic (C210)	1.4(3z)	Support for this Service Processor has been obsoleted. It is not tested or maintained.
Cisco UCS CIMC/Monolithic (C220)	4.0(1a)	N/A
Dell C Series (PowerEdge C6220)	2.53	N/A
Dell DRAC 4 (PowerEdge 1850)	1.75 (Build 06.03)	Support for this Service Processor has been obsoleted. It is not tested or maintained.
Dell DRAC 5 (PowerEdge 2950)	1.65 (12.08.16)	Support for this Service Processor has been obsoleted. It is not tested or maintained.
Dell DRAC/MC	1.6.0	Support for this Service Processor has been obsoleted. It is not tested or maintained.
Dell iDRAC blades (M600/M605/M805)	1.65	Support for this Service Processor has been obsoleted. It is not tested or maintained.
Dell iDRAC6 blades (M610/M710)	3.85	SSH sessions to the iDRAC6 blades are not functional; iDRAC6 is only supporting ciphers that are blocked from the appliance for security reasons. Telnet must be enabled to discover these iDRAC6 blades. We recommend that Telnet be disabled by default and disabled following discovery.
Dell iDRAC6 monolithics (R210/R410/R710)	2.91	N/A
Dell iDRAC7 blade (M520, M620)	2.61.60.60	N/A
Dell iDRAC7 monolithic (R320)	2.61.60.60	N/A
Dell iDRAC8 blade (M630, FC630)	2.61.60.60	N/A
Dell iDRAC8 monolithic (R430)	2.61.60.60	N/A
Dell iDRAC9 blade (M640) and monolithic (R640)	3.21.23.22	N/A
Dell M1000E Chassis	6.20	N/A
Dell FX2s Chassis	2.20	N/A
Dell VRTX Chassis (Express)	3.20	N/A
FSC iRMC (BX630 S2)	2.30G	Support for this Service Processor has been obsoleted. It is not tested or maintained.

SERVICE PROCESSOR	FIRMWARE VERSION	COMMENTS
FSC iRMC S2 (RX300 S4)	5.76A	Support for this Service Processor has been obsoleted. It is not tested or maintained.
FSC iRMC S4 (RX200 S8)	9.20F	N/A
HP BladeSystem	4.90	N/A
HP iLO 2 (DL580 G5)	2.33	N/A
HP iLO 3 (DL380 G7)	1.90	N/A
HP iLO 4 (DL360p Gen8)	2.62	N/A
HP iLO 5 (DL360p Gen10)	1.37	N/A
IBM BladeCenter (E/8677)	BPET68C	Support for blades connected to this Service Processor has been obsoleted. The blades are not tested or maintained
IBM IMM (x3550 M2, x3650 M2)	YUOOH2B	Support for this Service Processor has been obsoleted. It is not tested or maintained
IBM IMM2 (x3250 M4)	1AOO82E	Support for this Service Processor has been obsoleted. It is not tested or maintained
IBM RSA II (x3550, x3850)	GGEP42A	Support for this Service Processor has been obsoleted. It is not tested or maintained.
IPMI 1.5	N/A	N/A
IPMI 2.0	N/A	N/A
Lenovo Flex Chassis	1AON24A(2.0.0)	N/A
Lenovo IMM2 (x240 M5)	TCOO46E(5.10)	N/A
Lenovo XCC	CDI328M(2.10)	N/A
Oracle ILOM3 (Sun Server X3-2)	4.0.4.22	N/A
SUN ALOM (Netra 240)	1.6.10	Support for this Service Processor has been obsoleted. It is not tested or maintained.
SUN ELOM (x2200 M2)	3.2	Support for this Service Processor has been obsoleted. It is not tested or maintained.
SUN ILOM (Sun Fire x4250)	3.0.6.15f	Support for this Service Processor has been obsoleted. It is not tested or maintained.

Supported Service Processor Features Table

TABLE KEY			
✓	(Supported feature)	G	(Get only)

*	(Supported if available)	S	(Set only)
†	(Features inherited from chassis)	G/S	(Get and Set)
D	(Only via Direct Command support in the Avocent® DSView™ software)		

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	Auto Login SSH	vKVM	Virtual Media
IPMI 1.5	✓			✓	✓	✓	G/S	S*	✓			*	*	*	*			
IPMI 2.0	✓	G*	G*/S*	✓	✓	✓	G/S	S*	✓	✓	✓	*	*	*	*			
IDRAC 9 (14G)	✓	G	G/S	✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	*	*
IDRAC 8 (13G)	✓	G	G/S	✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	*	*
IDRAC 7 (12G)	✓	G	G/S	✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	*	*
IDRAC 6 (11G)	✓	G*	G*/S*	✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	*	*
Dell C Series	✓	G*	G*	✓	✓	✓	G/S		✓	✓	✓	*	*		*	*	*	*
Dell DRAC 5	✓			✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	✓	✓
Dell DRAC 4				✓	✓		G		✓	✓		D	*	*	*	*	D	D
HP ILO 5	✓	G	G/S	✓		✓	G	G/S	✓	✓	✓	*	*		*	*	✓	✓
HP ILO 4	✓	G	G/S	✓	✓	✓	G	G/S	✓	✓	✓	*	*		*	*	✓	✓
HP ILO3	✓	G	G/S	✓	✓	✓	G	G/S	✓	✓	✓	*	*		*	*	✓	✓
HP ILO2	✓	G		✓	✓			G/S	✓	✓		*	*	*	*	*	✓	✓
Oracle ILOM3	✓	G		✓	✓	✓	G/S	G/S	✓	✓		D	*		*	*	D	D
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	✓	✓	✓	*	*	*	*	*	✓	✓
FSC IRMC S4	✓	G*	G*/S*	✓	✓	✓	G/S	G/S	✓	✓	✓	*	*	*	*	*	✓	✓

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	Auto Login SSH	vKVM	Virtual Media
Dell M1000E	✓	G	G/S		✓		G/S	G/S	✓			*	*	*	*	*		
Dell M1000E (Blade)		G		✓				G/S	✓	✓		†	†	†	†	✓	*	
Dell FX2	✓	G	G/S		✓		G/S	G/S	✓			*	*	*	*	*		
Dell FX2 (Blade)		G		✓				G/S	✓	✓		†	†	†	†	✓		
Dell VRTX	✓	G	G/S		✓		G/S	G/S	✓			*	*	*	*	*		
Dell VRTX (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		✓						†	†	†
Lenovo Flex		G			✓		G/S		✓			*	*	*	*	*		
Lenovo Flex (Blade)	✓	G	G/S	✓						✓		*	*	*	*		*	†
Lenovo XCC	✓	G	G/S	✓			G/S	G/S	✓	✓	✓	*	*	*	*		*	†
Cisco UCS-B (Chassis)	✓	G	G			✓	G	G/S				*	*	*	*	*		
Cisco UCS-B (Blade)	✓	G	G			✓		G/S	✓	✓							✓	✓
Accessible Target (Generic)												*	*	*	*			

General Notes and Issues

- Service Processor vKVM access through the Microsoft Edge browser is not supported, unless noted, for the specific Service Processor.
- Service Processor SSH, Telnet and SoL sessions through the Microsoft Edge browser are not supported.
- 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:
  - 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).
  - 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.
- If the SPAccess port range is modified prior to appliance firmware upgrade, the port range must be reconfigured to the desired value after the appliance upgrade is completed.
- The SPAccess design assumes that the Service Processor port assignments will not be reconfigured to use different port(s). Please retain the default port assignments for correct operation.
- Termination of an SPAccess session from within the appliance session tab on a factory restored appliance may cause the appliance Web interface to become unresponsive. Please use other interfaces to close the SPAccess sessions.
- 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 Avocent® DSView™ software event log if the appliance is managed using DSView™ software.
- Currently, an SoL session cannot be disconnected by clicking the *X* button at the top right of the viewer window. Please disconnect the session from the appliance Web interface on the Service Processor session screen.
- Power state transitions from Service Processors may not be identified and displayed in the appliance Web interface or DSView™ 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.
- HP iLO3 and iLO4 Service Processors may be added or discovered using credentials with an IPMI/DCMI privilege of Administrator, Operator or User. The management capability of the HP iLO3 and iLO4 Service Processor through the appliance will be limited by the privilege of the credential used to add the Service Processor. All other Service Processors supported by the appliance can be added or discovered using credentials with an IPMI/DCMI Administrator privilege.
- The Java 7 Update 51 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.
- When connecting a Service Processor to a private port of the Avocent® Universal Management Gateway appliance for discovery, 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 an 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 manually adding or discovering Service Processors, occasionally the Service Processor is displayed on the Administration/Targets/Service Processors page but not in the Targets or the Administration/Targets page of the appliance Web interface. Close the browser and re-open it to resolve the issue.
- If the Rescue action is taken to restore management of a Service Processor set for automatic periodic password change, please wait several minutes for the Rescue action to complete.

Service Processor Firmware Upgrade

- The firmware files from the Service Processor vendors can be extracted for upgrade as follows:
  - Cisco UCS-B: Use the ucs*.bin file provided by Cisco.
  - Cisco UCS-C: Extract the upd-pkg-<model>.cimc.full.<version>.bin file from the <model>-cimc-.<version>.zip file from the <version>\cimc folder within the compressed executable provided by Cisco. For example, for version 1.4(3t), the upd-pkg-c200-m1-cimc.full.1.4.3t.bin file is extracted from the c200-m1-cimc.1.4.3t.zip file.

  - Dell DRAC5: Extract the firmimg.d5 file from the payload folder within the compressed executable provided by Dell.
  - Dell iDRAC6: Extract the firmimg.d6 file from the payload folder within the compressed executable provided by Dell.
  - Dell iDRAC7/iDRAC8: Extract the firmimg.d7 file from the payload folder within the compressed executable provided by Dell.
  - Dell iDRAC9: Extract the firmimgFIT.d9 file from the payload folder within the compressed executable provided by Dell.
  - Dell iDRAC7/8/9 blade programmed through the chassis: Provide the entire update package from Windows. For example, for version 3.21.26.22, the file is iDRAC-with-Lifecycle-Controller_Firmware_FDMV1_WN64_3.21.26.22.EXE. The Dell CMC Extended Storage Card must be installed and the Extended Storage feature must be enabled.
  - Dell M1000e: Extract the firmimg-<version>-A00.cmc file from the compressed executable provided by Dell. For example, for version 4.5, the extracted file is fmrimg-4.5-A00.cmc.
  - HP iLO2, iLO3, iLO4, and iLO5: Extract the ilox_<version>.bin file from the root folder or the image folder from the compressed executable provided by HP. For example, for version 2.03 for iLO4, the extracted file is ilo4_203.bin.
  - HP BladeSystem: The upgrade file is specifically provided by HP. For example, for version 4.30, the downloaded file is hpoa430.bin.
  - IBM IMM, IMM2: Extract the *.upd from the root folder within the compressed executable provided by IBM.
  - Lenovo IMM2: Extract the *.upd from the root folder within the compressed executable provided by Lenovo.
  - Oracle ILOM3 Extract the *.pkg from the Model/Firmware/service-processor folder within the compressed executable provided by Oracle.
- Service Processor firmware maintained in a remote share must be reinstalled in the remote share starting with appliance firmware version 3.2.0.30.
- Service Processor firmware for an iDRAC7 blade must be downloaded separately from firmware for an iDRAC7 monolithic or tower, even though the firmware is the same for blades, monolithics and towers.
- Service Processor firmware for an iDRAC8 blade must be downloaded separately from firmware for an iDRAC8 monolithic or tower, even though the firmware is the same for blades, monolithics and towers.
- The current firmware version of a Service Processor will be displayed as “---“ if the version cannot be identified. Please either re-discover or delete and re-add the Service Processor to the appliance to try to resolve this issue.
- The alert and optional trap indicating that the Service Processor is not using supported firmware does not currently include the Service Processor target name.

Cisco UCS-B Chassis and Blades

- If all blades within a Cisco UCB-B chassis are not present following upgrade to this firmware version, please delete the chassis and any blades that were discovered as standalone Service Processors and rediscover the chassis only to restore access to all 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 Avocent® 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.

- Blade vKVM sessions launched through the chassis are not currently supported. Please launch blade vKVM sessions through the blade underneath the chassis.
- Chassis auto login sessions are not supported.
- An HTML5 vKVM session to the Cisco blade will freeze if virtual media is activated. Please use one of the other viewers for this function.
- Power capping for the Cisco chassis cannot currently be set to more than 1100 watts. Please access the Cisco UCS Manager directly to control this function.
- The Cisco blade firmware cannot be updated when the Host Firmware Package within the Firmware Policy is configured to the Blade Package setting. Please remove this configuration in the Service Processor for proper firmware update operation.
- Power threshold for the Cisco blade cannot currently be configured. Please access the Cisco UCS Manager directly to control this function.

Cisco UCS-C210 Monolithics

The SPAccess vKVM session is not accessible when launched from the appliance local port interface.

Dell C Series

- The Dell C Series default username and password of root/root is not included in the appliance default names list. If discovery of these Service Processors is needed, please add the appropriate credentials to the default names list.
- The Dell C Series vKVM and Virtual Media applets fail when launched using Java 8 and when using the VGA console of the Avocent® Universal Management Gateway appliance. Please use Java 7 Update 71 for these operations.
- Occasionally power control failures are seen on the Dell C Series. Retry these power control operations.

Dell DRAC4 and DRAC5

- When the maximum number of sessions in DRAC4 or DRAC5 has been reached, a new Auto Login 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’.
- 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 vKVM and Virtual Media applets fail when launched using Java 8 and using the VGA console of the Avocent® Universal Management Gateway appliance. Please use the remote Web interface from a Windows client running Java 7 Update 71 for these operations.
- The DRAC5 firmware version may not be displayed properly on the Properties screen through the Web interface following an appliance upgrade.

- The server type associated with the DRAC5 Service Processor is currently not displayed on the Administration/Targets/SP Management page.
- The DRAC5 does not support use of the forward slash (“/”) in login passwords. Avoid use of the forward slash in the password definition.

Dell iDRAC6 Monolithics

- SPAccess vKVM is supported using the Edge browser for this Service Processor.
- SPAccess vKVM sessions using the Java viewer to this Service Processor are failing when Java JRE8u131 and newer is running on the client. Use the ActiveX viewer or Java JRE8u121 on the client.
- 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.
- Some lower-cost servers using the iDRAC6 Service Processor have a shared network port for the Service Processor and the server. If these servers are connected to the Avocent® Universal Management Gateway appliance on the public Ethernet port, the server functions are more easily available to the users. The servers may still be connected to the Avocent® Universal Management Gateway appliance on a private network port, but there may be firewall configuration needed to enable all the server functions.

Dell iDRAC6 Blades

- SPAccess sessions for the M600, M605 and M805 blade servers are currently not supported. The M600, M605 and M805 blade servers use a certificate with MD5 signature which is blocked from the Avocent® Universal Management Gateway appliance for security reasons.
- The Java vKVM viewer within current M610 and M710 blade Service Processor firmware is not compatible with the current Java 8u181 release, so SPAccess vKVM is not functional through the appliance local or remote Web interface.
- SSH Auto Login sessions are currently failing on the M610 and M710 blade Service Processor running v3.75 firmware due to an extended response delay in the Service Processor. Please use v3.60 of the Service Processor firmware to avoid this issue.
- SPAccess vKVM is supported using the Edge browser for the M600, M605 or M805 blade Service Processors.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10 for the M600, M605 or M805 blade Service Processors, as this browser is not supported through the native Service Processor interface directly.
- 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-Auto Login buttons are not enabled in the Web interface or in the Avocent® DSView™ 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.

- The M600, M605 and M805 blade Virtual KVM Java applets now fail when launched from a client running Java 8, which means they will fail using the VGA console of the Avocent® Universal Management Gateway appliance. Please use the remote Web interface with the client running Java 7 Update 71 for these operations.
- When a Virtual KVM session is launched for a M610 and M710 blade that is discovered through the M1000e chassis, the chassis vKVM preference is not used. If the alternate viewer is preferred, please launch the desired viewer through the blade native Web interface.
- 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 Auto Login 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.
- An HTML5 vKVM session launched from a blade installed in an M1000e blade chassis when the session was initiated by logging into the chassis is failing in the native Service Processor Web interface due to a limitation in the Service Processor firmware. The SPAccess sessions that operate in this scenario are also failing. To work around the Service Processor limitation, either use the Java or ActiveX viewers, or add the blade to the appliance as a standalone target.
- 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.
- SPAccess sessions launched to iDRAC blades in an M1000e blade chassis are currently not functional. Please add or discover the individual iDRAC blades separately from the chassis (if this has not already been done), then launch SPAccess sessions directly to the iDRAC blade server.
- SoL data buffering to blades installed in an M1000e blade chassis is currently not functional.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10 for the M600, M605 or M805 blade Service Processors, as this browser is not supported through the native Service Processor interface directly.
- SPAccess is not supported with the Internet Explorer 11 browser in Windows 10 for the M610 and M710 blade Service Processors.

Dell iDRAC7 Monolithics and Blades

- SPAccess vKVM is supported using the Edge browser for the monolithic Service Processors.
- Java vKVM sessions for iDRAC7 blades discovered thru the chassis are currently not functional. Please use the HTML5 vKVM viewer for these sessions.
- The Virtual Console plug-in in the native iDRAC7 Web interface cannot be selected during an SPAccess autologin or browser session. Please use the SPAccess vKVM to launch the vKVM (Virtual Console) session.
- SPAccess is not supported using the Internet Explorer 11 browser in Windows 10 for the monolithic or blade Service Processors, as this browser is not supported through the native Service Processor interface directly.
- 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.
- Some lower-cost servers using the iDRAC6 Service Processor have a shared network port for the Service Processor and the server. If these servers are connected to the Avocent® Universal Management Gateway appliance on the public Ethernet port, the server functions are more easily available to the users. The servers may still be connected to Avocent® Universal Management Gateway appliance on a private network port, but there may be firewall configuration needed to enable all the server functions.
- The iDRAC7 Basic Management Service Processor is currently not automatically discovered. Please manually add as an IPMI Service Processor.

Dell iDRAC8 Monolithics and Blades

- SPAccess vKVM is supported using the Edge browser for these Service Processors.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10, as this browser is not supported through the native Service Processor interface directly.
- The Virtual Console plug-in in the native iDRAC8 Web interface cannot be selected during an SPAccess autologin or browser session. Please use the SPAccess vKVM to launch the vKVM (Virtual Console) session.
- The SSH button may be disabled for these Service Processors. If so, please use the Command Line Interface (CLI) to initiate the SSH session.
- An SPAccess vKVM session is currently not launching to the iDRAC8 blade when the appliance is operating in DSView™ software proxy mode. Please use the appliance Web interface or DSView™ software non-proxy mode for this function.
- A SPAccess HTML5 vKVM session is currently not launching to the iDRAC8 monolithic server through the local Web interface. Please either use the remote Web interface or the Java or ActiveX viewers on the local Web interface for this function.
- A Virtual Media device cannot be mapped during a SPAccess HTML5 vKVM session. Please use the Java or ActiveX viewers for this function.

Dell iDRAC9 Blades

- An SPAccess HTML5 vKVM session is currently not launching to the iDRAC9 blade. To work around this limitation, please use the Java or ActiveX viewers.
- An SPAccess vKVM session is currently not launching to the iDRAC9 blade when the appliance is operating in DSView™ software proxy mode. Please use the appliance Web interface or DSView™ software non-proxy mode for this function.
- The Backspace and Delete keys are not functional during a Telnet session to the iDRAC9 blade or monolithic Service Processor. Please use the SSH session instead of Telnet, or press **CTRL+Backspace** to delete characters.

Dell iDRAC9 Monolithics

The Backspace and Delete keys are not functional during a Telnet session to the iDRAC9 blade or monolithic Service Processor. Please use the SSH session instead of Telnet, or press **CTRL+Backspace** to delete characters.

Dell FX CMC and Blades

An SPAccess vKVM session is currently not launching to the FX blade when the appliance is operating in DSView™ software proxy mode. Please use the appliance Web interface or DSView™ software non-proxy mode for this function.

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).
- The Java vKVM viewer within the current iRMC S2 Service Processor firmware is not compatible with the current Java 8u131 release, so SPAccess vKVM is not functional through the appliance local or remote Web interface. The previous Java 8u121 release appears to remain compatible with the Service Processor firmware, if use of a previous Java release is consistent with the security policy of the customer.
- iRMC S2 SPs that use login 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.
- The FSC iRMC S2 Service Processor only supports firmware upgrade through its native Web interface, so automated firmware upgrade through the Avocent® Universal Management Gateway appliance is not supported.
- SPAccess is not supported with the Internet Explorer 11 browser in Windows 10, as this browser is not supported through the native Service Processor interface directly.

FTS iRMC S4

- When launching an Auto Login SPAccess session, an extra prompt appears that the user must click to continue the log in to the Service Processor.
- The Java vKVM viewer within the current iRMC S4 Service Processor firmware is not compatible with the current Java 8u131 release, so SPAccess vKVM is not functional through the appliance local or remote Web interface. The previous Java 8u121 release appears to remain compatible with the Service Processor firmware, if use of a previous Java release is consistent with the security policy of the customer.
- The Java vKVM viewer within the current iRMC S4 Service Processor firmware is not compatible with the current Java 8u131 release, so SPAccess vKVM is not functional through the appliance local or remote Web interface. The previous Java 8u121 release appears to remain compatible with the Service Processor firmware, if use of a previous Java release is consistent with the security policy of the customer.
- SPAccess vKVM is not supported when the HTML5 viewer is selected for this Service Processor. Please configure the Service Processor to use either the Java or ActiveX viewers for this functionality.
- Virtual Media connections to the FTS iRMC S4 Service Processor are not supported from the appliance local port interface as the Service Processor does not natively support this functionality in a Linux environment.
- SoL configuration for the FTS iRMC S4 Service Processor is currently not functional.
- Power capping configuration for the FTS iRMC S4 Service Processor is currently not functional.

HP iLO2

- SoL sessions to iLO2 blades are currently not functional.
- SPAccess sessions for the iLO2 servers launch very slowly. Please wait up to three minutes for the launch to complete.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10.

HP iLO3

- 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 since the iLO3 does not support this function.
- The SoL baud rate selection should not be enabled in the appliance Web interface since the iLO3 does not support this function.
- The currently supported iLO3 firmware has compatibility issues with the Firefox browser version 33, which also impacts the SPAccess vKVM operation.
- The currently supported iLO3 firmware has compatibility issues with the Chrome browser version 45. Please use either the Internet Explorer or Firefox browsers for SPAccess vKVM operation.
- SPAccess vKVM is only supported using the Java viewer with the Internet Explorer 11 browser in Windows 10.
- An iLO3 with a password containing the ampersand special character (&) cannot currently be added, discovered or monitored by the appliance. Please use a password without this special character.

HP iLO4

- 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 since 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 Virtual KVM Native ActiveX preference selection for iLO4 should actually be labeled as “Native .Net”.
- 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:
    - Select *Java IRC* within the Remote Console section.
    - 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.

  NOTE: After a Virtual Media session is complete, the vKVM session window will disappear and the vKVM session must be restarted.
- The currently supported iLO4 firmware has compatibility issues with the Chrome browser version 45. Please use either the Internet Explorer or Firefox browsers for SPAccess vKVM operation.
- SPAccess vKVM is only supported using the Java viewer with the Internet Explorer 11 browser in Windows 10.
- An iLO4 with a password containing the ampersand special character (&) cannot currently be added, discovered or monitored by the appliance. Please use a password without this special character.
- Configuration of alert destinations for iLO4 Service Processors is currently not functional.

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.
- SPAccess sessions are not functioning to the HP BladeSystem chassis or blades due to an obsolete default certificate. Update the HP Blade System chassis certificate in the Service Processor Web interface by selecting *Active Onboard Administrator - Certificate Administration - Certificate Request - Generate a self-signed certificate.*

- SPAccess vKVM sessions using the Java viewer launched to blades in an HP BladeSystem blade chassis are not currently supported in a direct connection to the blade chassis or through the appliance. Please either use the ActiveX viewer or manage the blade as a standalone Service Processor.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10 when an iLO2 blade is discovered through the BladeSystem chassis.
- SoL data buffering to blades installed in a HP blade chassis is currently not functional.

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 log in 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 five 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.
- The vKVM viewer within the IBM BladeCenter will not load when launched under the latest Chrome and Firefox browsers. Please use the Internet Explorer browser for this functionality. The SPAccess vKVM even using the Internet Explorer browser is failing to load when using the latest (Java 8 or 9) run-time environments. The previous Java 7u60 release appears to remain compatible with the Service Processor firmware, if use of a previous Java release is consistent with the security policy of the customer.
- 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.

IBM IMM Monolithics

- The password set functionality does not support the double quote (”) special character as the character is not supported by the Service Processor.
- Remote SPAccess sessions for the IMM monolithic servers are currently not functional directly to the Service Processor or thru the appliance. SPAccess sessions launched through the appliance local port are functional.

- SPAccess vKVM is supported using the Edge browser for this Service Processor.
- SPAccess vKVM is only supported using the Java viewer with the Internet Explorer 11 browser in Windows 10.
- 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 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 vKVM is supported using the Edge browser for this Service Processor.
- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10, as this browser is not supported through the native Service Processor interface directly.
- 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 an SPAccess session to a IMM2-based server, all page elements are not downloaded. Refreshing the browser window will restore all page elements.
- Configuration of alert destinations for IBM IMM2 monolithic Service Processors is currently not functional.

IPMI 2.0 Service Processor

SPAccess vKVM sessions are not supported for this generic Service Processor, but this option is presented for some generic Service Processors. Please ignore this option.

Lenovo Flex Chassis

- Serial-over-LAN (SoL) configuration is currently not supported for the Lenovo Flex chassis or its blades.
- Configuration of alert destinations for the Lenovo Flex chassis is currently not functional.
- When attempting to launch a blade-through-chassis login from an SPAccess session to the chassis, the blade login must use https.

Lenovo IMM2 Blades

- SPAccess vKVM is not supported with the Internet Explorer 11 browser in Windows 10, as this browser is not supported through the native Service Processor interface directly.
- ActiveX vKVM sessions for IMM2 blades discovered thru the chassis are currently not functional. Please use the Java vKVM viewer for these sessions.
- SPAccess vKVM using the ActiveX viewer does not successfully launch with the initial launch action. The viewer must be launched again manually for proper operation.
- SPAccess vKVM is not supported when the HTML5 viewer is selected for this Service Processor and a blade-thru-chassis session is launched. Please discover the IMM2 blade as a separate Service Processor for this functionality.

Lenovo XCC

- Occasionally, the desktop screen is not displayed at the launch of a vKVM session using the Chrome browser. Please terminate and relaunch the session to restore the desktop display.
- SPAccess vKVM sessions to the XCC will disconnect if the XCC is connected to one of the private IP ports of the appliance. Please orient the XCC on the public IP ports to support this function.

Oracle ILOM3 Monolithics

- The Oracle ILOM3 can only be managed when connected to a public interface of the Avocent® Universal Management Gateway appliance.
- The Oracle ILOM3 viewer CD-ROM redirection is not compatible with the appliance local port environment. Please use the remote Web interface for this function.

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.

9 External Network Port Usage

The table below identifies the network port range, the built-in service name defining the port range, and a description of the port range usage.

NOTE: Incoming connections on all ports are blocked by default, and these firewall policies are exceptions to that default policy.

PORT RANGE	SERVICE NAME	FIREWALL POLICY DESCRIPTION AND USAGE
0	srv-PING	Open to allow network connectivity verification over icmp. If Related or Established connections are blocked, Service Processor discovery will fail.
20	srv-FTP-Data	Open to allow appliance firmware upgrade.
21	srv-FTP-Commands	Open to allow appliance firmware upgrade.
22	srv-SSH-Serial-Session	Open to allow SSH sessions to appliance and Service Processor Management.
23	srv-Telnet-Session	Open to allow Telnet sessions to appliance.
53	srv-DNS	Open to allow DNS connectivity.
67-68	srv-DHCPD	Blocked to disallow DHCP requests to the appliance over the public interfaces.
69	srv-TFTP-Services	Open to allow UMIQ module and Service Processor firmware update.
80	srv-HTTP-Services	Open to allow Service Processor firmware update.
137	srv-NetBIOS-NS	Used for Samba client connectivity initiated by the appliance.
138	srv-NetBIOS-DS	Used for Samba client connectivity initiated by the appliance.
139	srv-NetBIOS-SS	Used for Samba client connectivity initiated by the appliance.
161	srv-SNMP	Open to allow connectivity to PDUs and other SNMP-based targets.
162	srv-SNMP-Traps	Open to accept SNMP traps from PDUs and other SNMP-based targets.
443	srv-Web-UI	Open to allow Web interface operation, HTML5 KVM and serial sessions, and Service Processor Management using Redfish.
445	srv-MS-Directory-Service	Used for Samba client connectivity initiated by the appliance.
502	srv-Modbus	Open to allow connectivity to Modbus-based devices scanned by the *Trellis*™ platform.
514	srv-External-syslog	Open to allow Syslog server functionality.
623	N/A	Used for IPMI client connectivity initiated by the appliance.
843	srv-Adobe-Flex	Not included in firewall policy, no longer required by appliance.
1078	srv-DS-View-proxy	Open to allow KVM and serial sessions to be proxied through the DSView™ software.
2068	srv-KVM-session	Open to allow KVM sessions.
3211	srv-Discovery-protocol	Open to allow the DSView™ software to discover the appliance.

PORT RANGE	SERVICE NAME	FIREWALL POLICY DESCRIPTION AND USAGE
3212	srv-DRIP-protocol	Open to allow UMIQ module connectivity.
3502	srv-DS-View-plug-in	Open to allow DSView™ software connectivity.
3871	srv-Security-protocol	Open to allow DSView™ software -launched sessions and appliance authentication using DSView™ software.
4011	srv-PXE-boot-server	Open to enable PXE boot server functionality for Service Processors (currently not supported)
4112	srv-Data-logging-DSView	Open to allow serial port logging to DSView™ software (currently not supported).
4206	srv-KVM-websock-session	Blocked to disallow HTML5 KVM sessions using this alternate port.
4321	srv-UMG-Service-1	Blocked by default, policy and service defined for ease of debug.
4440	srv-UMG-Service-2	Open to allow *Trellis*™ platform connectivity.
6379	srv-UMG-Service-14	Not included in firewall policy, service defined for ease of debug.
6443	srv-Trellis-Platform-OHS	Open to allow *Trellis*™ platform connectivity.
7001-7040	srv-UMG-Service-9	Blocked to disallow Telnet access to serial port connections.
8011	srv-UMG-Service-3	Open to allow *Trellis*™ platform connectivity.
8012	srv-UMG-Service-4	Open to allow *Trellis*™ platform connectivity.
8080	srv-UMG-Service-6	Open to allow Java viewer download to client.
8123	srv-UMG-Service-7	Open to allow Service Processor firmware upgrade.
8128	srv-UMG-Service-8	Blocked by default, policy and service defined for ease of debug.
8161	srv-UMG-Service-13	Blocked by default, policy and service defined for ease of debug.
9002	srv-Trellis-Event	Open to allow *Trellis*™ platform connectivity.
9003	srv-Trellis-Event-2	Open to allow *Trellis*™ platform connectivity.
10191	srv-UMG-Service-5	Blocked by default, policy and service defined for ease of debug.
11099	srv-UMG-Service-10	Blocked by default, policy and service defined for ease of debug.
32123	srv-UMG-Service-11	Blocked by default, policy and service defined for ease of debug.
47777-48177	srv-Velocity-BACNet	Open to allow connectivity to BACNet and Velocity-based devices managed by the *Trellis*™ platform.
50000-59999	srv-SPAccess	Open to allow SPAccess sessions.
61616	srv-UMG-Service-12	Blocked by default, policy and service defined for ease of debug.

10 Known Issues

Upgrading

- KVM sessions may fail after the upgrade of an appliance that had been previously added to the Avocent® 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.
- When performing a local port upgrade using the CLI, please format the USB drive using the FAT32 format.

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.

Local Serial Console

If there is a need to execute a downloaded script through the local serial console or from a SSH session, the script to execute must be in the /download folder of the appliance. Scripts contained within the /diag folder can no longer be executed.

VGA Console

NOTE: Enabling the URL bar will allow anyone with access to the VGA console to use the browser.

- 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 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 log in 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.
- If the KVM session window is sent to the background by the Web interface session window, please press **Alt+Tab** to restore the KVM session window to the foreground.
- If the VGA console is used to set a static IP address for the appliance, the Web interface must be refreshed after the set to enable further use.

Authentication

- SSH connections can be made to disabled Serial Ports; however, the connection to the Serial Target itself will not be established.
- LDAP authentication will fail if not working if DNS servers are configured, but are not accessible by the appliance. Remove the DNS server configuration as a workaround if needed.

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.
- When switching networking mode from Failover to Failover-Routed, please switch to Normal mode first.
- When using the appliance in a failover scenario, Service Processors, PDUs and any other IP-based targets should be connected to a private port of the appliance and a public port so that access to those targets is retained following a failover.
- If the appliance was configured to use a static IP address prior to an appliance firmware upgrade, then the DNS settings are not retained after the upgrade is complete. Re-enter the DNS settings manually as a workaround.
- 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

- 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.
- 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.
- Occasionally when multiple clients are actively logged into the Avocent® Universal Management Gateway appliance, an exception error may be seen on one of the clients. Select *OK* to bypass the error and continue the session
- The password strength setting is not functional and will cause errors if set. As a workaround, please keep the strength setting to None and maintain the desired password strength through assignment convention.
- If a default user (admin/operator/user) is deleted from the appliance, that deleted user cannot be re-created.
- If the default user operator or user is deleted from the appliance, their corresponding Power User or User roles will not operate correctly.
- The contents of the Targets page are not always automatically refreshed when running the Firefox browser. If this occurs, please manually refresh or use the Internet Explorer or Chrome browsers.

- If a Discovery Range cannot be set following an appliance time configuration, please reboot the appliance to restore Discovery Range configuration.
- Events are not currently generated after scheduled backup.
- If the system date is set to January 1, 1970 (maybe through expiration of the clock battery), a user cannot log in to the Web interface using the Internet Explorer browser. Please use the Firefox or Chrome browsers to log in and correct the date. Use an NTP server, if possible, to automatically adjust the date.
- The USB ports cannot currently be disabled using the Web interface.
- 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.
- When performing a Factory Reset on a UMIQ module, an exception error may be displayed.
- 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.
- The targets on the /Administration/Targets screen cannot currently be sorted by clicking on a column name.
- Browsing in the Web interface consumes memory in the client browser that is not returned. Please close the browser session to recover client memory.
- The syslog destination configuration cannot be changed once it is configured the first time. Please contact Technical Support for assistance if this parameter must be reconfigured.
- The network port used for the Web interface cannot be reconfigured from port 443.
- 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.
- Please allow a target rename operation from the Administration/Targets screen to complete before attempting another target rename operation.
- If errors are seen when renaming multiple targets in one operation from the Administration/Targets screen, please only rename one target at a time.
- IP address filtering only supports the IPv4 address format.

- Intermittent failures occur when using the 1:1 NAT Wizard to add an SP or PDU. Please add the SP or PDU to the appliance prior to configuring a 1:1 NAT using that SP or PDU.

Logging

- 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 event logs may become excessively large over time. To improve performance, please export and save the event logs, then clear all entries periodically.
- 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.
- When SNMP events are logged, the embedded timestamp of the SNMP event is not updated with the appliance clock.
- Syslog and SNMP events that are associated with the target device in a 1:1 NAT configuration do not have the correct source IP address.

Target Discovery and Operations

- 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.
- After UMIQ modules are added to a Target Group, a view of the members of the Target Group will show all UMIQ modules in the appliance included in the Target Group, even though only the configured subset of the UMIQ modules are actually in the Target Group.
- Attempts to assign access to more than 30 targets to a User Group in one operation may fail. Please limit the number of targets assigned in one operation.
- When deleting many targets in one operation, please wait at least 30 seconds for the operation to complete.

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-E Module

- The port number for UMIQ-E modules not connected to a private port of the appliance is shown as “99” instead of “0” like other targets not connected to a private port of the appliance.
- When converting a UMIQ-V2 module to a UMIQ-E module, the target name and first six characters of the EID will change. The last six characters of the EID is a unique identifier of the module and can be used to track the module through the operation.
- A UMIQ-E module must be deleted from an appliance before it can be managed by a different appliance.

- When a UMIQ-E module is disconnected from the public interface of the appliance, it may remain in an online state on the appliance Web interface. The appliance must be rebooted to clear the online status.
- Occasionally, a successfully discovered UMIQ-E module may be shown as unsuccessfully discovered.

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.
- When logged into the appliance Web interface using the Internet Explorer browser, if a KVM session is launched, followed by a serial session, followed by an additional KVM session, the second and subsequent KVM launches will not open the KVM viewer. Launch another instance of the appliance Web interface to launch another KVM session.
- When scan mode is launched for several targets, subsequently launching a session to one of the targets being scanned will cause that target to be removed from the scan sequence.
- 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.
- A custom EDID may currently only be set through per-UMIQ module settings and not by default for all UMIQ modules.
- 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.
- The following settings are recommended on the server to optimize local mouse alignment:
    - Windows: Initial Setting- 50% Speed. No Acceleration
    - Linux: Uncheck Enable Absolute Synchronization in Tools/Session Options/Mouse/Mouse Synchronization.
    - Macintosh: Uncheck Enable Absolute Synchronization in Session Options/Mouse/Mouse Synchronization.

  NOTE: Refer to the Mouse and Pointer Settings Technical Bulletin found online with the other appliance user manuals and tech bulletins for detailed help. This technical bulletin can be found at http://pcs.mktg.avocent.com/@@content/manual/590809644b%283%29.pdf.
- Mouse absolute synchronization must be disabled for sessions launched using the Microsoft Edge browser.
- Mouse synchronization may be lost after switching to full screen mode in KVM sessions launched to Linux clients. Please refer to the Mouse and Pointer Settings Technical Bulletin found online (see previously listed link) for detailed help.
- Mouse synchronization may be lost after rolling the mouse over the Stat window. Please realign the local cursor to recover synchronization.

- 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.
- Selecting a higher resolution display will produce slower sessions and may cause mouse response to be jumpy. Reducing the screen resolution should improve mouse stability. 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 the UMIQ module is connected to a Dell M1000e chassis iKVM port, the mouse clicks may not always be passed to the Avocent® OSCAR™ graphical user interface. Please use the hotkeys and keyboard to operate the OSD if the mouse interface is not functional.
- When using the DSView™ 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™ 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.
- If KVM data is encrypted on an Avocent® DSView™ software KVM session, the appliance must be connected to the DSView™ software in secure mode.
- If KVM data is not encrypted but a DSView™ software KVM session cannot be established, the appliance must be connected to the DSView™ software in secure mode.
- 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™ software is managing the appliance, the appliance would need to be resynced in the DSView™ software.
- A Service Processor should not be assigned the same name as a UMIQ module target.

Java/ActiveX KVM Viewer

- 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.
- Within a Virtual Media session, an error is displayed when ejecting a mapped thumb drive from the target and the drive does not fully unmap. The mapped drive no longer appears in the details section and it is disconnected from the target, but the drive is still checked as mapped. Please restart the Virtual Media session to recover.
- If problems occur during ActiveX viewer installation, please launch the Internet Browser running as administrator, then attempt to install the viewer by launching a KVM session.

- If an ActiveX viewer installation fails to locate the Microsoft Visual C++ 2008 SP1 Redistributable Package and aborts, please install this package on the client and restart the ActiveX viewer installation. The package is available from https://www.microsoft.com/en-us/download/details.aspx?id=5582.
- 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 will crash with a *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.
- Clients using the Macintosh High Sierra (OS X 10.13) OS cannot map removable USB media to a target using the Java viewer, because permissions in OS X have changed such that the Java process is no longer able to access system devices, such as removable USB storage devices.

  To achieve this function:
  NOTE: The viewer must be launched with root permissions, using sudo or similar, through the following steps.

  1. Log in to the Avocent® Universal Management Gateway appliance from the Mac client.
  2. Download the Java viewer for intended target.
  3. Note the name of the downloaded jnlp file, to be referred to as [viewer.jnlp] going forward.
  4. Open a terminal.
  5. Run the following command, making sure to replace [viewer.jnlp] with the name of your downloaded file.

     sudo javaws Downloads/[viewer.jnlp]
  6. In the terminal, enter your OS X user password when prompted by the sudo command.
  7. Interact with the viewer as normal. You should now be able to activate virtual media and map USB devices as needed.
- A KVM session launched using the Firefox or Chrome browsers may freeze when a second smart card is connected to the client. Please either use the Internet Explorer browser if needed or restart the KVM session to use the second smart card.
- A KVM session launched using a smart card for authentication will not connect to a target running Windows 10.
- Virtual Media sessions do not connect to a CD/DVD drive on a target running the Sun Solaris 10 operating system. Please use a thumb drive on the target if needed.
- The Pass all keystrokes to target setting is enabled by default and is re-enabled at the beginning of every new viewer session.
- The Hagul key on a Korean keyboard will fail to function if Microsoft IME is enabled on the client. Please disable Microsoft IME for proper operation.
- 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.

HTML5 KVM Viewer

- Up to eight concurrent HTML5-based KVM sessions may be launched through a single appliance.
- Up to three concurrent HTML5-based KVM sessions may be launched through a single client to any set of appliances.
- The Internet Explorer browser is limited to supporting up to three concurrent HTML5-based sessions.
- HTML5-based session settings are not stored and need to be reset at the beginning of each session.
- An HTML5-based session cannot share a session or preempt another session. Please use the Java or ActiveX viewer for these operations.
- The HTML5-based viewer does not currently block multiple sessions from the same client and browser to the same target. Please avoid this scenario.
- The HTML5 KVM viewer supports ISO image creation only when launched in the Chrome browser.
- The HTML5 KVM viewer supports a single cursor mode only when sessions are launched using the Chrome and Firefox browsers.
- After setting a custom EDID and launching an HTML5 KVM session, an error may be seen when returning to the appliance Web interface. Refresh the screen to clear the error.
- Mouse synchronization for a Solaris target only occurs when the mouse is clicked.
- The HTML5 KVM Viewer “Allow clipboard paste” setting is inverted. Please clear the checkbox to enable clipboard paste.
- If file paste is cancelled within the HTML5-based viewer running in the IE browser, clipboard paste stops working for the duration of the session.
- HTML5-based sessions will not launch if the DNS settings are blank or set to 0.0.0.0. Please set the DNS parameter to a valid value.
- The Num Lock and Scroll Lock settings in the viewer cannot be automatically synchronized with the target. Please manually synchronize these key settings at the start of the KVM session.
- Occasionally the HTML5 KVM viewer will enter a state where a new session cannot be launched with the error “The session failed to launch because an HTML5 KVM session limit has been reached”. If this issue occurs, either use a different client or reboot the appliance to restore normal operation.

Serial Targets (including Terminal Servers)

- Serial sessions launched through the Microsoft Edge browser are not supported.
- If power is removed from an auto-sensed serial target while a session is in progress, the session must be restored after the serial target is powered up. If port auto-sense is disabled for the appliance port used for the serial session, the serial session will remain active during a power cycle.
- 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.

- The port signals within the Administration/Targets/Serial Management/Serial Ports screen are currently not displayed.
- Only one Terminal Server can be deleted from the appliance at a time. If multiple Terminal Servers are deleted in a single operation, exceptions may be seen in the Web interface and an appliance reboot may be required for recovery.
- Logging of virtual serial port sessions is currently not supported.
- If virtual serial ports are enabled in a Terminal Server after the Terminal Server has been added to the appliance, sessions to the newly enabled virtual serial ports will fail. Please delete and re-add the Terminal Server to the appliance to avoid this issue.
- Virtual serial ports are always displayed as port 0 within a Terminal Server.
- Session status for sessions launched to Virtual Serial Ports through the Web interface is always displayed as idle. Launch sessions using the Avocent® DSView™ software if correct status is needed.
- If an Avocent® ACS advanced console system or an Avocent® Universal Management Gateway appliance is discovered or manually added as a Terminal Server without matching credentials, sessions launched to the associated Virtual Serial Ports will fail. Manually add or discover these appliances using matching login credentials for complete functionality.

Power Distribution Units (PDUs)

- Serial sessions launched through the Microsoft Edge browser are not supported.
- 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™ 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.
- Please ensure that the Liebert® MPH™/MPX™ and Vertiv™ MPH2™ PDUs are upgraded to the latest released PDU firmware prior to connecting them to the Avocent® Universal Management Gateway appliance. Consult the PDU documentation as needed.
- When connecting the Liebert® MPH™/MPX™ and Vertiv™ MPH2™ PDUs 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 an 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™ and Vertiv™ MPH2™ PDUs) 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.

- 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 display 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.
- The SNMP community settings for each Liebert® MPH™/MPX™ PDU shown on the Administration/Targets/ Rack PDU/Network PDU tab will display as LiebertEM name and RO type following an appliance reboot.
- A browser connection to a Liebert® MPH™/MPX™ PDU configured for HTTPS operation cannot be completed since the Liebert® RPC-1000™ implementation uses an MD5-based certificate that is not accepted by the appliance. Please upgrade the PDU to use the RPC-2000 card.
- The default name assigned to a Vertiv™ MPH2™ or MPH2™ PDU does not follow the default naming convention to prefix the name with the appliance MAC address. When the appliance is used with the Avocent® 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.
- When manually adding a Liebert® MPH™/MPX™ PDU to the appliance, if the community name provided is not defined within the PDU, the PDU is not added to the appliance.
- When manually adding a Liebert® MPH™/MPX™ PDU to the appliance, the screen is not automatically refreshed to show the PDU after it has been added. Please switch away from the Administrator/Targets/PDU Management/Network PDU screen and return again to see the newly added PDU.
- The Browser function for Vertiv™ MPH2™ or MPH2™ PDUs is not operational if the PDU is configured to operate using HTTPS. If the PDU is connected on the appliance public port, please access the PDU native Web page directly instead of through the appliance. If the PDU is connected to an appliance private port, then the appliance firewall limits access to the PDU and it is less of a security risk to configure the PDU to operate as HTTP if needed.
- Occasionally when adding or modifying the community name of a Liebert® MPH™/MPX™ PDU, the Web interface will stop accepting alpha character input and only accept numeric character input. Please log out of the Web interface and back in to clear this error state, and avoid using tabs to switch between fields.
- The appliance currently does not support configuration of the Vertiv™ MPH2™ PDU. The Vertiv™ Mass Configuration Tool (MCT) available on the MPH2 PDU software download site should be used for PDU configuration. Please contact Technical Support for more workaround information if needed.
- A firmware update of Vertiv™ MPH2™ PDUs through the appliance Web interface requires that the PDU is added to the appliance using a userid and password.
- The Web interface display for Vertiv™ MPH2™ or MPH2™ PDU Phases does not include voltage, power consumption, apparent power or power factor.

- The Web interface display for Vertiv™ MPH2™ or MPH2™ PDU Branches always displays zero for power consumption, apparent power and power factor.
- The Web interface setting of outlet thresholds for Vertiv™ MPH2™ or MPH2™ PDUs is currently not functional. Launch a Browser session to the native MPH2™ or MPH2™ PDU Web interface to set outlet thresholds.
- Multiple outlet configuration accessed through the PDU will stop at the first locked outlet and not continue to further unlocked outlets. Please do not select locked outlets for configuration update.
- A PDU power limit configuration always displays an error when completed, even when there was no error. Please refresh the screen to check for an incomplete setting.
- The PDU environment sensor configuration screen allows multiple sensors to be selected, but only the first sensor selected is editable. Please select one environment sensor at a time for configuration.
- The PDU Sensors Humidity Reset is currently not functional.
- 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.
- Target state transition events may be generated when a PDU is added to the appliance.
- The outlets for Liebert® MPH™/MPX™ or Vertiv™ MPH2™/MPH2™ PDUs cannot currently be renamed.

Accessible Targets

Vertiv™ MPH2™ PDUs must be upgraded to firmware version 11.0.0.7 or later prior to being added to the Avocent® Universal Management Gateway appliance as an Accessible Target to enable HTTP/HTTPS access through 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.

FIPS Operation

IMPORTANT NOTE: FIPS mode is not functional in firmware version 4.2.3.16. Please revert to firmware version 4.2.1.19 for this capability.

- When *FIPS mode* is selected, the appliance will use the following for cryptographic operations:
  - An embedded FIPS 140-2 validated cryptographic module (Certificate #2473) built into a customized Linux 3.18.9 distribution
  - An embedded FIPS 140-2 validated cryptographic module (Certificate #1279) built into a customized Linux 3.18.9 distribution
- When the appliance is operating in FIPS mode, an MD5-based certificate is used to connect the appliance to the Avocent® DSView™ software in trust-all mode. Set the connection to Secure Mode to ensure that MD5 is not included in the certificate.
- Prior to setting an appliance to FIPS mode, the appliance should be deleted from the DSView™ software and then re-added to the DSView™ software after the appliance is set to run in FIPS mode. Similarly, before removing an appliance from FIPS mode, the appliance should be deleted from the DSView™ software and then re-added to the DSView™ software after the appliance is removed from FIPS mode.
- Prior to importing a third-party certificate through the appliance Web interface, the appliance must be set from FIPS mode back to normal mode. After the import, the appliance can be set back into FIPS mode.
- FIPS mode is not supported for the UMIQ-E operating mode of the UMIQ modules.

11 *Trellis*™ Real-time Infrastructure Optimization Platform Support

IMPORTANT NOTE: Firmware version 4.2.3.16 is an update of the Avocent® Universal Management Gateway 2000/4000/6000 appliance firmware. This firmware version is not intended for use with the *Trellis*™ real-time infrastructure optimization platform. Please wait for the next appliance firmware version before updating a *Trellis*™ platform installation. If there are failures related to appliance TCP port 4440 used by the *Trellis*™ platform, this port may be blocked in the appliance firewall in this release.